INSTITUTE OF COMPARATIVE LAW

CYBER LAW – SERBIA

Published by:
Institute of Comparative Law
Belgrade

For the Publisher:
Prof. Vladimir Čolović, PhD

Reviewed by:
Professor Dragan Simeunović, Ph.D.
Faculty of Political Sciences, University of Belgrade
Professor Božidar Banović, Ph.D.
Academy of criminalistics and police studies, Belgrade
Hatidža Beriša, Ph. D.
National Defence University of Defence, Belgrade

Authors:
Prof. dr. Mina Zirojević,
Institute of Contemporary Law, Belgrade
Prof. dr. Zvonimir Ivanović,
Academy of criminalistics and police studies, Belgrade

Prepress:
DOGMA

Printed by:
SAJNOS Doo, Novi Sad

ISBN 978-86-80186-79-5

Copies:
200

Publishing of this collection of papers was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia

INSTITUTE OF CONTEMPORARY LAW
MONOGRAPH NO. 180

CYBER LAW – Serbia

Prof. dr. Mina Zirojević,
Institute of Contemporary Law, Belgrade

Prof. dr. Zvonimir Ivanović,
Academy of criminalistics and police studies, Belgrade

Belgrade, 2021

TABLE OF CONTENTS

PART IV
PRIVACY PROTECTION

PART V
COMPUTER RELATED CRIME

GENERAL INTRODUCTION

General Background

The Republic of Serbia is a democratic state of all of its citizens. The Republic of Serbia in its composition also comprises two autonomous provinces: Vojvodina and Kosovo-Metohija. Belgrade is the capital of Serbia.

The territorial organisation of Serbia includes five regions (Belgrade region, Vojvodina region, Sumadija and western Serbia region, eastern and southern Serbia region and Kosovo-Metohija region). They include the City of Belgrade as a separate territorial unit established by the Constitution and law, and 30 administrative areas, 24 cities, 30 urban municipalities, 150 municipalities, 6,158 villages and 193 urban settlements. With a population of 1,659,440, it is the country's administrative, economic and cultural centre.

In 2009, the National Assembly adopted the Law on the design and use of the coat-of-arms, flag and anthem of the Republic of Serbia. According to this law, the Serbian coat-of-arms is the one defined by the Law on the coat-of-arms of the Kingdom of Serbia from 16 June 1882. The national anthem of Serbia is a 19th century ceremonial song "Bože Pravde" (God of Justice).[1]

> Serbia is located on the Balkan Peninsula or South Eastern Europe (about 79% of the territory) and the Pannonia Plain or central Europe (about 20% of the territory). Land border has a length of 2114 km. It occupies an area of 88,361 km². It borders Hungary to the north; Romania and Bulgaria to the east; Macedonia to the south; Croatia, Bosnia, Montenegro to the west and claims a border with Albania through the disputed territory of Kosovo.

The northern part of the Republic occupies the plains, and in the southern areas of the hills and mountains. There are over 15 peaks above 2,000 meters above sea level and the highest peak is Đeravica (on Prokletije Mountain) with a height of 2656 meters.

The climate is continental (Pannonia Plain and its rim to 600 m above sea level), moderate continental (in the central part of Serbia, up to 800 m above sea level), mountain (mountains over 800 m above sea level) and changed the Adriatic and Mediterranean (in Metohija and the southern part of Kosovo valley)

The mountain landscape of Serbia explains the emergence of many canyons, gorges and caves (The cave, Ceremošnja Risovača ...), and provides a wealth of additional beauty exceptionally preserved forests composed has many endemic species, as well as the wealth of water, streams, springs, lakes, etc. . Forests cover 26% of the territory.

Serbia's rivers drain into the sea three basins: the Black Sea, Adriatic and Aegean. Navigable rivers are the Danube (588 km), Sava (206 km), Tisa (168 km), and partly Velika Morava (185 km full course). Other major rivers include the Western Morava (308 km), South Morava (295 km), Ibar (272 km), Drina (220 km) and Timok (202 km). The largest lake in Serbia is lake of Đerdap with 163 km² (the Romanian part 253 km²).

[1] https://www.euprava.gov.rs/en/aboutserbia.

The natural heritage of the country's national parks occupies a special place. Serbia has 5 national parks: Iron Gate, Kopaonik, Tara, Šar Planina and Fruška gora. All national parks have a high-altitude climate, health and recreational values.

In Serbia, there are numerous natural and artificial lakes, as well as about 300 sources of mineral water, some of which are commercially exploited in famous bottled water brands.

> The ethnic composition of the population of the Republic of Serbia is very diverse as a result of turbulent history of the Western Balkans. The largest proportion of the population are the Serbs 82.7%, 3.9% Hungarians, Bosniaks 1.8%, Roma 1.4%, Yugoslav 1.1%. A smaller percentage of Croats, Montenegrins, Albanians, Slovaks, Vlachs, Romanians, Macedonians, Bulgarians, Bunjevacs Muslims are living in Serbia too. This data are from 2002, without Kosovo and Metohija.[2]

After the outbreak of the war in the former Socialist Federal Republic of Yugoslavia (SFRY), a large number of people migrated, mostly to their "parent" republics.

Depending on the severity of war conflicts and the sources of data, the number of refugees and desplaced persons varied and ranged from 350,000 to 800,000 persons. Terrorist activities of the Liberation Army of Kosovo, the NATO bombing and the arrival of KFOR troops forced the non-Albanian population to leave the territory of Kosovo and Metohija.

Registration of displaced persons from Kosovo and Metohija that was carried out in 2020 showed that more than 200,000 of them were in Serbia (on 01/07/2012 there were 196140 refugees).[3]

The UNHCR's of June 2010 shows that Serbia, with 86,000 refugees and 21,000 internally displaced persons, is the first country in Europe in terms of forced migration, as well as one of the top five countries in the world with a prolonged refugee crisis.

We should note here that Serbia is affected with migrant crissis too. Serbia is fourth in the number of asylum seekers. On 12 November 2017, **4,262** new refugees, asylum-seekers and migrants were counted in Serbia, **of which 3,938 were accommodated in the 18 government centres** - representing 92% of the total caseload.[4] Including Kosovo, 21,200 Serbian citizens sought asylum, mostly in the EU. Only Afghanistan, China and Iraq are ahead of Serbia. By the end of October 2012, 5,833 migrants were accommodated in 17 centers managed by the Commissariat for Refugees and Migration, and it is estimated that there are another 1,069 outside the centers.

All citizens have the same rights and responsibilities and enjoy full national equality. The Constitution of the Republic of Serbia guarantees rights to national minorities in accordance with the highest international standards.

> According to Article 10 of the Constitution of the Republic of Serbia, Serbian language and Cyrillic script are in official use.[5] The Law on Official Use of Languages and Scripts equated the use of Latinic script, in areas of Serbia inhabited by national minorities in official use, in addition to Serbian language, are also languages and scripts of national minorities.[6]

[2] Statistical Office of the Republic of Serbia, stable Internet address http://popis2011.stat.rs/?page_id=1221.
[3] Statistical Office of the Republic of Serbia, stable Internet address http://popis2011.stat.rs/?page_id=1221.
[4] https://reliefweb.int/report/serbia/unhcr-serbia-update-6-12-november-2017.
[5] Constitution of the Republic of Serbia, Official gazette RS, no. 98/2006.
[6] The Law on the Official Use language and alphabet, Official gazette *RS*, No. 45/91, 53/93, 67/93,48/94, 101/2005 and 30/2010.

> The Constitution of the Republic of Serbia guarantees freedom of religion. Churches and religious communities are separate from the state and no religion can be established as state or obligatory religion. However, the population in Serbia is mainly Christian Orthodox. The Serbian Orthodox Church, autonomous since 1219, has played an important role in the development and preservation of Serbian national identity. Besides the Serbian Orthodox Church, there are other religious communities in Serbia: Islamic, Roman Catholic, Protestant, Jewish and others.

Serbia is one of the religiously most diverse European countries, with an Eastern Orthodox majority, and a Catholic and Islamic minority, among other smaller confessions.

Orthodox Christians number 6,079,396 or 84.5% of country's population. The Serbian Orthodox Church is the largest and traditional church of the country, adherents of which are overwhelmingly Serbs. Other Orthodox Christian communities in Serbia include Montenegrins, Romanians, Vlachs, Macedonians and Bulgarians.[7]

There are 356,957 Roman Catholics in Serbia, roughly 5% of the population, mostly in Vojvodina (especially its northern part) which is home to minority ethnic groups such as Hungarians, Croats, Bunjevci, as well as to some Slovaks and Czechs. rotestantism accounts for about 1% of the country's population, chiefly among Slovaks in Vojvodina as well as among Reformist Hungarians.[8]

Muslims, with 222,282 or 3% of population, form third largest religious group. Islam has a strong historic following in the southern regions of Serbia, primarily in southern Raška. Bosniaks are the largest Islamic community in Serbia; estimates are that some third of country's Roma people are Muslim.

Atheists numbered 80,053 or 1.1% of population and additional 4,070 are Agnostics.[9]

> The Republic of Serbia is administratively and territorially divided into provinces, regions, administrative districts, the City of Belgrade, cities and municipalities. Territorial organization of the Republic of Serbia consists of five regions (Belgrade Region, Vojvodina Region, Sumadija Western Serbia Region, Southern and Eastern Serbia Region and the Region of Kosovo and Metohija). These include the City of Belgrade as a separate territorial unit established by the Constitution and the law and 29 administrative areas, 23 cities, 28 urban municipalities, 150 municipalities, 6,158 villages and 195 urban neighborhoods. [10]

> Over 60% of population lives in cities. They are mainly concentrated around the capital – Belgrade, followed by Novi Sad, Nis, Pristina, Kragujevac. However, each year the number of abandoned villages is increasing. This is best illustrated by the fact that about 50 000 houses are constantly, and 145 000 temporarily unoccupied.

The political system of the Republic of Serbia is based on multi-party parliamentary democracy. Serbia has the National Assembly, the President of the Republic and the Government. The National Assembly is the highest representative body and the bearer of constitutional and legislative power in the Republic of Serbia; it consists of 250 deputies elected through direct elections. The President of the Republic represents national unity of the Republic of Serbia in country and abroad. The President is elected through direct elections, by secret ballot, for five years and can

[7] Statistical Office of the Republic of Serbia, stable Internet address http://popis2011.stat.rs/?page_id=1221.
[8] *Ibid.*
[9] *Ibid.*
[10] The Law on Territorial Organization of the Republic of Serbia, *Official Gazette RS,* nr 129/2007.

perform this function up to two terms. The president appoints the Prime Minister after considering the programme opinions of representatives of elected election lists. The Government has executive authority in the Republic of Serbia and consists of the Prime Minister, Deputy Prime Minister and Ministers. The Prime Minister is the head of Government.

Local government is organized on the principle of local self-government, through municipal or city assemblies, councils and government authorities.

In addition to dozens of political parties, there are hundreds of non-governmental organizations and a large number of unions.

The main principle of the Constitution of the Republic of Serbia (Article 1) is that the Republic of Serbia is a state of Serbian people and all citizens who live in it, based on the rule of law and social justice, principles of civil democracy, human and minority rights and freedoms, and commitment to European principles and values.

> Legislative power is defined in Article 4 of the Constitution of the Republic of Serbia, which says that the legal system is unique and that it is based on the division of power into legislative, executive and judiciary. The relation between three branches of power is based on balance and mutual control.

Judiciary power is independentand that power rests on a separation of powers into legislative, executive and judicial. The relationship between the three branches of government is based on checks and balances.

Legislative power belongs to the National Assembly, which is a unicameral legislature with 250 members. The National Assembly approves the Prime Minister and the Government. Deputies are elected to four-year terms.

> The judicial authority in Serbia is performed by courts of general jurisdiction (municipal courts, district courts, courts of appeal), the Supreme Cassation Court and specialized courts (commercial courts, the High Commercial Court, the Administrative Court).

> In the Republic of Serbia, there are the Autonomous Province of Vojvodina and the Autonomous Province of Kosovo and Metohija, as forms of territorial autonomy.

According to the census of 2012, Serbia had 7,186,862 residents (excluding the data from Kosovo and Metohija), of which 3,499,176 men and 3,687,686 women. The estimated number of inhabitants in the Republic of Serbia in 2020 is 6,899,126. Observed by gender, 51.3% are women (3,538,820), and 48.7% are men (3,360,306). The trend of depopulation has continued, which means that the population growth rate, compared to the previous year, is negative and amounts to -6.7 ‰.

Serbia has over 100 000 refugees currently living in shelters, camps, private households.

Average life expectancy is 71.6 years for men, and 76.8 years for women.

Serbia has a negative population growth rate (mortality rate is higher than the birth rate, and in Central Serbia emigration exceeds immigration).

The Republic of Serbia with an average age of its residents of 41.6 (2011), is one of the oldest countries in the world. The percentage of people over 65 will amount to at least 22% by 2030, which is nearly one in four residents. The main feature of age and gender structure of the population of the Republic of Serbia today is the numeri-

cal dominance of men among young population, i.e. the dominance of women among middle-aged and older persons. "The oldest" region is the Southern and Eastern Serbia Region, where 25% of the population is older than 60 years.

The current infant mortality rate for Serbia in 2021 is **4.469 deaths per 1000 live births**, a 3.12% decline from 2020. The infant mortality rate for Serbia in 2020 was 4.613 deaths per 1000 live births, a 3.01% decline from 2019.

Telecommunications infrastructure

Telecommunications in Serbia have a developed and efficient telephone network, and has a number of radio and television broadcast stations. The country code for Serbia is "SRB", the ccTLD is ".rs".

Serbia boasts an extensive broadcasting market, with programming available via radio and TV programme distribution via cable, wireless cable, terrestrial free-to-air and broadband TV. An analogue switch off (ASO) plan has been adopted and digital TV is widely available on cable networks.

Serbia's high mobile penetration, the result of multiple SIM card use, has seen lower revenue in recent years, placing further pressure on operators to develop business models, which encourage consumer use of mobile data services as also the continued substitution of fixed-line for mobile voice calls.

The telecommunication system of the Electric Power Industry of Serbia (EPS) consists of a network of fiber optic cables in main and regional plane, the transmission networks based on SDH technology and packet network based on IP/MPLS technology. In 2013, the network had 6 000 Optical Groud Wire (OPGW), All Dielectric Self-Supporting (ADSS) and inlet optic cables.

The most common way to access the Internet in Serbia in 2013 was the ADSL access with over 690 000 outlets, and it accounted for 47% of all broadband connections (excluding subscribers of 3G networks). In addition to the ADSL access technology, access to Internet could also be accomplished through a cable modem, which is just another service of cable television operator; directly, via Ethernet; via an optical cable; wirelessly in the frequency bands of 2.4 GHz and 5.8 GHz in free acces mode, also using the range 3.4-3.6 GHz, and through a network of mobile operator (through mobile-phone or special modems).

Telekom Serbia focused on network upgrades rather than privatization; Mundio Mobile and Globaltel licensed as MVNOs hosted on Vip Mobile's network; SBB given approval to acquire I.KOM; Telekom Serbia; Telenor Serbia and SBB launch joint multi-play service; regulator licences three MNOs for spectrum in the 800MHz band, stimulating LTE development; Telenor Serbia upgrades mobile network with carrier aggregation technology, begins transition to an all-IP architecture; report update includes the regulator's 2015 annual report, market report to December 2016, telcos' operating and financial data to Q1 2017, recent market developments.[11]

[11] For more information, please see stabile internet address https://www.budde.com.au/Research/Serbia-Telecoms-Mobile-Broadband-and-Digital-Media-Statistics-and-Analyses.

The Information and Communications Technology Market

Despite the global economic crisis, telecommunication market continues to grow. In gross domestic product of the Republic of Serbia, revenues from telecommunications in 2016, had a share of about 4.51%, while the total investment in the electronic communications sector in 2016 amounted to about 262,5 million euros, which is 4.9% lower than in 2015.[12]

Fixed Communications Market

According to the data of the Statistical Office of Serbia, percentage of households with fixed phone lines was 81.2% in 2016, and more then 90% housolds with LTE signal . The number of operators is increasing every year, so the number of license holders for public fixed telecommunications networks and services was 3 (Telekom Serbia, Orion Telekom, SBB). Pursuant to Art. 149 of the Law on Electronic Communications, since 1 January 2012 the provision of public fixed telecommunications network and services has been under the general authorization regime, hence, in addition to the above license holders, public voice service via fixed network was also provided by the following operators (as by the end of 2015): SBB, I.Kom, Radijus vector, Kopernikus technology, BeotelNet, Telemark systems, Masko, Invest-Inžinjering, ABA tel, Softnet, Sat Trakt, ASG net, BPP Ing, JP Pošta Srbije.[13] Up to 30 June 2016, the public telephone service over fixed-line network was provided by 24 registered operators. Approximately 2.5 million fixed telephony subscribers generated approximately 1.4 billion minutes of traffic.

The introduction of the service of number portability in fixed networks represents a step towards the full liberalization of the telecommunications market in the Republic of Serbia.

In 2016 investments in fixed-line services amounted to about 7.2 billion dinars.[14]

The distribution of traffic is nearly unchanged each year, and the share in total traffic (domestic and international) in 2016 was 52,9%, the share of traffic from fixed to mobile telephony decreased to 6,9% (in 2012 it was 10%), and the share of international traffic fis about 6,6% of the total traffic.[15]

The total number of users of VoIP operators at the end of 2016 was approximately 56,000, representing an decrease of 14,4% compared to 2015. About 14,4 million minutes of talk time was realized, and 48 million minutes of traffic in international transit was realized.[16]

[12] See Regulatory Agency for Electronic Communications and Postal Services RATEL, can be found at stable internet address: http://www.ratel.rs/upload/documents/Pregled_trzista/Pregled%20trzista_2016.pdf, p. 7-9.
[13] See http://www.ratel.rs/upload/documents/Pregled_trzista/RATEL_Annual_Report_2015_eng.pdf, p. 26.
[14] *Ibid*., at 41.
[15] *Ibid*., at 49.
[16] *Ibid*., at 60.

Mobile Communication Market

In the mobile market in the Republic of Serbia in 2016, three operators were present (Mobile Telephony of Serbia MTS, Telenor LLC, Vip Mobile). Licences are issued by RATEL for a period of 10 years, and after this period the validity of the license is extended to another 10 years without additional requirements, only with the fulfillment of the conditions.

The quarterly mobile telephony market indicators include the data submitted by all three operators, i.e. 100% of the market. 9 million active mobile telephony subscribers generated approximately 4 billion minutes of national and international voice traffic and sent approximately 2 billion messages at the quarterly average. As of the 2016 Q1, the number of postpaid subscribers exceeded the number of prepaid subscribers, displaying gradual growth in the given period. The postpaid subscribers are still primarily residential users, but their share is slowly decreasing in favor of business users.

Percentage of territory covered by GSM network is 90.73%, and the percentage of population covered by GSM network signal is 99.15%.[17]

In 2017, revenues obtained from mobile network service were 111.8 billion dinars, or 922 million euros, which is 0.1 % higher than in 2016.[18]

Interactive Services

In recent years, the Internet market in Serbia is constantly increasing. This statement primarily refers to the number and structure of the Internet connections, as well as the amount of total revenues from Internet services. This distribution of the number of Internet connections was quite expected, considering the growing amount of data exchanged over the Internet.

The total number of broadband connections in Serbia in 2017 amounted to nearly 6 million including also 233 000 M2M subsribers.[19]

Data transmission over mobile network showed growth in the analyzed period, amounting to approximately 22.7 million GB in Q3 2017, which means that a mobile Internet user spent on average 42MB or approximately 1.2 GB a month. The majority of fixed broadband subscribers have xDSL or cable access. The number of xDSL subscribers showed a slight drop and the cable access a slight rise in 2017.

E-Commerce: Facts and Figures

Supporting electronic payment (e-payment) is a necessary condition for closing the trading process in E commerce. A set of technological and institutional requirements has to be met for e-payment to function smoothly. The institutional push for

[17] See RATEL at 5.

[18] *https://www.ratel.rs/uploads/documents/empire_plugin/5bd194d2428d3.pdf.*

[19] https://www.ratel.rs/upload/documents/Pregled_trzista/Q3%202017%20ENG.pdf.

advancing e-payment and E-banking in Serbia was marked by the Law on Payment Operations introduced on January 1, 2003. All payment operations were transferred from the Accounting and Payments Operations Office to commercial banks, and all payment transactions were completely overtaken by the banks. The reform of the payment system opened a new segment of commerce and urged the banks to compete for clients. The payment-card market has shown the fastest growth in the region.[20]

A "chip card" center was established in 2004 and it renders the services of payment-card issuing, authorization, connecting to POS terminals and ATMs, and home and foreign card processing. Both the banks and the government work on promoting payment cards.

The government's support to advancing the e-payment strategy is particularly evident in the National Dina Card Program. This program involves different types of debit and credit cards. Moreover, the central bank has financed the establishment of Switching Centre that works as part of the Central Bank. The Centre enables connections among 500 ATMs in the DinaCard system as well as among 20,000 POS terminals installed in stores and shops.

The legislative layer of E commerce is just developing in Serbia, influenced by the corresponding EU legislature, international standards, certain regional initiatives Serbia has endorsed, and Serbia's legal tradition. Challenges refer to the validity of documents produced and exchanged electronically, security of transactions, and trust, copyright and ownership issues in trade using a website. The Criminal Code has been amended in accordance with the basic recommendations of the Council of Europe. It now covers software piracy, unauthorized use of computers and computer networks, computer sabotage, creation and spreading of computer viruses, computer fraud, disruption of electronic data processing and transmission, unauthorized access to a protected computer or computer network, and protection against unauthorized limits to the access of public computer networks. Changes have also been made in the intellectual property legislature, inclusive of software products. New laws exhibit a basic compliance with international regulations. Digital signature is regulated by a law adopted in late 2004. This law is in line with common practices and regulations in the EU and the US. However, no systemic approach has been taken toward local electronic payments yet. Business players rely on the National Bank Ordinance on Electronic Payments and the Law on Payment Operations. While issuing payment cards, local banks rely on the Law on Banks and Other Financial Organizations, international standards, and available experience.

The e-commerce industry in Serbia has shown some fantastic results as it grew 39% to 8.16 billion dinars or 70.4 million euros in 2013. A downside to the story may be the fact the lion's share of all transactions went to non-Serbian online stores, as its inhabitants shop drastically more abroad than at local stores. Of the total number of 1.7 million transactions, 1.45 million took place on foreign websites. To be more precise, the National Bank of Serbia (NBS) recorded 1,641,491 domestic payments with credit cards and in dinars, euro's dollars, Swiss francs or British pounds. If the number of transactions in other currencies is added, there were 1,681,850 transactions last year.

[20] See Emilija Vuksanović, „The role of bankcard industry in transition of Yugoslav Economy", *Proceedings of theInternational Conference ICES 2002. Sarajevo, Bosnia-Herzegovina, October 17-18, 2002*, pp. 767-775.

About 190,000 transactions happened between Serbian consumers and Serbian online stores, which together realized a turnover of only 8.8 million euros. The average transaction at a domestic online store was €47,47, while the average transaction value at foreign online stores was about €42,70.

Revenue in the eCommerce market amounts in Serbia to US$319m in 2018. Revenue is expected to show an annual growth rate (CAGR 2018-2022) of 10.8%, resulting in a market volume of US$480m by 2022. The market's largest segment is Electronics & Media with a market volume of US$148m in 2018. User penetration is 56.3% in 2018 and is expected to hit 61.5% by 2022. The average revenue per user (ARPU) currently amounts to US$79.73.[21]

E-Government Initiatives

In the Republic of Serbia, regulations related to development of information society can be categorized in two groups: regulations adopted by the year 2001, and regulations adopted in the period 2003.-2005.[22]

In the Republic of Serbia, operations of government administration and tasks in the area of information society development are under jurisdiction of Ministry of Telecommunications and Information Society (jurisdiction taken over from the Ministry of Science and Environment Protection in former government), National Information Technology and Internet Agency, and Office for Common Operations of Government Institutions.

Serbia is far away from EU average on online sophistication. The full enforcement of Law on Electronic Signature could significantly improve this result without bigger technological change in short period.[23]

A new law on Public Administrative Procedures was adopted as of March 9th, 2016 that promises to make citizens' services much smoother as data currently residing within a government office is not supposed to be requested for a second time by another government office. As of March 16th 2016, on portal http://www.euprava.gov.rs/eusluge/usluge_po_slovu there were 635 different e-services available in total, out of which 441 services for citizens, 181 for businesses, 13 for state authorities.

The Government of the Republic of Serbia adopted the Strategy for e-Government Development of the Republic of Serbia by 2018. Through the adoption of the Strategy for e-Government Development, citizens of Serbia will gain a more efficient, transparent government, providing for a one-stop shop system at the National e-Government Portal, in order to stop wasting time and money in the bureaucratic system. Likewise, the implementation of the Strategy will provide savings at all levels, primarily through the swift resolution of requests by citizens and businesses, the optimization of public administration and significant savings on costs due to red tape.

[21] https://www.statista.com/topics/2802/serbia/.

[22] National Information Technology and Internet Agency, *Analysis of legislative framework for e-Government in Serbia*, 2006.

[23] Darko Spasić, *Digital certificate as digital identity of Internet users*, Serbian Post Company, 2006.

PART I

REGULATION
OF THE ICT MARKET

REGULATORY FRAMEWORK OF THE TELECOMMUNICATIONS SECTOR

Background

The law of Electronic communication (LEC) was adopted after several public discussions and after a great need for regulating this field in 2010[1]. The main reason for such a long time not to have this kind of law in Serbia was ignorance of new conditions in telecommunications for their existence. New market conditions and new climate for market was the sole reason for emergence of such kind of laws in Europe and that was a beginning of new era. This great need has come from pressure created by foreign influences and very vivid nature of electronic communications. This need is also born from different perspectives of business and public authorities, and their essential urges for regulation in this area of life. Maybe this conjunction of factors has to be blamed for its differences with real life needs. Nevertheless, this law was a target of initiative for constitutional check and review of Constitutional court of Serbia and in 2013 there has been Constitutional Court decision published in Official gazette no. 60/2013, also this law was changed published in Official gazette no. 62/2014.

This law is not regulating areas of electronic communication networks for special purposes, except those articles which determine using radio-electronic frequencies for special purposes and special cases of interconnection of electronic communication networks for special purposes and public communication networks.

Scope of the law

Law of electronic communication (LEC), as it is strictly underlined in article 1. (which is determining scope of the law) are arranging: terms and methods of commercial and other activities in area of electronic communications; jurisdictions of state agencies and institutions in area of Electronic communications (EC); role and powers of Republic agency for electronic communications – RAEC; administrative charges; management and execution of public consultations in area of EC; General Authorization of Electronic Communications Networks and Services and providing services under general Provision of Services; Projection, construction or establishment, usage and maintenance of EC networks, additional means and devices, electronic communication equipment and terminal equipment; right of way and communal usage; interconnection and access; Provision of universal services; determination of markets eligible to prior regulation, analysis of market, determination of operator with considerable market power (OCMP) and powers of RAEC in relation to OCMP; management and usage of addresses and numbering (in further text numbering); management

[1] Official gazette of Republic of Serbia no. 44/2010, 60/2013 – Constitutional Court decision and no. 62/2014.

usage and control of Radio-Electric Spectrum; distribution and emitting of media content; protection of rights of users and subscribers; security and integrity of electronic communication networks and services; privacy of electronic communication, lawful interception and retention of data; supervising implementation of LEC; measures for those acting against this law, and also of other issues of significance on functioning and development of electronic communication in Republic of Serbia.[2]

- Article 4 provides the meaning of certain terms and according to it particular terms used in this law have the following meanings:
- The activity of the electronic communication (defined in point no. 4.) includes the construction or installation, maintenance, use and administration of the use of public communication networks and related resources, as well as the provision of publicly available electronic communication services;
- Electronic communication network is defined (point 7) as: transmission systems and, where it is applied, devices for switching and directing, as well other resources, including passive network elements that enable the transmission of signals using wired, radio, optical or other electromagnetic means, including satellite networks, fixed (commutation circuits and packages, including Internet) and mobile networks, power cable systems, in the part that is used for the transmission of signals, networks used for the distribution and broadcast media, regardless of the type of data and information to be transmitted;
- Electronic communications service is (defined in point no.10) a service that is regularly provided for a fee, and consists wholly or mainly of signal transmission in electronic communications networks, including telecommunications services and services of distribution and broadcasting media, but does not include services providing media content or performance of editorial control over media content transmitted using electronic communications networks and services, or involves services of the information society, which is not consisted, wholly or mostly, of signal transmission by electronic communication networks;
- The Internet is (defined in point no.15) a global electronic communication system composed of many interconnected computer networks and devices that exchange information using a common set of communication protocols;
- Public communications network is (defined in no.18) an electronic communications network that, in its entirety or mainly, is used for the provision of publicly available electronic communication services and enables data transmission between terminal points of the network;

Policy objectives and regulatory principles

The core objectives and principles regulating relations in the field of electronic communications are based on (Article 3) and main of those could be listed as:

- Provision of: conditions for the leverage development of electronic communications to the entire territory of the Republic of Serbia; business predictabili-

[2] Mina Zirojević, Zvonimir Ivanović, *Zaštita prava intelektualne svojine u sektoru informaciono – komunikacionih tehnologija*, Institut za uporedno pravo, Belgrade, 2016

ty and equal conditions for business operators; harmonization of activities in according with appropriate standards; accessibility to universal services with meeting the needs of specific social groups (including persons with disabilities, elderly and socially disadvantaged users); interconnection of electronic communications networks and services, and operators under equal and mutually agreed terms; encourage competition, efficiency and effectiveness in carrying out the activities of electronic communications; ensuring a high level of protection of consumers' interests in relation to the operators, in particular by providing access to clear and complete information on prices, conditions of access and use (including limitations) and the quality of public communications networks and services, as well as an efficient treatment of complaints on the work of the operator; improvement in the quality of services of electronic communications; high level of protection of personal data and privacy of the user, in accordance with the Law on the Protection of Personal Data and other laws;

National regulatory authorities

LEC delivers (in article 5.) the specific competencies of the Government agencies and ministries. In this area, competences are proscribed for Government, Ministry responsible for telecommunications and information society, Regulatory Agency for Electronic Communications and Postal Services.

The Government, on the proposal of the ministry responsible for telecommunications and information society (hereinafter: the Ministry): determines policy in the area of electronic communications; creates strategic documents and action plans for their implementation, defining the principles, objectives and priorities for the development of electronic communications in the Republic of Serbia and decides on other matters when provided by this law[3]. This is at strategic level. Ministry is actually state agency in charge of administrative monitoring of the Agency.

The Ministry, in accordance with the law, according to Article 6 (at tactical level): supervises the implementation of LEC and the regulations made thereunder; represents the Republic of Serbia in international organizations and institutions in the area of electronic communications and ensure the implementation of international agreements in that area; contributes to the harmonization of national legislation in the area of electronic communications with relevant regulations of the European Union; takes measures to encourage investment in the area of electronic communications and the use of information and communication technologies; take measures to encourage research and development in the field of electronic communications, in cooperation with the ministry responsible for development and promotion of scientific research**.** Also, Ministry is to decide on other matters when provided by law (like in administrative actions).

Regulatory Agency for Electronic Communications and Postal Services (hereinafter: the Agency), established by the LEC, is an independent regulatory organization as a legal entity. It is vested with public authority for the purpose of effective implementation of established policy in the area of electronic communications, encouraging competition of electronic communication networks and services, improving their capacity

[3] In preparing defined regulations, at first two shall participate competent authorities of the autonomous regions.

or quality, contributing to the development of electronic communications markets and to protect the interests of users of electronic communications, in accordance with the provisions LEC and regulations adopted thereunder, as well as regulatory and other tasks in accordance with a special law regulating the postal services. So those powers lie in the area of tactical and operational activities in the field.

Relations between Government, Ministry and The Agency are very strictly determined. The Agency is functionally and financially independent from the state authorities, as well as persons and organizations performing activities of electronic communications and postal services. It operates in accordance with the regulations of public agencies. Supervision over the legality and purposefulness of the Agency in carrying out entrusted tasks is performed by the Ministry. The Agency may, professional activities within its jurisdiction, engage other domestic or foreign legal entities and individuals. Mode and the internal arrangements of the Agency shall be governed by the statute, which provides the board of directors of the Agency. The government gives its consent to the Agency's Statute.

The Agency, in accordance with the law (Art. 8) adopts bylaws. It decides on the rights and obligations of operators and users, cooperates with the competent authorities and organizations in the area of broadcasting, competition protection, consumer protection, protection of personal data and other bodies and organizations on issues significant for the area of electronic communications. It cooperates with the relevant regulatory and professional bodies of the Member States of the European Union and other countries to harmonize the practice of enforcing regulations in the area of electronic communications and to encourage the development of cross-border electronic communications networks and services. Agency participates in the work of international organizations and institutions in the field of electronic communications as the national regulatory authorities in the field of electronic communications. It also, performs regulatory and other tasks in the field of postal services in accordance with a special law regulating the postal services and performs tasks in accordance with LEC.

Organization of regulatory authority

Agency performs impartially and publicly described Affairs as entrusted tasks. The bodies of the Agency, according to the law, are Management Board and Director. The Management Board shall consist of five members, of whom one is the chairperson and one vice president. The chairperson, deputy chairperson and members of the board are appointed and removed by the National Assembly at the proposal of the Government, based on a public competition, in accordance with the provisions of LEC. The mandate of the board member is for five years. The same person may be elected as a board member maximum for two mandates.

The Management Board shall, in accordance with the law:

1) Adopt the Agency's annual work plan, aligned with the strategic acts and action plans in the area of electronic communications and postal services, no later than 15 December of the current year for the following year;

2) Issue other acts prescribed by LEC or a special law regulating the postal services;

3) Perform tasks set by a special law regulating the postal services;

4) Perform other tasks that law or statute of the Agency did not put in the competence of the Director.

The Management Board (MB) shall decide by a majority vote of all members, except in cases where the law or the statute of the Agency specified otherwise. MB adopts the statutes of the Agency by two-thirds majority of members. The chairperson of the MB manages the work of the Board and performs other duties stipulated in LEC and the Statute of the Agency. The MB shall adopt its rules of procedure. Members of the board are entitled to compensation for their work on the board, which is determined in accordance with the Statute of the Agency, with the consent of the Government.

Criteria for the selection of members of the Board are set out in Art.13. Members of the Board shall be elected from the ranks of distinguished experts with high academic qualifications in the area relevant to the work of the Agency, particularly in the field of electronic communications, economics and law, who have made a significant and recognized work or practice in the areas of electronic communications and postal services, and who enjoy a reputation in professional circles. Three members of the board must be experts in the field of electronic communications, and one board member must be an expert in the field of postal services.

The budgetary fund for the promotion and development of the area of electronic communications and information society are defined by the newly introduced Article 27a. The budgetary fund for the promotion and development of the field of electronic communications and information society (hereinafter: Budget Fund) shall be established to record funds provided by Art. 27, paragraph 6, which are to be paid to the appropriate account prescribed for payment of public revenues of the budget of the Republic of Serbia. Budgetary fund is established for an indefinite period, in accordance with the law governing the budgetary system. Budgetary funds are managed by the Ministry. Funds to finance the budget funds are provided:

1) From the funds referred to in Article 27, paragraph 6 shall be paid into the appropriate account prescribed for payment of public revenues of the budget of the Republic of Serbia;

2) Donations.

The Ministry will adopt the annual plan of using the means of budget funds for financing activities and measures of improvement and development of the field of electronic communications and information society in line with the development strategies in the area of electronic communications and information society, other laws and regulations in these areas, contracts, and international treaties signed by the Republic of Serbia. The autonomous province may establish a fund budget to be funded from part of the Article 27, paragraph 6 shall be paid into the account of the budget of the autonomous region, in which case they are in this budget fund pursuant to the provisions of paragraphs. 1 - 5 of this Article.

Provision of Electronic Communications: Requirements and Conditions

General Authorization of Electronic Communications Networks and Services

Chapter VI is titled "the performance of electronic communication by the general authorization regime" and by it, first it is determined: the general conditions for conducting activities. Electronic communications are carried out by the general authorization regime, and in accordance with the general terms and conditions as may be prescribed for all or certain types of electronic communications networks and services, in accordance with the provisions of the LEC.

General conditions relating to usage conditions are:

1) Notification to the Agency of the start, change and termination of electronic communications networks or services, as well as providing other data and information in accordance with the provisions of the LEC;

2) Payment of fees established in accordance with the LEC;

3) The construction or installation, use and maintenance, as well as the common use of electronic communications networks and associated facilities, in accordance with the provisions of the LEC, the special law governing the planning and construction, the regulations governing environmental protection, as well area protection of cultural heritage;

4) Control of population exposure to electromagnetic fields caused by the operation of electronic communications networks, associated facilities and electronic communications equipment, in accordance with the regulations governing the protection of the environment;

5) Ensuring compliance with the prescribed technical and other requirements;

6) The obligation of the operator in relation to interconnection, access and ensuring interoperability of networks and services;

7) Providing communication between emergency services, authorities, and organizations, as well as to inform the public in the event of natural disasters and catastrophes;

8) Participation in the financing of the universal service, the amount determined by the Agency in accordance with this Law;

9) Ensuring the availability of numbering to end users in accordance with the provisions of the LEC;

10) Providing services using radio frequencies by the general authorization regime;

11) Transferring media content of public interest, in accordance with the provisions of LEC;

12) Protecting the rights of consumers in the field of electronic communication in accordance with the provisions of LEC, and the requirements in terms of ensuring the accessibility of universal services for people with disabilities;

13) Ensuring the availability of clear and complete information about prices, conditions of access and use (including limitations) and the quality of public communications networks and services;

14) Protecting personal data and privacy in the electronic communications sector, in accordance with the provisions of LEC and the law governing the protection of personal data;

15) Implementing of measures to prevent and combat abuse and fraud in connection with the use of electronic communications networks and services;

16) Implementing of measures to maintain the security and integrity of public communications networks and prevent electromagnetic interference between electronic communications networks and services;

17) Facilitating the exercise of lawful interception of electronic communications and access to stored data.

The Agency shall prescribe the above conditions, and impose requirements that apply to all or some of electronic communications in the general authorization regime, depending on the electronic communications networks or services to which they relate, being careful in that to be justified, sufficiently specific, proportionate and non-discriminatory.

Rights and obligations attached to the general authorization

Establishing of Rights and Obligations

As mentioned before, the operator shall, at least 15 days before commencement, change or termination of the provision of an electronic communications network or service, inform the Agency of this in writing. The notice must contain:

1) Name, or the title of the operator, identification number and tax identification number, address or headquarters, as well as the contact details of responsible persons;

2) A brief description of electronic communications networks and services to which the notice relates;

3) Projected start date, changes or termination of activities.

Announcement submitted on the form of which shall be prescribed by the Agency. The Agency shall keep updated records of public communications networks and services (hereinafter referred to as records of operators) and should make it available on its website. The Agency shall issue a certificate of registration in the records of operators within seven days of receipt of the notice, and at the request of the operator. Registration in the registry operator is not required for the commencement of operations and the rights and obligations of operators in the general authorization regime under LEC. The Agency clears the operator from the register of operators:

1) If the operator in writing notifies the Agency of the termination of the activity, the date of cessation of service as specified in the notice;

2) If the operator fails to perform electronic communications for more than six consecutive months;

3) If the operator has court prohibited performance of electronic communication by a final judgment.

The basic rights of operators by the general authorization regime are defined by Article 39 of the LEC. The operator, in accordance with the law, has the right to:

1) provide electronic communications

2) request the right of way over someone else's property or the right to use someone else's property (easement);

3) negotiate and agree on interconnection and access to other domestic and foreign operators;

4) be designated for service of all or some of the universal service, on the whole or part of the territory of the Republic of Serbia.

Operator shall, upon request of the Agency, submit all the necessary data and information necessary to perform the tasks of the Agency, in particular the data and information relevant to:

1) control of the operator`s treatment in accordance with the prescribed general conditions for the performance of electronic communication, certain specific obligations on operators with OCMP, the conditions set conditions for the use of numbering, individual licenses for use of radio frequencies, as well as other obligations stipulated in the LEC and the regulations adopted thereunder;

2) Respond to requests for shared use, interconnection and access, as well as maintaining a database of facilities that may be subject to claims for common use or access;

3) Analysing the market in accordance with the provisions of this Act;

4) Assessing the impact of the development of new networks and services in the preservation of competition in the electronic communications sector;

5) Ensuring effective management and rational use of numbering and radio frequency spectrum, as well as keeping the database on the use of numbering and radio-frequency spectrum;

6) Publication of comparative examination and maintaining a database of prices, terms and conditions for access and use (including limitations), and the quality of public communications networks and services;

7) Mediation in resolving disputes between subscribers and operators;

8) Ensuring the protection of personal data and the privacy of users, as well as assessing the security and integrity of electronic communications networks and services, including security policy, ensuring the continuity of work and data protection;

9) Collection and publication of statistical data.

Each request issued by the Agency to an operator shall contain the legal basis, scope and objective requirements, the level of detail requested information and appropriate deadline for compliance with the request. Period may not be shorter than 15 days from the date of receipt of the request by the operator, unless otherwise provided by law. Members of the Board, Director of the Agency, the Agency employees, as well as other legal and natural persons engaged by the Agency to perform certain tasks, are obliged to maintain the confidentiality of the collected data and information, which are

marked with a certain degree of confidentiality in accordance with the law governing the confidentiality of data, or that are designated as trade secret act of the originator or by contract, in accordance with the law. Those people are obliged to maintain the confidentiality of the collected data and information, regardless of the manner in which they have learned them, during and after the termination of service, employment or contractual relationship, until the expiration of the period for which the data were collected and for which the information was indicated for some degree of secrecy or until the decision of the data owner on removing the obligation of secrecy.

The data and information that is publicly available, which is published on the basis of LEC, other regulations or decisions of the originator, or the public's right to know in accordance with the law governing access to information of public interest, aren't to be considered confidential, or trade secrets in this article.

Rights of way and communal use

Title VIII. LEC regulates the right of way and common use. Law is defining the public interest for expropriation in Article 49 for the construction and installation of electronic communications networks. It is prescribed that for the associated facilities, also, may be determined the public interest for expropriation in accordance with the law governing expropriation. The right of way is defined in Article 50; the operator has the right to demand a right of way over someone else's property or the right to use someone else's property, when it is necessary for the construction or installation of electronic communications networks and associated facilities.

Operator and owner, holder of the right to dispose of or use of property, conclude a contract which shall specify the manner of exercising the servitude, as well as the existence and amount of remuneration for the establishment of servitude. If such persons fail to reach agreement on the right of easement, then the easement shall be regulated in accordance with the law. Once the easement is based on the property in public ownership, unless the law on governing public property hasn't otherwise provided, the public authority shall decide on the conclusion of the contract, and those shall be the conditions for acquiring easements designated on a non-discriminatory manner and publicly announced, and that decision on the signing of the contract should be taken without delay, but no later than 30 days from the date of application for the conclusion of the contract.

Joint use is treated in Article 51. The operator has the right to request joint use (including physical collocation) network elements and associated facilities of another operator or a third party, as well as property whose use is another operator's or a third party's relied upon the right of easement or property that is acquired by expropriation, when it is necessary for a competitive, cost-effective and efficient performance of electronic communications, or when new electronic communications network and associated resources can't be built or installed without harmful effects on the environment, public safety, the implementation of spatial plans and preservation of cultural heritage. The operator concludes a contract with another operator or a third party, the holder of disposal right or use of the network elements, related assets and other property, which closely regulates the mutual rights and obligations in terms of common use, including cost allocation, taking into account previous investments, encouraging further investment and the possibility of return on investment at a reasonable rate considering the associated risks.

If this agreement is not concluded within 60 days from the application date, the Agency is authorized, when statutory requirements are met (previously described), at the request of an interested party or ex officio, to issue a decision to establish mutual use, including cost allocation, taking into account the previous investments, encouragement of further investment and the possibility of investment return at a reasonable rate considering the associated risks.

Databases of Capacities and monitoring

In order to fully control and supervise such resources, as well as to establish transparency, the law establishes a database of facilities that may be subject to joint use and access. The Agency shall keep an updated database on the type, availability and geographical location of assets, particularly information about routes and capacity of electronic communications networks. The Agency shall specify the collection and publication of information regarding this database. It publishes and updates the information on its website[4] with a comprehensive search capability.

Access and Interconnection

Chapter IX defines the interconnection and access. The operator shall be entitled, in accordance with the provisions of LEC, to achieve interconnection with another operator, as well to access network elements and associated facilities of another operator, to provide electronic communication services to end-users. The operator who receives a request for interconnection or access is obliged to enter into negotiations on the terms of interconnection or access to, with the operator who submitted the request. An operator with OCMP shall offer interconnection to other operators and access in accordance with the provisions of LEC and the decision of the Agency, which is designated as an operator with OCMP. Technical and commercial terms of interconnection and access, at the national and international levels, are regulated by an agreement between operators. Operators are required to submit, within 30 days from the date of signing, the application to the Agency about contract for interconnection at the international level. The Agency maintains a register of interconnection agreements at the international level. The operator is required to maintain the confidentiality of information obtained before, during or after the negotiation or conclusion of the interconnection or access to, and use them only for the purposes for which they were given. If the operators of electronic communications do not reach an agreement in relation to interconnection and access, within 60 days of the start of the negotiations, and when necessary to protect the interests of end-users and ensure the interoperability of electronic communications networks and services, the Agency, at the request of interested parties or ex officio, shall adopt a decision establishing the interconnection or access, including technical and commercial requirements. The Agency will regulate the content and method of application interconnection agreements at the international level.

Special cases of interconnection of electronic communications networks for specific purposes and public communication networks thoroughly are regulated by Article.

[4] http://www.ratel.rs accessible on 15.02.2018.

The Agency, at the request of the defence, security and emergency services, may bind the operators by the decision, in the framework of existing technical capabilities, to primarily provide interconnection with electronic communications network for the specific purposes for a period not longer than 14 days, in the case where in a certain area electronic communication network is lacking the capacity for a particular purpose, or where, for reasons of urgency or unpredictability has not been possible to predict and implement timely and necessary interconnecting for the purpose of the statutory tasks of the defence, security and emergency services (e.g. visit to ensure foreign leaders, sporting events and public meetings, action in cases of major accidents, fires and accidents, emergency response in case of terrorist attacks, military exercises and the like). By this decision the requirements and fees for interconnection are determined.

Numbering

Chapter XII of the LEC deals with the matter of numbering. Management of numbering and the definition of the numbering plan are stipulated in Article 72. Management and assignment of addresses and numbers, as a limited good, are done in a way that ensures their rational, equitable and effective use, in accordance with the numbering plan.

National numbering plans

The numbering plan defines the purpose of the addresses and numbers, provides equal access to numbering for all publicly available electronic communication services or for all operators who provide these services, provides conditions for number portability, carrier pre-selection and introduction of new electronic communication services, as well as meeting the obligations under the relevant international agreements. The Agency proscribes numbering plan and makes it published it on its website.

Numbering management and allocation

The right to use the numbering is acquired on the basis of a license for the use of numbering (Art. 73), which is issued by a decision of Agency, based on operator`s request. The request shall contain the following information:

1) the identity of the applicant;

2) the nature of electronic communication networks or services which require allocation of numbering;

3) The numbering for required assignment;

4) The need and purpose of use of numbering;

5) The planned time of use of numbering;

6) The period for which is allocation of numbering required.

The request shall be submitted on the form of which shall be prescribed by the Agency. Deciding upon requests shall be made in the order of filing, within 20 days from the date of the request, unless the relevant international agreements are provided for a different term. The request may be denied if it is not in accordance with the numbering plan or if the requested numbering is not available.

Decision (article. 74) by which is issued permit for the use of numbering contains information on:

1) the license holder;

2) granted numbering;

3) the period for which the assigned numbering;

4) the period within which the holder must start using assigned numbering;

5) the purpose for which it was granted the right to use numbering;

6) the method of ensuring the efficient and rational use of numbering, including the method of keeping records for the used numbering and informing the Agency about the degree of utilization;

7) specific obligations in connection with the use of assigned numbering, arising from the relevant international agreements.

The Decision may contain other data, if such data are in connection with the prescribed conditions for issuing permits or arising from relevant international agreements. Licensee for the use of numbering is required to notify the Agency of changes to the information on the license holder within 30 days of such change.

Duration and renewal of a license for the use of numbering is defined by Article 75. The license for the use of numbering shall be issued for a period not to exceed ten years. Permission for the use of numbering can be extended under the same conditions as for a new license for a period of no longer than the period for which it can issue new licenses. Licensee for the use of numbering has to fill an application for extension of licence within a period neither less than 30 days nor more than 90 days before the expiration of the license.

Licensee for the use of numbering can lease assigned numbering for the use of a third party (art.76), which intends to use ceded numbering for commercial purposes, and not for their own use, on the basis of contract made in writing, on which previously was given consent by the Agency. The provision does not apply to the numbering by operators licensed for use to its subscribers, as well as to subscriber numbers which were transferred to other operators in accordance with the provisions of this law on number portability. In the event of a status change of holder for the use of numbering, which occurs in accordance with the law governing the legal status of companies, transfer of right to use the assigned numbering can be made only on the basis of documents drawn up in writing, which the agency previously approved. Data on the approval of the Agency shall publish on its Web site.

Seizure of the assigned numbering is stipulated in Article 77. The Agency shall decide on the confiscation assigned numbering if it finds that:

1) a license for the use of numbering issued based on incorrect data or faulty documentation relevant to decision making;

2) assigned numbering is not used in accordance with the numbering plan or a permit issued for the use of numbering;

3) The holder of a license for the use of numbering, even after receiving the notice, it is not within the specified period paid a fee for the use of numbering;

4) the holder of a license for the use of numbering is prohibited the performance of electronic communication in accordance with LEC or by a final court judgment;

5) the holder of a license for the use of numbering in writing waived his right to use the assigned numbering;

6) the holder of a license for the use of numbering ceased to exist, without a legal successor;

7) the holder of a license for the use of numbering did not eliminate irregularities found during inspection;

8) the seizure of assigned numbering is necessary to comply with the amendments to the Numbering Plan, made in order to implement relevant international agreements or the public interest that could not be met otherwise.

Licensee for the use of numbering, where the numbering revoked for the reasons set point 8), has the right to substitute numbering. Agency assigns a new numbering at the request of the person, taking into account proportionality, protection of the public interest and economic consequences of replacing the numbering.

The Agency shall keep up to date database of numbers (art.78.) which specifically includes information on allocated numbering, with corresponding data on the conditions of the grant and use, the geographic scope of their use, as well as operators which is numbering assigned. Agency publishes and updates the information on its website with a comprehensive search capability.

Number Portability

Number portability is proscribed by Article 79. The operator of publicly available telephone services (operator provider of number) is obliged to provide its subscribers, upon request, while changing the operator (operator receiver of number), possibility to keep the assigned number in the numbering plan in a particular location, to which the applicable geographic access code, or in any location, if the access code is not geographically assigned. Request to transfer the subscriber shall submit to the operator receiver of number. When such a request is submitted it shall be considered a request for termination of the contract between the subscriber and operator provider of number on the use of services in relation to the number that is the subject of the transfer, and the contract will be terminated as of the moment the number of exclusions from the network operator's provider number. Subscriber shall, upon submission of the request, submit particular information about their identity to the operator receiver of number, the number which is transferred and the statement by which he or she commits to the donor operator to settle all obligations under the contract resulting from the moment the number was excluded from the donor network operator, under the threat of a temporary or permanent suspension of service provision by

the operator of the recipient number. Operator receiver of number pays a fee for the transfer of the number to operator provider. The Agency manages information system for number portability and maintains a database of ported numbers, taking into account the protection of personal data, and it shall prescribe the terms and manner of number portability, as well as fees for transferring the number from this article. For operations management information system for porting and maintaining a database of ported numbers, the Agency may engage any other legal entity. Operator provider of the number and the operator receiver of number are required to achieve mutual cooperation as well as cooperation with the Agency, in the process of number porting, to ensure that the duration of the interruption of service to the subscriber during the transfer does not exceed one working day, and to refrain from actions aimed at hindering or preventing the transfer number.

Operator of publicly available telephone services shall enable to all users to establish free calls to a single number for emergency services – 112 and other numbers for access to emergency services in the Republic of Serbia (Art.80), according to the numbering plan, from any telephone, including the public telephone booths. The operator is obliged to centre to service calls to emergency services free of charge, forward all available information about the calls to the number 112 and other numbers for access to emergency services, especially information about the identity of the calling party, the calling number, time and duration calls, as well as information about the location from which the call was made, in accordance with the technical possibilities.

Radio Spectrum

Introduction

Article 43 of the LEC relates to compatibility. Electronic communications networks, associated facilities, electronic communication equipment and terminal equipment must not cause impermissible electromagnetic interference, which may adversely affect the operation of other electronic and other equipment and facilities in their vicinity. They also must have adequate immunity to electromagnetic interference, so that in their presence they also have function continuance without unauthorized degradation of its characteristics. The Ministry, at the proposal of the Agency, shall prescribe the requirements for ensuring electromagnetic compatibility.

The Agency measures the levels of the electromagnetic fields of electronic communications networks, associated facilities, electronic communication equipment and terminal equipment, in accordance with the limits prescribed by the regulations. The Agency shall report to the competent inspection established exceeding during these measurements.

Chapter XIII regulates the radio frequency spectrum. Management of radio frequency spectrum, particularly management principles are defined in Article 81.

Management of the Radio-Electric Public Domain

Management of radio frequency spectrum, as a limited good, is based on the principles of rationality, efficiency, transparency and non-discrimination, and includes in particular:

1) Planning the use of radio frequencies in accordance with relevant international agreements and recommendations, the interests of the citizens, economy, security and defence;

2) The allocation of radio frequencies on the basis of land use plans and the distribution plan;

3) Coordinated use of radio frequencies;

4) Control of radio-frequency spectrum, determining harmful interference, and measures for their elimination.

The Agency manages the radio-frequency spectrum and coordinates satellite orbit use in accordance with relevant international agreements, and in accordance with the provisions of this LEC and the regulations promulgated thereunder. The Agency shall cooperate with international organizations and the administrations of other countries that perform the tasks of managing the radio frequency spectrum, either independently or through the competent authorities.

Coordination of the use and application of providing radio frequencies are defined in Article 82. Radio frequencies designed for use in certain border areas, before assigning, are coordinated with neighbouring countries, with which Serbia has separate agreements on the coordination of the use of radio frequencies. Radio frequenciesof certain radio frequency bands, if necessary, prior to the assigning, are coordinated with neighbouring countries and other interested countries. Assigning of radio frequencies is subdued to application of the International Telecommunication Union Radio Regulations, in particular:

1) when the use of radio frequencies may cause harmful interference to radio communications services of another country;

2) if the radio frequencies are intended for international radio-communications;

3) to protect the radio frequencies at the international level.

Rights of use of the radio spectrum

General principles

Chapter VII LEC is dealing with electronic communications networks, associated facilities, electronic communication equipment and terminal equipment. Design, construction or installation, use and maintenance of electronic communications networks and associated facilities is treated in Article 24. Electronic communications networks and associated facilities shall be designed, constructed or installed, used and maintained:

1) in accordance with the technical and other requirements;

2) in accordance with the law governing the planning and construction, the regulations governing environmental protection, and the protection of cultural property;

3) in a manner that will not cause interference with other electronic communications networks, associated facilities and electronic communications equipment.

In this sense, the use of radio communication networks is submitted to many rules. One example is Article 25. During the construction of business and residential buildings, investors are required to build the supporting infrastructure required for the installation of electronic communications networks, associated facilities and electronic communications equipment to the user's premises, in accordance with technical and other requirements. The Ministry, at the proposal of the Agency, considering the prior opinion of the ministry responsible for spatial planning and environmental protection, shall prescribe technical and other requirements.

The Ministry, at the proposal of the Agency, adopts technical regulations prescribing requirements for certain types of electronic communications networks, associated facilities, electronic communication equipment and terminal equipment. If these regulations stipulate that conformity assessment should be carried out by a conformity assessment body, that body is appointed by the Ministry in accordance with the law governing technical requirements for products and conformity assessment. Agency may be appointed as a conformity assessment body, in accordance with the law.

The law defines radio corridors and protected zones (Article 42). The planning document identifies the available routes for entry and exit of radio-relay links (radio corridors). Along the radio corridor, and along the radio signal between the radio stations, a protective zone is defined in which shall not be permitted construction or installation of other radio stations, antenna systems or other objects that may interfere with the emitting of radio signals or that may cause harmful interference. If the modification of the planning document has affected the functioning of electronic communications in the radio corridor, these amendments shall be determined by the new radio corridor to allow unhindered electronic communications. At the proposal of the Agency, considering the prior opinion of the ministry responsible for spatial planning and environmental protection, shall prescribe requirements relating to the determination of radio corridor protection zone dimensions and construction of buildings within the zone.

Radio-frequencies, according to art.85, are used:

1) based on an individual license, which is issued on request or after completion of a public tender;

2) based on the general authorization regime;

3) for a special purpose.

The Agency shall prescribe the manner of use of radio stations by radio amateurs and radio stations that are used in domestic and foreign aircrafts, locomotives, ships and other vessels, in accordance with relevant international agreements and recommendations.

Licenses issues upon individual request

Article 86 defines the use of radio frequencies based on individual permits issued per request. The right to use radio frequencies shall be acquired on the basis of individual licenses for use of radio-frequency (hereinafter: the individual license) issued

on request, ifn the plan determined this way of issuing individual permits for specific radio frequency bands. Individual permits are issued for a solution. The decision is made on a request addressed to the Agency. The request shall contain the following information:

1) the identity of the applicant;

2) the nature of electronic communication networks or services for which the request for assignment of radio frequencies is made;

3) the radio frequencies whose assignment is requested;

4) the need and purpose of use of the radio frequencies;

5) the planned time of use of the radio frequencies;

6) the period covered by the request of radio frequencies assignment;

7) a technical solution that, depending on the radio-communications services and activities, particularly containing data about the geographic areas of use and the locations of the transmitter, signal propagation calculation and the service area, provided for the antenna system and the characteristics of the radiation, the method of ensuring the rational use of radio-frequency estimate impact on the environment and the work of other radio-communications systems.

The request shall be submitted on a form prescribed by the Agency, including instructions on mandatory elements of technical decision referred to in item 7) according to radio-communication services and activities, to which the technical solution is applied.

Deciding upon requests shall be made in the order of filing, within 40 days from the date of the request, unless the relevant international agreements provided for a different term.

The request may be refused if:

1) it is not in accordance with the allocation plan and the distribution plan;

2) the required radio frequencies are not available;

3) the use of the requested radio frequencies may have harmful effects on the environment or the operation of other radio communication systems, which cannot be prevented by using special measures.

Article 87 defines the issuance of individual permits to diplomatic and consular representations. Foreign diplomatic and consular representations (hereafter FDR) have the right to use radio frequencies on the basis of individual licenses which are to be issued upon request. Individual license issued by the Agency, at the request of FDR, by the procedure stipulated by LEC, which is carried out through diplomatic channels. Fee (remuneration) and conditions of use of radio frequencies shall be determined under conditions of reciprocity, based on the opinion of the ministry responsible for foreign affairs in accordance with the concluded international agreements.

It is possible to issue a single license to a foreign legal entity under Art.88. A foreign legal entity in the Republic of Serbia which, under the relevant international agreements, does business and technical, informational, scientific, cultural, sports and other co-operation with the relevant authorities, organizations and other entities in the country, has the right to use radio frequencies on the basis of an individual permit

issued upon request. Such an individual permit is issued by the Agency, at the request of a foreign legal entity, according to the procedure established by the LEC. Remuneration and conditions of use of radio frequencies in this article shall be determined in accordance with the provisions of LEC, unless the relevant international agreement specified otherwise.

Licenses issued after a public tender procedure

Using radio-frequency based on individual permits, which are issued after the completion of the public tender procedure under Article 89. The right to use radio frequencies shall be acquired on the basis of individual licenses. Those are to be issued after the completion of a public tender process, and when is, in that manner, defined issuing individual permits. The Agency, *ex officio* or at the initiative of the interested parties, shall decide on the requirements for the issuance of individual permits after the completion of the public tender procedure and notify the Ministry. Upon receipt of notification of the decision, the Ministry shall define (in the act) minimum requirements for the issuance of individual permits for completion of a public tender. In particular it must contain a number of individual licenses that can be issued for a specific radio frequency band, the period for which individual licenses are issued, the smallest amount of one-time fee that is paid when issuing individual permits, the requirements in terms of providing coverage of a specific piece of territory or population, as well as other minimum requirements for the issuance of individual permits. Agency makes a decision on the initiation of the tender procedure for the issuance of individual permits within 15 days from the date of entry into force of the said Act and establishes Commission for the implementation of the tender procedure.

For the implementation of the tender procedure for the issuance of individual permits, the Agency shall:

1) provide that the public tender is available to all interested parties on equal terms, the publication of the public notice;

2) determine and announce the decision-making criteria that are non-discriminatory, objective and measurable, and are appropriate to the activities or services for which a separate license is granted;

3) determine which of the applicants meets all the requirements prescribed by LEC, and laws made thereunder;

4) The decision on the selection of the best bidder on the basis of economic, technical and other criteria published in the announcement of tendering;

5) ensure that a decision on the best bid or cancellation of public tendering is adopted and publish not later than four months from the closing date for submission of applications.

Advertisement for the publication of the call for tenders must contain:

1) Subject of individual license;

2) The deadline for participation in the auction, which cannot be shorter than 45 days from the date of posting;

3) Conditions for participation in public bidding;

4) Conditions for the submission of bids (under the code or the full name of the bidder);

5) Notice of the date, time and place of opening of submitted bids;

6) Criteria for evaluation of bids and the method of determining the most advantageous offer;

7) The name and contact person in charge of providing all information relevant for the tendering process.

Announcement is published in the "Official Gazette of the Republic of Serbia", and in at least one widely available international publication, and in at least one daily newspaper distributed throughout the territory of the Republic of Serbia, as well as on the Agency's website.

One-time fee that is paid when issuing individual permits, after the completion of a public tender process, are transferred to the revenue budget of the Republic of Serbia.

Procedural rules applicable to all individual licenses

The decision for the issue of a separate license contains the following information:

1) The holder of an individual license;

2) Allocated radio frequencies;

3) The period for which a separate license is issued;

4) The period within which must begin using the allocated radio frequencies;

5) The purpose for which it was granted the right to use radio frequencies;

6) Locations or areas of coverage;

7) The time limits for notifying the Agency on the set radio stations and performing technical reviews;

8) The terms and manner of verifying the compliance with the conditions under which a is given individual permit and when an individual permit is issued to the public bidding;

9) The method of ensuring the efficient and rational use of radio frequencies;

10) Technical and operational measures to be applied in order to avoid harmful interference, ensuring electromagnetic compatibility and limiting human exposure to electromagnetic fields;

11) Obligations in connection with the use of assigned radio frequencies, stemming from the relevant international treaties;

12) The conditions for the experimental use of assigned radio frequencies.

The described decision may contain other data, if such data are in connection with the prescribed requirements for the issuance of individual permits or arising from relevant international agreements.

The holder of an individual license is required to notify the Agency of changes to the information on the holder of an individual license within 30 days of such change.

Individual permits are issued for a period not to exceed ten years. It may be extended under the same conditions for the issuance of new individual licenses, except that when extending an individual license, it is not mandatory to pay a onetime fee that is paid when first issuing individual permits and for a period not longer than the period

for which it may issue new individual permits. The holder of an individual license submits an application for renewal of a single permit within a period neither less than 30 days nor more than 90 days before the expiration of the individual permit.

Sublicensing and temporary licenses

The right to use the radio frequency assigned by individual permit cannot be transferred, rented, leased or otherwise transferred to another person (Art.93). This provision does not apply to the status change of the holder of an individual license, which occurs in accordance with the law governing the legal status of companies. In this case, the transfer can be made only on the basis of documents drawn up in writing which the Agency previously approved. The Agency may refuse to consent to this act especially if it determines that it would lead to distortions of competition. Agency shall publish the data on the approvals for these acts on its website.

Temporary licenses for the use of radio frequencies are regulated in Article 94. The right to temporary use of radio frequencies for market and technical testing of products and services, research and design, as well as for the maintenance of sports, cultural, entertainment and other events of limited duration, is acquired on the basis of temporary permits for the use of radio-frequency (hereinafter referred to as the temporary permit), issued by a decision. This decision by the Agency is issued on the basis of a reasoned request that meets the prescribed requirements. The request shall be submitted on a form prescribed by the Agency. Deciding upon requests shall be made in the order of filing, within 15 days from the date of application. The Agency determines appropriate temporary admission, which may not be longer than 60 days, and the corresponding requirements for the award and use of radio frequencies.

The request for issuance of a temporary permit may be refused if it is purpose filed in order to avoid the application of the procedures for issuing individual permits (under Art. 86 and 89 of the LEC).

Forfeiture of assigned radio frequencies is regulated in Article 95. The Agency shall decide on the forfeiture of the allocated radio frequencies if it finds that:

1) the individual's license has been issued on the basis of incorrect data or faulty documentation relevant to decision making;

2) The allocated radio frequencies are not used in accordance with the allocation plan, the Distribution Plan or issued a single permit, especially in cases where the holder of an individual license does cause harmful interference determined in the control of radio-frequency spectrum;

3) The holder of an individual license, even after receiving the notice, hasn't paid a fee for the use of radio frequencies, within the specified period;

4) the holder of an individual license is prohibited performance of electronic communication in accordance with LEC or by a final court judgment;

5) the holder of an individual license has in writing waived the right to use the assigned radio frequencies;

6) the holder of an individual license ceased to exist, without a legal successor;

7) the holder of a license for the use of radio frequencies hasn't corrected irregularities found during inspection;

8) the revocation of allocated radio frequencies necessary to comply with the changes of land use plan or plans of distribution, made in order to implement international agreements or the public interest that could not be met in any other way;

9) the revocation of allocated radio frequencies necessary for the implementation of spatial planning and environmental protection, which could not be provided by other means;

10) the body accountable for broadcasting revoked a broadcasting license to the holder of an individual license or that the time for a broadcasting license issued has runout, when a special law stipulates that an individual permit is issued as part of a broadcasting license.

11) the holder of an individual license hasn't started using frequencies in the time prescribed by law.

The holder of an individual license, whose licence was seized for the reasons mentioned in items. 8) and 9) is entitled to a replacement or allocation of new radio frequencies.

Agency assigns a radio frequency at the request of, taking into account proportionality, protection of the public interest and economic consequences of the replacement of radio frequencies.

General authorizations

The use of radio frequencies under the general authorization regime[5] is defined by Article 96. If there is risk of negligible interference or there are a harmonized radio frequency bands, especially if it is in accordance with relevant international agreements and recommendations, the radio frequencies are used by the regime general authorization. Every person has the right to use radio frequencies that are planned to be use used by the general authorization regime. The Agency shall specify the use of radio frequencies in the general authorization regime, in accordance with the agreements and recommendations.

Procedure for Limiting the Number of Rights of Use[6]

Special purpose radio frequencies usage

Defence and security agencies, as well as services for emergency response, use radio frequencies in the bands which are allocated by allocation plan exclusively for their use, without prior acquiring of permission to use radio frequencies in accordance with the terms and conditions established by the plan. These agencies are required to inform in writing and in advance the Agency of the commencement or termination of use of radio frequencies. They also submit to the Agency, at its request, or at least annually, a report on the extent and manner of use or non-use of radio frequencies. For

[5] Conditions are defined in article 39. and were already explained in the text.

[6] Under the general regime there are limitations and special areas. Those are defined here.

the use of the radio-frequency (for special purposes) fee is not paid. These authorities may use radio frequencies in the range of allocation plan that are not designated for specific purposes, in the manner and in accordance with the terms of the allocation plan and use of these bands that are prescribed by LEC and the regulations promulgated thereunder. Compensation for the use of these (which are not designated for specific purposes) radio frequencies is determined by the Agency in cooperation with the mentioned agencies, taking into account the public interest and that the authorities budget users.

Control of radio spectrum and protection against harmful interference

The Agency carries out a constant control of the use of radio frequency spectrum in the territory of the Republic of Serbia (Article 98) and the report on that is published at least once a year, while control of selected radio frequencies is conducted when needed. Technical examinations and other tests to determine the existence and causes harmful interference are performed by the Agency or any other person engaged by the Agency. Control of radio-frequency spectrum for a particular purpose, the Agency conducts in cooperation with the authorities referred to in Article 97, paragraph 1 of LEC. Control of radio-frequency spectrum intended for distribution and broadcast media, the Agency conducted in cooperation with the Agency responsible for broadcasting (about it we will be elaborating later). The Agency shall take measures to eliminate harmful interference identified in the control of radio-frequency spectrum, in accordance with the provisions of LEC, and shall propose the adoption of measures of inspection, especially if it detects unauthorized use of the radio frequency spectrum. Described measures are undertaken by the Agency without delay whenever there is threat for the defence and security, emergency services, as well endangering normal functioning of aviation, marine and radio-navigation radio-communication services. The Agency shall specify the methods to control the use of radio-frequency spectrum, and to perform technical inspections and protection methods from harmful interference.

The database on the use of radio-frequency spectrum

The Agency shall keep updated database on the use of radio frequency spectrum which specifically contains information on the assigned radio frequencies and radio frequency bands, with corresponding data on the conditions of the grant and use, the geographic scope of their use, as well as information about the holders of individual licenses and other users' radio-frequency spectrum. Agency publishes and updates the information on its website with a comprehensive search capability. The Agency shall keep updated a database relating to the control of radio-frequency spectrum and technical examinations.

Distribution and emitting of media content distribution and broadcasting media

Chapter XIV regulates distribution and transmission of media. Cooperation of the Agency with the authority in charge of broadcasting is covered by Article 100. In determining the conditions and methods of radio frequencies use for distribution and broadcast media, the Agency shall cooperate with the authority in charge of broadcasting. When it is prescribed by a special law that as an integral part of the broadcasting license there is licence for use of radio frequencies, the Agency shall issue an individual permit at the request of the competent authority for broadcasting, in accordance with the provisions of LEC and for the period specified in the license for broadcasting.

Coordination of use and application for getting radio frequency

Radio frequencies designed for use in certain border areas before the assigning are coordinated with neighbouring countries, with whom they entered into separate agreements on the coordination of the use of radio-frequency (Article 101). Radio frequencies of certain radio frequency bands, if necessary, prior to the assigning are coordinated with neighbouring countries and other interested countries. Application for allocation of radio frequencies to the International Telecommunication Union shall be submitted when:

1) the use of radio frequencies may cause harmful interference to radio communications service of another country;

2) if the radio frequencies are intended for the international radio-communication;

3) to protect the radio frequencies at the international level.

Allocation plan of radio frequency bands is treated by Article 102. Allocation plan of radio frequency bands (hereafter allocation plan) shall be determined by use of radio-frequency bands for each radio-communications services and products, in accordance with relevant international agreements and recommendations, the interests of the citizens, the economy, security and national defence.

Allocation Plan includes in particular the following information:

1) The limits of radio frequency bands;

2) The use of radio frequency bands, the technologically neutral basis, for one or more radio communication services and activities;

3) The basic conditions for the use of radio frequencies;

4) Basis of the use of radio-frequency and manner of issuing licenses under Article 85 of LEC.

Allocation Plan may be used to determine different types, conditions and the basis for the use of the different sub-bands within the same radio-frequency band. Allocation Plan is adopted by the Government, on the basis of proposals made by the Ministry, with the participation of the competent authority of the autonomous province, which is prepared by the Agency. In the process of preparing the draft plan purposes,

the Agency carries out a public consultation in accordance with the provisions of LEC and seeking the opinion of the defence, security and emergency services.

Plans for distribution of radio frequencies

Plan of radio frequency distribution (hereinafter referred to as the distribution plans) contains requirements for the allocation of radio frequencies from intended radio-frequency bands, the allocation of radio frequencies for locations or areas for one or more radio-communications services, and activities, as well as other necessary technical conditions for the use of radio-frequency (article. 103). Plans shall be based on the allocation plan and the relevant international agreements and recommendations, taking into account the needs and requirements of users. Plans shall be adopted by the Ministry, with the participation of the competent authority of the autonomous province, on the proposal of the Agency. In the process of preparing the draft plan of distribution, the Agency carries out a public consultation in accordance with the provisions of LEC and seeking the opinion of the defence, security and emergency services.

Radio frequencies are, in accordance with the law (art.104), used:

1) based on an individual license, which is issued on request or at completion of a public tender;

2) under the general authorization regime;

3) for a special purpose.

The Agency shall prescribe the manner of use of radio stations by radio amateurs and radio stations that are used in domestic and foreign aircraft, locomotives, ships and other vessels, in accordance with relevant international agreements and recommendations.

The right to use radio frequencies shall be acquired on the basis of individual licenses for use of radio-frequency (hereinafter referred to as individual licenses, art.105) which is issued on request, when the purpose of the plan is determined this way of issuing individual permits under certain radio band. Individual permits are issued through a decision. The decision is made on the request made to the Agency. The request shall contain the following information:

1) the identity of the applicant;

2) the nature of electronic communication networks or services for which the request of assignment of radio frequencies is submitted;

3) radio frequencies for which assignment is required;

4) The need and purpose of use of radio frequencies;

5) the planned time of use of radio frequencies;

6) the period covered by the assignment request of radio frequencies;

7) a technical solution that, depending on the radio-communications services and activities, particularly containing data about the geographic areas of use and the locations of the transmitter, signal propagation calculation and the service area, provided for the antenna system and the characteristics of the radiation, the method of ensuring the rational use of radio-frequency estimate impact on the environment and the work of other radio-communications systems.

This request is submitted on the form of which shall be prescribed by the Agency, including instructions to the mandatory elements of the technical solution (referred to in paragraph 4, item 7) art.105), depending on the radio-communications services and activities to which the technical solution applies. Deciding on the requirements, shall be in the order of filing, within 40 days from the date of the request, unless the relevant international agreements envisaged a different term.

The request may be refused if:

1) is not in accordance with the plan and purpose of the plan of distribution;

2) the required radio frequencies are not available;

3) the use of the requested radio frequencies may have harmful effects on the environment or the operation of other radio communication systems, which cannot be prevented by using special measures.

Issuing of licenses for single diplomatic - consular represent

Foreign diplomatic and consular representation (hereafter FDR) has the right to use radio frequencies on the basis of individual licenses to be issued upon request (Article 106). Individual license issued by the Agency, at the request of FDR, throughout the procedure stipulated by LEC, which is carried out through diplomatic channels. Remuneration and conditions of use of radio frequencies in this article shall be determined under conditions of reciprocity, in the opinion of the ministry responsible for foreign affairs in accordance with the concluded international agreements.

Issuing of single licenses for foreign law person (Art.107) - Foreign legal entity in the Republic of Serbia, under the relevant international agreements, which does business and technical, informational, scientific, cultural, sports and other co-operation with the relevant authorities, organizations and other entities in the country, has the right to use radio frequencies on the basis of individual permit issued upon request. This individual license issued by the Agency, at the request of a foreign legal entity, the procedure established by LEC. Remuneration and conditions of use of radio frequencies shall be determined in accordance with the provisions of LEC, unless the relevant international agreement otherwise specified.

Using radio – frequencies based on single license – Using radio-frequency based on individual permits issued after the completion of the public tender procedure. The right to use radio frequencies shall be acquired on the basis of individual licenses which are to be issued after the completion of the public tender procedure (Art.108), when the allocation plan, due to the limited availability of radio frequencies within a certain radio frequency band, has defined a way of granting individual permission. Agency, *ex officio* or at the initiative of the interested parties, shall decide on the requirements for the issuance of individual permits after the completion of the public tender procedure and shall notify the Ministry. Upon receipt of notification of the decision, the Ministry shall act with prescribing minimum requirements for the issuance of individual permits for completion of a public tender, which must contain a number of individual licenses that can be issued for a specific radio frequency band, the period in which the issue of individual licenses, the smallest amount of one-time fee that is paid

when issuing individual permits, the requirements in terms of providing coverage of a specific piece of territory or population, as well as other minimum requirements for the issuance of individual permits.

Agency makes a decision on the initiation of the tender procedure for the issuance of individual permits within 15 days from the date of entry into force of the act referred to in previous text and shall appoint a committee to conduct the public auction.

For the implementation of the tender procedure for the issuance of individual permits, the Agency shall (art.109):

1) provide that the public tender is available to all interested parties on equal terms, the publication of the public notice;

2) determine and announce the decision-making criteria that are non-discriminatory, objective and measurable, that are appropriate to the activities or services for which a separate license is granted;

3) determine which of the applicants meets all the requirements prescribed by this law, laws made thereunder;

4) The decision on the selection of the best bidder on the basis of economic, technical and other criteria published in the announcement of tendering;

5) a decision on the best bid or cancellation of public tendering adopts and publish not later than four months from the closing date for submission of applications.

Advertisement must contain:

1) subject of individual license;

2) the deadline for participation in the auction, which can not be shorter than 45 days from the date of posting;

3) conditions for participation in public bidding;

4) manner of submission of bids (under the code or the full name of the bidder);

5) notice of the date, time and place of opening of submitted bids;

6) criteria for evaluation of bids and the method of determining the most advantageous offer;

7) the name and contact person in charge of providing all information relevant for the tendering process.

Announcement is published in the "Official Gazette of the Republic of Serbia", and at least one widely available international publication and at least one daily newspaper distributed throughout the territory of the Republic of Serbia, as well as the Agency's website. Funds on one-time fee that is paid when issuing individual permits after the completion of a public tender process represent the revenue budget of the Republic of Serbia.

Decision for the issue of a separate license contains information about (art.110):

1) The holder of an individual license;

2) Allocated radio frequencies;

3) The period for which a separate license is issued;

4) The period within which must begin using the allocated radio frequencies;

5) The purpose for which it was granted the right to use radio frequencies;

6) Locations or areas of coverage;

7) The time limits for notifying the Agency on the set radio stations and performing of technical reviews;

8) The terms and manner of verifying the compliance with the conditions under which a given individual permits when an individual permit is issued to the public bidding;

9) The method of ensuring the efficient and rational use of radio frequencies;

10) Technical and operational measures to be applied in order to avoid harmful interference, ensuring electromagnetic compatibility and limiting human exposure to electromagnetic fields;

11) Obligations in connection with the use of assigned radio frequencies, stemming from the relevant international treaties;

12) The conditions for the experimental use of assigned radio frequencies.

The decision may contain other data, if such data in connection with the prescribed requirements for the issuance of individual permits or arising from relevant international agreements.

The holder of an individual license is required to notify the Agency of changes to the information on the holder of an individual license within 30 days of such change.

Individual permits are issued for a period not to exceed ten years (art.111). Individual licenses may be renewed under the same conditions for the issuance of new individual licenses, except that when extending an individual license when a onetime fee is not needed and for a period not longer than the period for which it may issue new individual licenses. The holder of an individual license, an application for renewal of a single permit within a period neither less than 30 days nor more than 90 days before the expiration of the individual permit.

Conditions Attached to the Rights of Use and Procedure for Its Modification

Use of radio frequencies for special purposes

Agencies of defence and security, as well as services for emergency response, are using radio frequencies in the bands that use a particular plan exclusively for their use (Art. 116) without prior permission to use radio frequencies in accordance with the terms and conditions set forth allocation plan.

These agencies are required to inform the Agency in writing in advance of the commencement or termination of use of radio frequencies. They have to submit to the Agency at its request, or at least annually, a report on the extent and manner of exploitation of radio frequencies. For the use of radio frequencies for specific purposes operators (or carriers) are not subject to fees. These authorities may use radio frequencies in the range of plan applications that are not designated for specific purposes, in the manner and in accordance with the terms of the allocation and use of the range set forth in LEC and the regulations promulgated thereunder. Compensation for the use of

the radio frequencies Agency determines in conjunction with the prescribed authorities, taking into account the public interest and that the authorities budget users.

Control of radio-frequency spectrum and protection against harmful interference

The Agency carries out a constant control of the use of radio frequency spectrum in the territory of the Republic of Serbia (art.117) and a report on that publishes at least once a year, and a control of selected radio-frequency is conducted as needed. Technical examinations and other tests to determine the existence and causes of harmful interference are performed by the Agency or any other person engaged by the Agency. Control of radio-frequency spectrum for a particular purpose, the Agency conducts in cooperation with the authorities referred to in Article 97, paragraph 1 of LEC. Control of radio-frequency spectrum intended for distribution and broadcast media, the Agency conducts in cooperation with the body responsible for broadcasting. The Agency shall take measures to eliminate harmful interference identified in the control of radio-frequency spectrum, in accordance with the provisions of LEC, and to propose the adoption of measures of inspection, especially if it detects unauthorized use of the radio frequency spectrum. The Agency is taking this action without delay when it endangers defence and security, work of emergency services, as well as normal functioning of aviation, marine and radio-navigation radio-communication services. The Agency shall specify the methods to control the use of radio-frequency spectrum of technical inspections and protection from harmful interference.

Debridement of Revocation issued licenses allocated radio frequencies

The Agency shall decide on the forfeiture of the allocated radio frequencies if it determines that (art.114):

1) the individual's license is issued on the basis of incorrect data or faulty documentation relevant to decision making;

2) the allocated radio frequencies weren't used in accordance with the allocation plan, the Distribution Plan or issued single permit, especially in cases where the holder of an individual license has caused harmful interference which was determined in the control of radio-frequency spectrum;

3) The holder of an individual license, even after receiving the notice, did not pay, within the specified period, a fee for the use of radio frequencies;

4) The holder of an individual license was prohibited to maintain service of electronic communication in accordance with LEC or by a final court judgment;

5) The holder of an individual license in writing waived the right to use the assigned radio frequencies;

6) The holder of an individual license ceased to exist, without a legal successor;

7) The holder of a license for the use of radio frequencies hasn't remedied irregularities found during inspection;

8) The revocation of allocated radio frequencies is necessary in order to comply with the changes of (land use) allocation plan or distribution plan, made in order to implement international agreements or the public interest that could not be met in any other way;

9) The revocation of allocated radio frequencies is necessary for the implementation of spatial planning and environmental protection, which could not be provided by other means;

10) The body responsible for broadcasting revoked a broadcasting license to the holder of an individual license or that the time, for which was a broadcasting license issued, has expired, when a special law stipulates that an individual permit be issued as part of a broadcasting license.

11) The holder of an individual license hasn't started using frequencies in the time prescribed by law.

The holder of an individual license, which had been seized of allocated frequencies for the reasons stated in the item. 8) and 9), is entitled to a replacement or allocation of new radio frequencies.

Agency assigns a radio frequency at the request of the person, taking into account proportionality, protection of the public interest and economic consequences of the replacement of radio frequencies.

Use of radio frequencies in the general authorization regime

If there is negligible risk of interference or a harmonized radio frequency bands, especially if it is in accordance with relevant international agreements and recommendations, the radio frequencies are used by the general authorization regime (art.115).

Every person has the right to use radio frequencies that are planned to be use used by the general authorization regime. The Agency shall specify the use of radio frequencies in the general authorization regime, in accordance with the agreements and recommendations referred to in paragraph 1 of Article 115.

The Transfer of Rights to Use the Radio and Electrical Public Domain

Transfer of rights to use radio frequencies

The right to use radio frequencies allocated through individual permit is at same regime as article 94 (art.112). This provision doesn't apply to the status change of the holder of an individual license, which occur in accordance with the law governing the legal status of companies. In such a case, the transfer can be made only on the basis of documents drawn up in writing, which the Agency previously approved. The Agency may refuse to consent to the act especially if it determines that it would lead to distortions of competition. Data on the approval for the acts of the Agency shall publish on its website.

Temporary licenses for use of radio frequencies

The right to the temporary use of radio frequencies in order to market and technical testing of products and services, research and design, as well as for the maintenance of sports, cultural, entertainment and other events of limited duration, is acquired pursuant to a temporary permit for the use of radio-frequency (in hereinafter referred to as the temporary permit) and issued by a decision (art.113). This decision by the Agency is issued on the basis of a reasoned request that meets the requirements. The request shall be submitted on a form whose form and content prescribed by the Agency. Deciding upon requests shall be made in the order of filing, within 15 days from the date of application. Agency determines appropriate temporary admission, which may not be longer than 60 days, and the corresponding requirements for the award and use of radio frequencies. The request for issuance of a temporary permit may be refused in particular if it is deemed filed to avoid the application of the procedures for issuing individual permits under Art. 86 and 89 of LEC.

Database on the use of radio-frequency spectrum

The Agency shall keep updated database on the use of radio frequency spectrum (Article. 118), which in particular contains information on the assigned radio frequencies and radio frequency bands, with corresponding data on the conditions of the licence and use, the geographic scope of their use, as well as data on holders individual licenses and other users of the radio frequency spectrum. Agency publishes and updates the information on its website with a comprehensive search capability. The Agency shall keep updated a database relating to the control of radio-frequency spectrum and technical examinations.

Chapter XIV deals with the distribution and broadcasting media. Cooperation of the Agency with the authority responsible for broadcasting is defined by art.119. In determining the conditions and methods of use of radio frequencies for distribution and broadcast media, the Agency shall cooperate with the authority in charge of broadcasting. When a special law prescribes that as an integral part of the broadcasting license is also licence for use of radio frequencies, the Agency shall issue an individual permit at the request of the competent authority for broadcasting, in accordance with the provisions of this Act and for the period specified in the license for broadcasting.

Public service obligation to transfer

Agency, at the request of the broadcasting agency determines operator (carrier) of electronic communication networks for distribution and broadcast media, which is required to transmit one or more radio and television programs at the national, provincial, regional or local level, when (Articles 120) :

1) a significant number of end-users using an electronic communication network of the operator as the sole or primary method for delivering media content, and

2) it is necessary to achieve clearly defined objectives of public interest in the media, as determined by the authority responsible for broadcasting, in accordance with the law regulating the electronic media and the law governing public information respecting the principle of proportionality and the public.

Specific responsibilities of providing access

The Agency may oblige the operator (carrier) of electronic communications networks for distribution and broadcast media content to allow access to application software interfaces and electronic program guides to another operator, under reasonable and non-discriminatory terms, to the extent necessary to provide services to end users (Article 120). Conditional access services are provided by Article 121. Operator (carrier) of electronic communications networks for distribution and broadcast media, which offers conditional access to media content (hereinafter referred to as conditional access service operator), shall make it possible for full control of media content delivery via such a system. Conditional access service operator is obliged to offer, under fair, reasonable and non-discriminatory conditions, media content providers of technical services that enable their subscribers to access media content with the use of conditional access devices. Operator of services conditional access shall not interfere with the reception of media content which is distributed and transmitted without conditional access.

Conditional access service operator is obliged to track its business activity that is related to a conditional access by using separate accounting. Holders of industrial property rights on devices and systems with conditional access shall cede these devices and systems to manufacturers of terminal equipment under conditions that are fair, reasonable and non-discriminatory and that producers are not decapacitated to implant interfaces for connecting to other access systems or parts of characteristic other access systems, into the same device, to the extent that it does not jeopardize the security of conditional access systems.

Switchover from analogue to digital television broadcasting

At the proposal of the Agency, Ministry prepares in cooperation with the authority in charge of broadcasting, the act about the transition from analogue to digital television broadcasting and multiplex access to terrestrial digital broadcasting (art.122). This Act regulates in particular:

1) the manner and timing of the transition;

2) requirements and dynamics in terms of establishing a network for the distribution of digital television broadcasting in the territory of the Republic of Serbia;

3) requirements for the formation of the multiplex;

4) the extent of use of radio frequencies, to the extent necessary for successful transition to digital television broadcasting.

Public company established to manage the broadcasting infrastructure, in accordance with the decision on the establishment and the act establishes an electronic

communications network for multiplexing, distribution and broadcasting digital television programs.

In order to establish the network, the Agency issues to Public company (PC) "Emission techniques and connections" individual license for the use of radio frequencies in accordance with the act described. PC "Emission techniques and connections" is obliged enable multiplex access to the network to the holders of licenses for the broadcasting of television programs, in accordance with the licenses issued for broadcasting.

No later than the completion of the transition from analogue to digital television broadcasting by the Government, at the proposal of the Ministry, in cooperation with the autonomous provincial body in charge of electronic communications, the principles governing the use of the remaining radio frequency bands intended for terrestrial digital broadcasting, as well as the provision of broadband services (digital dividend). In the process of preparing the proposal for the Act, the Ministry shall conduct a public consultation of at least 30 days. Assigning individual permit in accordance with this act shall be in accordance with the provisions of this Act.

In order to increase accessibility to services of general economic interest in the field of electronic communications, the Government, in accordance with the regulations governing the protection of consumers, establish support measures and the requirements regarding the criteria for determining vulnerable consumers in the purchase of equipment for the reception of digital television (article. 104a).

The obligation to retain data[7]

General statement

Records of requests for access to retained data

The operator keeps the data in accordance with the provisions of Art. 128 -130 of LEC, as well as the authorities that access data in a manner determined by the provisions of Article 128, paragraph 2 of LEC, are obliged to keep records of requests for access to retained data in a calendar year.

The records referred to in Article 130a contains information on:

1) the number of requests for access to stored data;

2) the number of filled requests for access to stored data;

3) The time that has elapsed from the date when the data is kept up to date until when the access to the data was requested in accordance with Article 128, paragraph 2 of LEC.

The records do not contain personal data. Described persons shall submit records, not later than 31 January for the previous calendar year, to the authority responsible for the protection of personal data.

[7] Mina Zirojević, Zvonimir Ivanović, *Zaštita prava intelektualne svojine u sektoru informaciono-komunikativnih tehnologija*, Institut za uporedno pravo Beograd, 2016.

Protection of retained data

The operator shall, in respect of the protection of retained data, in particular secure (art.130):

1) that the retained data is of the same quality and subject to the same security measures and protection as well as data in the electronic communication network operators;

2) the retained data is protected in an appropriate way against accidental or unauthorized destruction, accidental loss or alteration, unauthorized or unlawful storage, processing, access or disclosure, in accordance with the law governing the protection of personal data, or the law governing the protection of classified information when it comes to data that are stored and distributed in accordance with Article 128, paragraph 7 of LEC;

3) to access stored data in an appropriate manner is limited only to authorized persons who have access to the retained data in accordance with Article 128, paragraph 7 of LEC;

4) that retained data are destroyed after the deadline referred to in Article 128, paragraph 6 of LEC, other than the data stored and delivered in accordance with Article 128, paragraph 7 of LEC.

The operator shall provide, for the purpose of exercising the obligations referred to in paragraph 1 of this Article, at its own expense the necessary technical and organizational requirements, as well as evidence thereof to the Agency, in accordance with the provisions of LEC.

Supervision of the execution of the obligations of operators referred to in paragraph 1 of this Article shall be performed by competent authority for the protection of personal data and when the data is submitted in accordance with Article 128, Paragraph 7 of the law by the authority responsible for supervising the implementation of laws that regulate the protection of confidentiality.

Records of requests for access to retained data

The operator keeps the data in accordance with the provisions of Art. 128 -130 of LEC, as well as the authorities that access data in a manner determined by the provisions of Article 128, paragraph 2 of LEC, are obliged to keep records of requests for access to retained data in a calendar year.

The records referred to in Article 130a contains information on:

1) the number of requests for access to stored data;

2) the number of filled requests for access to stored data;

3) The time that has elapsed from the date when the data is kept up to date until when the access to the data was requested in accordance with Article 128, paragraph 2 of LEC.

The records do not contain personal data. Described persons shall submit records, not later than 31 January for the previous calendar year, to the authority responsible for the protection of personal data.

Subjects of supervision and inspection

Agencies

Chapter XVIII processes verification procedures and operator inspection. In this regard, the Agency's powers are prescribed by art.131. Operators are required to carry out electronic communications in accordance with the prescribed general conditions for conducting activities, certain specific obligations on operators with OCMP, set conditions for the use of numbering, individual licenses for use of radio frequencies, as well as other obligations stipulated in LEC and regulations adopted thereunder.

The Agency is authorized to require from the operator data and information it needs to check their compliance in accordance with their obligations, as well as to perform measurements and tests the operation of electronic communication networks and services, associated facilities, electronic communication equipment and terminal equipment.

The tasks of measuring and testing agency is carried via a control-measuring centres as organizational units of the Agency (regional unit), or through persons authorized for performing measurements and tests.

If the Agency determines that the conduct of the operator is not in compliance with its obligations under paragraph 1 of Article 131, shall notify the operator and the period within which the operator can comment on the irregularities, or to remedy found irregularities and inform the Agency.

This period may not be shorter than eight days from the date of receipt of the request by the operator, unless the Agency determines harder or repeated violation of prescribed duties. If the Agency determines that the operator did not rectify the irregularities within the deadline, submit an application to inspection by the Ministry.

Inspection Supervision

Inspection supervision over the implementation of this Act, the regulations governing electronic communications, as well as international agreements in the field of electronic communications, is conducted by the Ministry through inspectors of electronic communications (hereinafter referred to as the inspector). Inspection supervision over the implementation of laws and regulations governing the electronic communications sector in the autonomous province shall be done through autonomous province agencies. These activities are conducted as an autonomous province entrusted.

Legal Framework

Law on public information and media[8]

General provisions

The aim of the legal regulation is defined in Article 2 of the Law on Public Information and Media (hereafter, LPIM). Rules on public information provide and protect

[8] *See* "Official gazette of RS", nr. 83/2014.

exposing, receiving and exchanging of information, ideas and opinions through the media in order to promote the values of a democratic society, conflict prevention and peacekeeping, truthful, timely, credible and complete information and allow the free development of personality.

Subject to legal regulation is intended by article 3. and according to it: the law is governing the manner of exercising the freedom of information that specifically includes the freedom to gather, publish and receive information, freedom to form and express ideas and opinions, freedom to print and distribute newspapers and freedom of production, delivery and publishing of audio and audio-visual media services, freedom to impart information and ideas over the Internet and other platforms, as well as freedom of publication of media and the activity of public information.

LPIM is governing principles of the mass media, the public interest in public information provision and allocation of resources for the public interest, impressum, summary impressum and identification, public information about the media and the Register, the protection of media pluralism, the position of editors, journalists and representatives of foreign media, distribution, media, temporary storage and access to the media track, special rights and obligations of public information, information about the personality, the means and methods of legal protection, supervision over implementation of laws and penalties.

Freedom of information

Article 4, declares the freedom of the media and proclaims the principles. Public information is free and is not subject to censorship. It is prohibited to directly and indirectly discriminate of editors, journalists and others in the area of media, Public informing, because of their political affiliation and beliefs, or other personal property. It shall not endanger the free flow of information through the media, as well as the editorial autonomy of the media, particularly through pressure, threat or blackmail editor, reporter or source of information.

Physical attack on editors, journalists and other persons involved in the collection and publication of information through the media is punishable by law. Freedom of information cannot be diminished by abuse of official position and public authorities, property and other rights, as well as the influence and control of the means of printing and distribution of newspapers or electronic communication networks used for the distribution of media content.

Information on matters of public interest

Through the media are published the information, ideas and opinions on the happenings, events and personalities that the public has a legitimate interest to know, regardless of the manner in which the information was obtained in accordance with the provisions of LPIM (Article 5). Everyone has the right to be informed truthfully; complete and timely on matters of public interest and means of public information are obliged to respect this right.

In order to enable citizens to form their own opinions on matters, events and personalities, a variety of information sources and media is provided. In order to protect

competition and diversity of ideas and opinions it is forbidden to form any kind of monopoly in the area of public information. No one can have a monopoly on the publication of information, ideas and opinions in the media. No one can have a monopoly on the foundation, or distribution media. By this it is proclaimed protection of media pluralism and stipulated the prohibition of monopolies in the area of public information (Article 6).

To form their own opinions about the credibility and reliability of information, ideas and opinions published in the media, and in order to assess the possible impact of the media on public opinion, as well as for the protection of media pluralism to the public information media.

Position holders of public and political office

Elected, appointed, or appointed holder of a public and political office is obliged to tolerate the expressing of critical thinking, which is related to the results of his work, or policy implemented in connection with the exercise of his functions, regardless of whether they feel personally offended by presenting these opinions (Article 8).

Due Diligence

LPIM in Article 9 introduces a new standard for responsibility in the media. According to it, editor and journalist, both have a duty to the due diligence prior to the publication of information that contains data about a particular phenomenon, event or person and to verify its origin, authenticity and completeness.

Editor and reporter shall transfer information, ideas and opinions accurately and thoroughly, with due diligence and if the information is taken from other media – to specify the name of the media.

Institutions of public service media and other media that operate in accordance with the principles of public service media in particular are bound to the phenomena, events and personalities report promptly and impartially, to facilitate the expression of ideas and opinions that are represented in the community, to encourage debate in the spirit of tolerance on all matters of public interest, to produce a variety of program content and to strive for the highest level of service quality.

Law on electronic media – Electronic Media Law (ELC)

Scope of the Law

Law is stipulating in Article 1, in accordance with international conventions and standards, organization and operation of the regulatory body for the electronic media, the conditions and the manner of audio and audio-visual media services, conditions and procedures for issuing licenses for the provision of audio and audio-visual media services, and other issues relevant to the area of electronic media.

The provisions of this Act shall not apply to the performance requirements of electronic communication, conditions and manner of use of radio frequencies for

distribution and broadcast media, as well as the conditions of the installation, use and maintenance of broadcasting radio station (broadcasting, fixed and mobile).

Provisions of the ELC shall be interpreted in favour of promoting values of a democratic society, in accordance with the principles of the Constitution of the Republic of Serbia, the law governing public information and the applicable international standards in the field of human and minority rights, as well as the practice of international institutions which supervise their implementation.

Article 4 defines the basic concepts and terms for the area that regulates ELC. Terms used herein shall have the following meanings:[9]

1) electronic media is program or program content of radio and television, as well as program content available on demand via electronic communication networks and content of electronic publications;

2) the media service is audio-visual media services and media radio services;

3) audio-visual media service is audio-visual program content providing to unlimited number of users via electronic communication networks, the editorial responsibility of the service provider, in the form of television broadcasting, audio-visual media services on demand, as well as audio-visual commercial communication;

4) the program content, information, ideas and opinions, as well as works of authorship in audio form (hereinafter: the audio content), or in the form of moving images with or without sound (hereinafter referred to as audio-visual content), which is a single item in program and are available to the public through electronic media for information, entertainment, education etc…

5) editorial responsibility represents responsibility for the control over the selection of programs and their organization, whether it is on the order of delivery to the chronological scheme or providing content at the request of the catalogue, unless the law provides otherwise;

6) the media service provider is any natural or legal entity who has editorial responsibility for the choice of audio-visual content of audio-visual media services, and audio content of media services and radio, which determines the organization of the content;

7) electronic communication network for the distribution of media content is an electronic communication network in terms of regulations governing electronic communications, which is used for the distribution of media content;

8) operator of electronic communication networks for the distribution of media content (hereinafter referred to as the operator) is a person who performs or is authorized to perform an electronic communications service media content distribution;

9) multiplex operator is a person who performs or is authorized to perform an electronic communications service multiplexing media content and other data in terms of regulations governing electronic communications;

10) television broadcasting (linear audio-visual media service) is a service which is provided by carrier through audio-visual media services for simultaneous monitoring program based on the program schedule;

11) audio-visual media services on demand (non-linear audio-visual media service) is a service of audio-visual media services provided by carrier for monitoring

[9] "Official gazette of RS", nr. 83/2014.

program for a period selected by the user, at his own request, from the catalogue of programs from which the selection and organization is performed by provider (carrier);

12) audio-visual commercial communications are images with or without sound intended for direct or indirect recommendation of goods, services or properties of the natural or legal entities in respect of activities which that person is done for profit, in exchange for cash or other consideration or for self-promotional reasons (e.g. television advertising, sponsorship, television sales and marketing of products);

17) covert audio-visual services is to present, in a word or picture, goods, services, corporate name, trade mark or other designation, or activities of a natural or legal entity engaged in the production of goods or provision of services, with the intention of presenting in the purpose of advertising and may result in misleading the public as to its true nature, it is considered that there is the intention especially if that is done for financial or other compensation;

18) media service of radio service is providing audio content to an unlimited number of users via electronic communication networks with the editorial responsibility of the service provider, for simultaneous monitoring based on the schedule of the program (linear radio media services), or in order to monitor in the time selected by the user at his own request on the basis of catalogue of programs whose selection and organization performs provider (media services on demand);

19) electronic publication is editorially designed web page or website;

20) protected service is a media service that is provided with conditional access;

21) Conditional Access is a technical measure or software solution which enables the use of protected services provided payment of compensation, as well as other form of prior individual authorization;

22) zone distribution (allotment) is an area in which are distributed transmitter locations to ensure coverage of digital terrestrial television signal within the area in accordance with the Law on Ratification of the Final Acts of the Regional Conference on the Radio Communications for planning of the digital terrestrial broadcasting service in parts of regions 1 and 3, with in the frequency bands ranging from 174-230 MHz and 470-862 MHz (RRC-06)[10] [11];

23) coverage area is a single service area or the sum of individual service areas to any analogue or digital radio transmitter in case of network radio transmitter inside that provides coverage of analogue and digital terrestrial signal of individual audio-visual media services and media services, radio, and that in the case of digital broadcasting includes one or more distribution zones;

24) public media services are the production, purchase, processing and publication of information, education, science, culture, art, children, entertainment, sports, and other programs of general interest, particularly for the purpose of exercising their constitutional rights and freedoms, exchange of ideas and opinions, to foster political, gender, ethnic and religious tolerance as well as the preservation of national identity through a program of public service media;

28) As European audio-visual works are treated works that are created in the member states of the European Union; acts that were created in other European coun-

[10] "Official Gazette RS - International treaties", Nr. 4/10.

[11] Stable Internet adress: https://www.ratel.rs/upload/documents/Regulativa/Strategije/Serbia_bb_development_strategy.pdf.

tries that are parties to the European Convention on Trans frontier Television of the Council of Europe and works that are jointly produced under the agreement relating to the audio-visual sector, and which have been concluded between the European Union and third countries and fulfilling the conditions defined in these agreements.

European audio-visual works that were created in the member states of the European Union and the acts that occurred in other European countries that are parties to the European Convention on Trans frontier Television of the Council of Europe must also meet one of the following conditions:

1) that are created by one or more producers who are established in one or more of these states;

2) the production of these works was constantly monitored or controlled by one or more producers who are established in one or more of these states,

3) the contribution of co-producers of those States, in the total co-production costs, is much higher and that given co-production is not controlled by one or more co-producers who are based outside of those countries.

Works that are not European works within the meaning of this law, but are produced in the framework of bilateral co-production agreements, which are concluded between Member States and third countries shall be European works provided that the co-producers from the European Union provided a majority share in the total cost of production and the production is not controlled by one or more productions that are established outside the territory of the member States.

Title II determines the regulatory body for the electronic media. Article 5 stipulates the establishment of that body. The regulatory body for the electronic media (hereinafter Regulator), established by this Law, is an independent, alone standing regulatory organization with legal entity exercising public authority in order to: the effective implementation of the policy set in the provision of media services in the Republic of Serbia; improving the quality and variety of electronic media; contribution to the preservation, protection and development of freedom of opinion and expression; in order to protect the public interest in the field of electronic media and the protection of users of electronic media in accordance with the provisions of this Act, in a manner befitting a democratic society. The controller is functionally and financially independent of government agencies and organizations, service providers and media operators. The seat of the regulator is in Belgrade. For the execution of professional and to administrative jobs it is established a professional service of the Regulator whose basic rules of organization and operation prescribed by the Statute. To the rights and duties of employees in professional services regulator are applied the regulations governing the rights and obligations of civil servants. In order to achieve more efficient supervision of the activities of providers of media services, regulator may establish branch offices. In carrying out specific activities within their jurisdiction, the Regulator may engage other domestic or foreign legal entities and individuals. For carrying out activities within its jurisdiction Regulator is responsible to the National Assembly. Mode and the internal organization of the Regulator are regulated by the Statute, which is adopted by the Council of the Regulator.

Regulatory bodies are the Council and the President of the Council. Council decides on all matters within the scope of the Regulator. President of the Council represents the regulator or, in his absence the Deputy President of the Council.

Regulatory Council (hereinafter: the Council) consists of nine members who are elected from the ranks of distinguished experts in the field that are of importance for carrying out responsibilities of the Regulator (media specialists, economists, lawyers, engineers, telecommunications, etc..). Council member's official pursuant to the regulations governing conflicts of interest in exercising public functions. Council member can only be a person who has a higher education, who is a citizen of the Republic of Serbia and resides in the territory of the Republic of Serbia.

Council members are elected by the National Assembly at the proposal of the authorized nominators. Council member is elected if he is to his majority vote of the total number of deputies.

Authority and responsibility to elect members of the Council are (Article 9):

1), the competent committee of the National Assembly of Republic of Serbia;

2) The competent committee of the Assembly of the Autonomous Province of Vojvodina;

3) universities accredited in the Republic of Serbia by mutual agreement;

4) The association of publishers of electronic media, whose members have a minimum of 30 licenses for the provision of audio and audio-visual media services and journalists' associations in Republic of Serbia which each individual has at least 500 members and were registered at least three years prior to the announcement of the public invitation by mutual agreement;

5) associations of film, stage and theatre artists and composers' associations in Serbia, if they are registered for at least three years prior to the announcement of the public invitation by mutual agreement;

6) association whose aims are freedom of expression and the protection of children, if they were registered for at least three years prior to the date of the public announcement of the call and have a minimum of three implemented projects in this area in the last three years by mutual agreement;

7) national councils of national minorities, by mutual agreement;

8) Churches and religious communities, by mutual agreement.

Authorized proponent proposes two candidates for the Council, taking into account the uniform territorial representation candidates.

Responsible Service of the National Assembly published a public call for the nomination of candidates for members of the six months prior to the expiration of the term of the Council, or within 15 days of the termination of the mandate of the reasons set forth in Article 15 of the items. 2) -4).

Proposer authorized under Article 9, paragraph 1, items. 1) and 2) the ELC or organization that enters into the circle of organizations that together form a single authorized proponent of Article 9, paragraph 1, items. 3) -8), submits to the competent authority of the National Assembly reasoned proposal of two candidates for the Council within 15 days of publication of the call. Two or more organizations may submit a joint proposal of the candidate. With the proposal it is obligatory to submit a proof of fulfilment of the requirements for the organization of Article 9, paragraph 1, ELC, and written consent of the candidate to the proposal.

Responsible Service of the National Assembly shall establish a list of candidates for the Council, as well as a list of organizations that together form a single authorized proposer within seven days of the expiry and publish them on the Web site of the National Assembly.

In Exception to that a candidate list and the list of organizations can be established within 15 days from the date of expiry, if the competent service of the National Assembly left the organization additional time to correct their proposal and submit evidence of compliance with requirements.

In charge of the National Assembly within seven days of the publication of the list of candidates and lists of organizations under Article 10 of the LEC determines the date of determination of the joint proposal of two candidates for the Council.

Responsible Service of the National Assembly provides organizations that together form a single authorized proposer space to hold a meeting to determine the joint nomination of a candidate.

Between dates of the filing date and date of the meeting of the organizations can't pass more than seven days. At the meeting, the organizations' settle the final proposal of the two candidates for the Council, by agreement. If agreement cannot be achieved by consent of all organizations, the final draft of joint candidates shall be determined by ballot. The candidate is the one who received the most votes. Responsible Service of the National Assembly provides and organizes a vote and publishes it on the web site of the National Assembly. The competent committee of the National Assembly organized a public discussion with the nominated candidates for the Council within 15 days of the determination of the motion referred to in paragraph 8 of this Article.

Council member's election shall be placed on the agenda of the next session of the first National Assembly after the public discussion.

Council member cannot be a person who performs a public or office in a political party in terms of regulations governing the rules relating to the prevention of conflicts of interest in exercising public functions. The applicant shall submit to the authorized nominating authority a written statement that there are no such restrictions set.

Council members do not represent the views or interests of the bodies or organizations that nominated them, but perform their duties independently, according to their knowledge and conscience, in accordance with the law. Council member function may only be terminated on the grounds and procedure prescribed by this law. No one has the right to in any way affect the work of the Council members, nor are they obliged to respect anybody's instructions in relation to their work, except a decision of the competent court passed in the judicial review proceedings of the Council.

Member of the Council shall be elected for a term of five years and may be re-elected.

Regulator

The scope of work of the Regulator is prescribed by Article 22. So, by it, regulator:

1) determines the Draft Strategy for Development Media Services radio and audio-visual media services in the Republic of Serbia, and submits it, respecting the legally stipulated procedures, the Government for approval;

2) adopts the Statute;

3) adopts general bylaws prescribed by law;

4) issues licenses for the provision of media services, television and radio linear media services (hereinafter referred to as licenses);

5) regulates the procedure, requirements and criteria for the issuance of permits in accordance with the provisions of this Act and shall prescribe the form and content of such licenses;

6) issues licenses for provision of media services at the request and shall specify the authorization process;

7) keeps the Register of media service providers and record media services on demand;

8) controls the operation of media service providers and ensure the consistent application of the provisions of this Act;

9) imposes measures providers of media services in accordance with this Law;

10) provides rules that are binding on media service providers, especially those that provide the implementation of the Strategy under item 1;

11) decides on charges in connection with the program activities of providers of media services;

12) shall define the logical channel numbering;

13) provides opinion to the competent state authorities in connection with accession to international conventions relating to the area of the provision of media services;

14) Initiates the preparation and amendment of laws, regulations and by-laws for the effective performance of tasks within their scope of work;

15) establishes detailed rules relating to program content in relation to the protection of human dignity and personal rights of others, protecting the rights of minors, prohibition of hate speech and other;

16) Performs analysis of relevant media market, in cooperation with the body responsible for the protection of competition, in accordance with the methodology prescribed by the act passed by the Regulator;

17) conducts research of the user needs of media services and protect their interests;

18) cooperates and coordinates their work with the body in charge of electronic communications and the body responsible for the protection of competition, as well as with other regulatory authorities in accordance with ELC;

19) encourages the preservation and protection of Serbian culture and language as well as culture and language of national minorities;

20) encourages the improvement of the availability of media services to people with disabilities;

21) encourages the development of creativity in the field of radio, television and other audio-visual media services in the Republic of Serbia;

22) encourages the development of professionalism and high level of education of employees in the electronic media in Serbia, as well as improving the editorial independence and autonomy of the media service provider;

23) performs other duties in accordance with law.

The Affairs stipulated in items. 3) 4) 5) 6) 9) 10) 12) and 15) Regulator performs as entrusted. The regulator is bound to the regulations enacted on the basis of points. 3), 5), 10), 12) and 15) of this Article to obtain an opinion on their constitutionality and legality and to publish them in the "Official Gazette of the Republic of Serbia".

The regulator controls the operation of media service providers with respect to the consistent implementation and promotion of the principles underlying the regulation of relations in the field of electronic media, in terms of meeting the requirements for the provision of media services, as well as carrying out other obligations under the provisions of this Act and the bylaws are service providers, and undertake required measures without delay.

In implementing control regulator is obliged to take special care that providers of media services comply with the obligations relating to program content provided by ELC and the conditions under which they were issued the license, which is particularly related to the type and character of the program.

Regulator initiates proceedings before a competent court or other governmental authority against the media service provider or responsible person, if his (its) act or omission has the character of an offense punishable under the law. Regulator is adopting regulations, guidelines and recommendations for more efficient implementation of ELC. By Ordinance Regulator brings closer detailed specific provisions of the law. Guidelines governing the manner in which the regulator applies the provisions of law or regulation relating to obligations relating to program content. Regulator makes a recommendation in the case of inconsistent but approved practice of providers of media services in the implementation of the provisions of this Act relating to program content, if it is in the interests of users of media services to establish a uniform practice in order to improve ways of providing these services. The recommendation is not binding media service providers. Regulations and instructions are published in the "Official Gazette of the Republic of Serbia", a recommendation is published on the website of the Regulator.

Regulator, at the request of the competent state authority, gives its opinion on the accession to international conventions and other agreements relating to the area of providing media services. The controller is cooperating with authorities and organizations responsible for public information, electronic communication, protection of competition, consumer protection, protection of personal data, the protection of equality and other agencies and organizations on issues relevant to the area of providing media services. Regulator is working with regulatory bodies of other countries in the field of media services, and the relevant international organizations on matters within its jurisdiction. Competent state authorities must obtain the opinion of the Regulator in the preparation of regulations relating to the field of electronic media.

The controller can issue to media service provider with a warning, warning, temporary ban on the publication of the program content or he may revoke the license for violation of obligations relating to program content, (prescribed by Art. 47-71 ELC), as well as violations of the conditions contained the permit or approval for the provision of media services in accordance with the provisions of this Act.

Regulator imposes measures described independently of the use of other means of legal protection available to the injured or another person, in accordance with the provisions of special laws. In imposing measures Regulator is obliged to observe the principles of objectivity, impartiality and proportionality, and during the process of imposing measures media service provider must be able to plea on the fact and the reason for the procedure. Described measures, except measures relating to revocation of the license, shall apply accordingly to the media service provider for which there is no requirement to obtain a license.

Media services (art.44) are provided by:

1) institutions of public service media in accordance with the law governing the operation of public service media;

2) commercial media service provider;

3) The media service provider of civil society.

Providers provide media services throughout the Republic of Serbia and its part.

Media service provider under the jurisdiction of the Republic of Serbia is obliged to abide by the rules that apply to audio-visual media services in the Republic of Serbia. Media service provider is under the jurisdiction of the Republic of Serbia if:

1) it was established in its territory;

2) if is not established in the territory, but:

(1) using satellite earth transmitting station, which is located in the Republic of Serbia,

(2) use satellite capacity appertaining to the Republic of Serbia.

It shall be considered as media service provider established in the Republic of Serbia if:

1) is based in the Republic of Serbia and it is making editorial decisions about media services;

2) has its control body in the Republic of Serbia, and the editorial decisions of media services are brought in another EU Member State, provided that a significant number of people work for it in the Republic of Serbia, engaged under the contract of employment or otherwise, involved in carrying out activities related to with media services;

3) is based in the Republic of Serbia, and a significant number of persons are engaged in the work contractually or otherwise involved in carrying out activities related to media services, operating in the Republic of Serbia and other European Union countries;

4) originally started its activities in accordance with the law, in the Republic of Serbia, provided that it maintains a stable and effective link with the Serbian economy, and that a significant number of persons are engaged in the work contract or otherwise involved in carrying out activities in related to media services not working in one of the Member States of the European Union;

5) has its centre of business in the Republic of Serbia, a decision on media services are made in a State which is not a member of the European Union, or *vice versa*, provided that a significant number of persons are engaged in the work contract or oth-

erwise involved in the conduct of activities in the related to media services, operating in the Republic of Serbia.

If according to the described criteria couldn't determine whether the media service provider is under the jurisdiction of the Republic of Serbia or other European Union Member States, the media service provider is in the jurisdiction of the Member State in which he was established within the meaning of Art. 56-58. of the Stabilisation and Association Agreement between Serbia and the European Communities and their Member States.

Freedom of reception and retransmission

The freedom of reception and retransmission of media services from other countries, which is guaranteed by the Republic of Serbia, through ratified international treaties. Regulator temporarily can restrict freedom of reception and retransmission of television media service in the case of obvious, serious and severe violations of the provisions of Article 68, paragraph 1, ELC, as in the case of incitement to hatred based on race, sex, religion or national origin, repeated at least twice in the past 12 months, upon written notification of service provider, his (its) state of residence and other competent bodies, if so provided by an international agreement, and if the decision in consultation with the country of residence or other competent authority, does not occur even in the period of 15 days from notification, and a violation of the above provisions of this Act continue.

Media service provider, which is under the jurisdiction of the Republic of Serbia, for the violation of these provisions may be subject to court proceedings. Regulator temporarily can restrict freedom of reception and retransmission of audio-visual media services on demand in the event that it is necessary for the preservation of public order, a particularly to: prevent committing, investigate, detect and prosecute of criminal offenders, protect minors, to prevent incitement to hatred based on race, sex, religion or nationality, and violations of human dignity, for reasons of public health, for public safety, national security and defence, the protection of consumers, including investors, in case of serious violations or threats of violation of those interests, and in proportion to the interest on which in this case the word.

The controller will temporarily restrict freedom of reception and retransmission of audio-visual media services on demand, under specified conditions,[12] as previously requested by the home country to take appropriate measures, and when non was taken, or those measures have not proved sufficient, and if the intention of taking measures informed home country or other competent authority, if so provided by an international agreement.

Regulator may deviate from the law prescribed conditions for reasons of urgency, in which case the home country or other competent authority, if so provided by an international agreement on the measures taken and the reasons for urgency because it has not acted in the manner specified ELC notify you as soon as time.

[12] Because of reasons of protection of public health, public safety, national security and defense, protection of consumers, including investors in case of severe breach or threat of breaching defined interests in proportion to interests in concrete case. Provisions relating to all the media services.

The controller will immediately suspend the implementation of measures if the competent authority provided for by an international agreement establishes that the measure was not determined in accordance with the provisions of an international agreement, or the rights and principles on which the treaty calls.

General obligations of providers of media services in relation to program content.

Media service provider in relation to its program content, in accordance with their program concepts, shall:[13]

1) provide free, true, objective, complete and timely information;

2) transmit communications of public authorities, of emergency nature relating to the endangerment of life, health, safety, or property;

3) contribute to raising the general cultural and educational level of the population;

4) does not provide program content that is highlighting and supporting drug abuse, violence, criminal or other misconduct, and the contents of abusing the credulity of viewers and listeners;

5) comply with the ban on political advertising outside an election campaign, and during the election gives opportunity to campaign to registered political parties, coalitions and candidates provide representation without discrimination;

6) by program content for children of preschool age synchronizes the Serbian language or languages of national minorities,

7) conducts prize competitions fairly, with the publication of clear rules about these facilities and publicly promised reward;

8) Provide a quality program in terms of content, from technical point of view, applying international and national standards.

All media service providers are required to program contents in accordance with the regulations governing public information and in accordance with the regulations governing the protection of cultural property.

Specific technical duties

Commercial media service provider licensed to provide service television broadcasting or radio media services, through analogue terrestrial transmission, must provide good quality reception of radio or television analogue signals for at least 60% of the population in the coverage area. Media service provider must not use the technique that works on the subconscious. Media services are provided in a manner that ensures a level tone of all program content, especially audio-visual commercial communication in relation to other programming content. The obligation of identifying media service provider shall be subject to the laws governing public information and the media.

The obligation to respect human rights

Media services are provided in a manner that respects human rights and personal dignity in particular. The regulator ensures that all program content respects personal

[13] "Official Gazette of RS", nr. 42/02, 97/04, 76/05, 79/05 - other Law 62/06, 85/06 and 41/09.

dignity and human rights, especially the minds that is not showing degrading treatment and scenes of violence and torture, unless there is a programmatic and artistic justification. Facilities that can harm the physical, mental or moral development of minors must be clearly marked and are not published at the time it is reasonable to expect them to follow the minors, given the usual schedule of their activities, except as a very protected with conditional access services in a way envisaged by this Law.

Limitations

The controller ensures that the programming media service provider does not contain information inciting, open or covert, discrimination, hatred or violence because of race, colour, ancestors, nationality, ethnic origin, language, religion or political beliefs, gender, gender identity, sexual orientation, economic status, birth, genetic characteristics, health status, disability, marital and family status, criminal record, age, appearance, membership in political, trade union and other organizations, and other actual or presumed personal characteristics.

Media service provider shall, in accordance with its financial and technical capabilities, make available its program and its content for the individuals with impaired hearing and impaired sight. Regulator instigates media service providers to adjust its program and contents of it and make them available to the parties with disabilities (article. 52).

The regulator ensures that all providers of media services comply with the regulations on copyright and related rights.

Responsibility for Content

Media service provider is responsible for program content, regardless of whether it is produced by a provider or other person (e.g. Independent productions, leased term, exchange program, program announcements, SMS and other messages of the audience, etc...) (Article 54). The provisions of Art. 47-54. of ELC shall apply to teletext services and interactive services related to program content.

It is forbidden to display pornography, scenes of brutal violence, and other programs that can harm the physical, mental or moral development of minors. The regulator ensures that programs that can harm the physical, mental or moral development of minors are not available via the media service radio and television broadcasting, except when the time of broadcast or technical process ensured that minors are generally not able to see them or hear. Regulator encourages media service providers to organize a permanent internal control of content from the perspective of the protection of minors. Regulator informs media service providers about content that is found to be inconsistent with the rules on the protection of minors. Regulator, at the request of the media service provider, provides an opinion on the conformity of a program content with the rules on protection of minors and the conditions that make that content available (during the broadcast, the way of presenting etc..).

Program content unsuitable for minors under the age of 16 years must not be broadcasted before 22.00 or after 6.00 pm and unsuitable for minors under the age of

18, before 23.00 hours or after 6.00 pm. Program content unsuitable for minors under the age of 12 years may not be aired as part of the children's program. Mentioned program content also must not be advertised outside of time which is allowed to broadcast such content. Media service providers are required to notify the Regulator about complaints report about non-compliance with the rules on protection of minors. Media service providers are required to clearly indicate the programs that are able to endanger minors or are unsuitable for them, and to warn their elders. For the participation of minors in the audio-visual program it is required to have the consent of a parent, guardian or adoptive parent, which does not exclude the duty of broadcasters to pay special attention to the minor's participation in the program and does not exclude its responsibility for published content.

Audio-visual commercial communication

Audio-visual commercial communication shall be clearly identifiable. Covert audio-visual commercial communications are prohibited. Audio-visual commercial communications must not:

1) violate human dignity;

2) contain information that constitutes hate speech;

3) encourage behaviour that is detrimental to the health or safety of the people;

4) encourage conduct that disregards the environment.

All forms of audio-visual commercial communication recommending tobacco and tobacco products are prohibited. Audio-visual commercial communication recommending alcoholic beverages may not be explicitly intended for minors and must not encourage immoderate consumption of such beverages. Audio-visual commercial communications intended for recommending drugs, medical devices, healthcare services, professional medical procedures and methods of health care, including health services, policies and procedures of traditional medicine may be issued in accordance with the provisions of the law regulating the sale of drugs and the law governing health care. Telesales of medicines and medical resources are prohibited.

Audio-visual commercial communications must not:

1) encourage minors to behaviour that may harm them;

2) directly encourage minors to purchase or rental of goods or services by abusing their inexperience and credulity;

3) directly encourage minors to seek from of a parent or other person purchasing of goods or services that are being recommended;

4) abuse the special trust that minors place in parents, teachers or other persons,

5) unnecessary show minors in dangerous situations.

Providers of audio-visual media services can, with the consent of the Regulator, individually or jointly establish rules of conduct in relation to inappropriate audio-visual commercial communication, which is broadcasted immediately before, during or after the show – exclusively for children or the program that specializes for children, and which is intended to recommended food or drink containing the ingredi-

ents with nutritional or physiological effects of the excessive consumption of which is not recommended, in particular of fat, the trans-fatty acid salt / sodium or sugar. The provisions of this Article shall also apply to the media service radio.

Sponsorship

Sponsor must not influence the content of sponsored media services and program content, and in the case of television broadcasting and the distribution of their presentation, in a way which affects the responsibility and editorial independence of the media service provider. Sponsored media services and program content must not directly encourage the purchase or rental of goods or services, especially by promotional references to those goods or services. Sponsored media service or program content must include a notification of sponsorship and sponsor notification, specifying the appropriate name or sign sponsors, or by checking the names of its goods or services required at the beginning, and can during the emission, but not all the time, and at the end of sponsored programming. Media services and program content may not be sponsored by state authorities and organizations and political organizations. Media services and program content must not be sponsored by natural or legal entity whose main activity is the manufacture or sale of tobacco products or a person engaged in the production or sale of goods or services whose advertising is prohibited by ELC or any other law.

When the media service or program content is sponsored by natural or legal entity whose business includes the manufacture and sale of medical devices and health care provision, sponsored services or content may promote the name or the title the sponsor.

It is forbidden to sponsor news and current affairs television programme, except for sports news and weather forecasts. Specifying a character sponsor in children's and religious programming content is permitted only at the beginning and end of such content. The same provisions shall also apply to the media service radio.

It is prohibited to do marketing proliferation of goods. Exceptionally, the placement of goods is allowed only in feature films, television movies, fiction series, sports and entertainment programs, unless they are intended solely for children, as well as placement of certain services free of charge for their involvement in the program as props or prizes, and under these conditions:

1) if it does not affect the content and, in the case of television broadcasting, the broadcast schedule content which contain the placement of goods in a manner that endangers editorial independence of the audio-visual media services;

2) it must not at the show, which includes the placement of goods, in any way directly encourage the purchase, rental or use of the products or other services;

3) that goods, services, goods or service or other designation does not stand out inappropriately during the program, which includes the placement of goods, especially long-term close-ups of the goods which is the subject of the placement or by emphasizing its quality by managers, guests or other program participants;

4) contain a notice concerning the placing of the goods at the beginning or at the end of the program content, as well as after the advertising blocks, except if exceptionally program content in which are goods which are not produced or commissioned by the media service provider or a related party within the meaning of the law on companies,

5) The subject matter of placing the goods must be goods, services, goods, service or other designation which is television advertising is prohibited by this Act or any other law or bylaw.

The duration of the promotion of goods is not included in the duration of television advertising or teleshopping during one full hour of broadcast.

In matters relating to the content of audio-visual commercial communication, the regulations on advertising are implemented, unless is otherwise provided by ELC. Media service provider is responsible for the publication of audio-visual commercial communications whose content is contrary to the provisions of this or any other law or regulation that governs the content of audio-visual commercial communication, if it knew or on a regular basis of checking the circumstances of the case (e.g. Insight the content of the advertising message) should have known that its content is contrary to the above regulations, or if it was released without obtaining duly filled declaration.

The Regulator brings the general laws which establish detailed rules for carrying out the obligations laid down in Articles. 47-59 of ELC.

Register of media services

The controller maintains and regularly updates the Register of media services (hereinafter referred to as the Register). It shall contain in particular:

1) the name of the media service provider;

2) the title (name) of the media service provider and information about the service (name, tax identification number, address);

3) the number and date of issuance of the permit or the basis of service if it is provided without obligation to obtain authorization or permission;

4) the type of media services in accordance with Art. 43 and 44 of ELC,

5) the period for which the permit is issued;

6) information on the person responsible media service provider;

7) information on the measures imposed to media service provider;

8) Alert to the media service provider of the existence of violations of media pluralism.

Regulator *ex officio* deletes the service from the Register on the basis of its termination provision. The Register is published in accordance with the law.

The mandate of the person appointed or elected under the Broadcasting Act[14] until the entry into force of the LEC ceases upon the expiry of the period for which a person is appointed or elected.

Council members who are elected from a list of candidates proposed by the unique authorized proponents of Article 9 items 5) and 7) of LEC, will replace two

[14] Broadcasting Act, http://www.minoritycentre.org/library/broadcasting-act-republic-serbia-amandments.

members whose terms of office stops and who were elected on the proposal of the committee in charge of Culture and Information of the National Assembly at the last election of the members of the Council.

On the effective date of LEC Republic Broadcasting Agency which was established by the Broadcasting Law continues to work as a regulatory body for the electronic media in accordance with the provisions of ELC. Employees in the Republic Broadcasting Agency continue to work as an employee of the Regulatory body for electronic media, on matters on which they worked. Members of the Council of Republican Broadcasting Agency continue to work as members of the Regulatory Council.

Regulatory Council is obliged to harmonize the Statute and other acts within 90 days from the date of entry into force of ELC. Regulator creates new or updates existing registers, records and databases and prescribes forms for entering and editing data within six months from the date of enactment of ELC. Regulatory Council adopts general acts on the basis of ELC within six months from the date of its entry into force. Until the general laws are fully in charge it shall be applied general laws passed pursuant to the Act which shall cease to have effect on the date of entry into force of ELC, except the provisions of these acts, which are contrary to ELC.

Audio-visual politics

Audio-visual policy is one of the most important policies of the European Union. In March 2010, the EU has by the Directive 13/2010 of European Parliament and of the Council on the provision of audio-visual media services (AVMS Directive) established a new regulatory framework in relation to the provision of audio-visual media services. Considering that the Republic of Serbia has candidate status for membership in the EU, the Directive has imposed, to further the process of becoming a member, or of the accession of the Republic of Serbia to full membership in the EU, the need for harmonizing current legislation of the Republic of Serbia with the standards set forth therein.

In the above context, from of the international documents in the field, it should be noted European Convention on Trans frontier Television[15] of the Council of Europe (revised version), which entered into force on 1 March 2002, and ratified by the Republic of Serbia through the Law on Ratification of the European Convention on Trans frontier Television of 2009.[16]

So far, the current Broadcasting Act[17] was passed in 2002 year. As the system law in the field of electronic media, this law is substantially followed international standards. In the meantime, standards have improved, the practice of the law has shown some disadvantages, and the transition to a digital signal and the issue of the provision of audio-visual media services, in accordance with the aforementioned standards, led to the necessity and need for this law to be replaced by new one, which will re - "catch up" with the new time and issues in the field of electronic media.

The need for a fundamental redefinition and improvement of the electronic media, hence the adoption of the electronic media law as a fundamental law in this area, it

[15] See http://conventions.coe.int/Treaty/en/Treaties/Html/132.htm last accessed on 21.09.2014.
[16] "Official Gazette of RS" Nr. 42/09.
[17] "Official Gazette of RS", nr. 42/02, 97/04, 76/05, 79/05-second version, 62/06, 85/06 and 41/09.

was noted in the Strategy of Public Information System in the Republic of Serbia until 2016, by the Government of the Republic of Serbia adopted on 28. 09. 2011. Adoption of this strategy was one of the key conditions for the Republic of Serbia, through which on 01.03.2012. Serbia has earned candidate status for membership in the European Union. The Action Plan for the implementation of the Strategy, as one of the key activities, for whose execution was scheduled period of 18 months, provided the identification of the draft law regulating the field of electronic media. As part of these activities, it is specifically stated that the adoption of this law is necessary in order to align these areas with the EU Directive 13/2010 of the European Parliament and of the Council on the provision of audio-visual media services (AVMS Directive).[18]

In the design of the proposed solutions in this law it started from the following objectives:

1. needs to harmonize terminology and establish definitions of terms in accordance with the Directive on Audio-visual Media Services

2. necessity of normative regulation of the jurisdiction and duties of the regulatory bodies in the electronic media, especially considering changed circumstances that will occur by switching from analogue to digital broadcasting;

3. precisely defining the jurisdiction of the Republic of Serbia for audio-visual media services

4. guarantee the freedom of reception and retransmission of media services

5. purposes of defining and determining the type of audio-visual media services in accordance with the AVMS Directive EU;

6. precise definition of the obligations of providers of audio-visual media services (linear and on-demand)

7. definition of European audio-visual works and obligations to their impressions

8. precisely regulate access to events of major importance for public

9. establishing new, transparent process conducted by the regulatory body in the field of electronic media in connection with the issuance of licenses for the provision of media services;

10. protection of media pluralism;

11. Protection of minors

12. security requirements for adequate administrative and judicial protection in the event of violation of the rights of providers of audio-visual services and their punishment in case of non-compliance with the provisions of the proposed law.

Law on public service media (LPSM)[19]

Scope of the Law

This law (LPSM) governs, in accordance with European standards and international instruments in the field of electronic media, the work of public service media

[18] "Official Gazette of RS" Nr. 65/2011.
[19] "Official gazette of RS", nr. 83/2014.

and public media institutions, "Radio-Television Serbia" and public media institutions "Radio Television of Vojvodina", their activities and principles underlying the performance of activities of public interest that exercise transparency, election and authority, the adoption of laws, as well as providing the tools and the financing.

LPSM defines public service broadcaster in Article 2, it is an independent and autonomous entity that, the performance of its core business, to the public interest in the field of media, and provides a general and comprehensive media services that include informational, educational, cultural and entertainment facilities intended for all sections of society. Public service media are national and provincial public service broadcaster.

Republican public broadcaster is public media institution "Radio-Television Serbia" (hereinafter referred to as RTS), based in Belgrade. Provincial public broadcaster is public media institution "Radio Television of Vojvodina" (hereafter RTV), headquartered in Novi Sad. RTS and RTV cooperate in carrying out its core business.

The main activity of public service media is in the function of the public interest as defined by this law, and includes the production, purchase, processing and dissemination of radio, television and multimedia content, especially news, education, culture, art, children, entertainment, sports, religious and others who the public interest for citizens, aimed at the realization of human rights and freedoms, the exchange of ideas and opinions, cherishing the values of a democratic society, the promotion of political, sexual, ethnic and religious tolerance and understanding, and preservation of the national identity of the Serbian people and ethnic minorities as well as providing audio and audio-visual media services and publishing electronic editions as a service of public interest (Article 3 LPSM). In addition to the described, public broadcaster can perform commercial activities, which must not compromise the performance of the core business, such as:

1) the assignment of the right to public communication of radio, television, or other media contents;

2) The publication of advertisements or other forms of audio-visual commercial communications (e.g. Sponsorship, product placement, etc.)

3) the provision of interactive services that are related to media services or other interactive services;

4) organization of public performance of music contents and other events that are not part of public service media;

5) manufacturing, leasing and sales of phonograms and videograms;

6) the provision of technical services and rental production and other capacities;

7) other commercial activities that serve the performance of the core business, if they are on a smaller scale and usually performed by the activity (providing intellectual services, publishing, etc..).

The basic principles of public service media

The work of the public service broadcaster is based on the following principles (Article 4. LPSM):

1) true, unbiased, complete and timely information;

2) editorial independence;

3) independence of the sources of financing;

4) prohibition of all forms of censorship and unlawful interference in the work of public service media, editorial boards and journalists;

5) the application of internationally recognized norms and principles, in particular the respect of human rights and freedoms and democratic values;

6) compliance with professional standards and ethics.

In performing the basic activities of the public service broadcaster has institutional autonomy and editorial independence, and especially in terms of:

1) determination of the conception and determining program content, in accordance with the law;

2) editing program schedule;

3) organization of the activities;

4) selection of managers, editors in chief and employment;

5) purchase and sale of goods and services;

6) management of financial resources, in accordance with the law;

7) the preparation and execution of the financial plan;

8) the negotiation and preparation and signing of legal documents pertaining to business establishments;

9) election of representatives to legal matters and other legal matters.

In its action public broadcaster provides the public interest, upholding the requirements of the public for their actions and accountable to the public. Accountability of public service media to the public as well as the influence of the public on its operation is realized as:

- The publicity of appointment process for the bodies of public service broadcaster;

- Public participation in the improvement of radio and television programs;

- The obligation of public service media to promptly and accurately inform the public about the performance of their business, on the terms and manner of their services and other matters related to the activity for which it was established;

- Publication of the work plan, financial plan and report on the activities and operations;

- Submission of a report on the activities of public service media to the National Assembly and the Council of the Regulator;

- Timely fulfilment of obligations prescribed by the law governing access to information of public importance**.**

Public interest that is provided by the public service broadcaster

Public interest, in accordance with the law governing public information that the public service broadcaster is realized through its program content is:

1) truthful, timely, complete, impartial and professional informing citizens and allowing the free formation and expression of opinions of listeners and viewers in the Republic of Serbia, autonomous province and local self-government;

2) respect for and introduction of basic human rights and freedoms, democratic values and institutions and improving the culture of public dialogue;

3) respect for privacy, dignity, reputation, honour, and other fundamental rights and freedoms of man;

4) respect for and promotion of pluralism of political, religious and other ideas, and enable the public to become familiar with these ideas, not serving the interests of certain political parties and religious communities, as well as any other single political, economic, religious and similar viewpoint or interest;

5) meet the needs of information of all sections of society without discrimination, with particular attention to socially vulnerable groups such as children, youth and the elderly, minorities, persons with disabilities, socially challenged, etc..;

6) meet the needs of citizens for programs that ensure the preservation and expression of cultural identity to the Serbian people and ethnic minorities, taking into account that national minorities follow a certain program area and in their own language and script;

7) impartial processing of political, historical, economic, social, health, cultural, educational, scientific, environmental and other issues, allowing for equal presentation of different points of view;

8) free of charge and equal representation of political parties, coalitions and candidates who have confirmed their electoral list for the republic, provincial, or local election, during the election campaign;

9) affirmation of national cultural values of the Serbian people and ethnic minorities living in the Republic of Serbia, as well as convergence and interpenetration of their culture;

10) the development of media literacy;

11) domestic production of documentaries and feature programs;

12) timely information about current events in the world and the scientific, cultural and other achievements of civilization;

13) improvement of general education, health education and training relating to the protection of the environment;

14) the development of culture and artistic creativity;

15) fostering human, moral, artistic and creative values;

16) satisfying entertainment, recreation, sports and other needs of citizens;

17) informing our citizens abroad, as well as members of the Serbian people living outside the territory of the Republic of Serbia;

18) presentation of cultural heritage and artistic creation in the country and abroad;

19) inform the international public about events and developments in the Republic of Serbia.

In achieving the public interest public service broadcaster is obliged to:

1) takes into account the linguistic and speech standards of the majority population and, proportionately, of ethnic and national minorities in the area where the program is broadcasted as well as language and speech standards for deaf and people with hearing disabilities;

2) at the national, provincial and local levels using all their available capacities including correspondent network in order to realize the rights of all citizens to equal information;

3) ensure the use and development of modern technical and technological standards in the production and publication programs in the allotted time implementing plans for the transition to new digital technologies;

4) cooperate with other public service media and exchange program content that are of interest to the citizens of the Republic of Serbia;

5) to ensure preservation of radio and television media as a cultural heritage of national interest.

The public service broadcaster is obliged to use Serbian language in programs, the Cyrillic alphabet and sign language as a form of communication for deaf and people with hearing disabilities.

The use of Serbian language is not mandatory in programs intended for national minorities, but these programs can be subtitled in Serbian. The use of Serbian language and the Cyrillic alphabet is not mandatory:

1) if films and other audio-visual and radio work are in their original form;

2) musical works are published with text that is written in a foreign language;

3) if the programs are intended for learning a foreign language;

4) if these programs are intended for foreign nationals or citizens of the Republic of Serbia who live outside its territory that such programs can't be followed on the Serbian language;

5) if in the program, due to the credibility of information are published documents, name or a statement in their original form.

Public media service provides at least 10% of the annual program time or at least 10% of the annual program budget for the audio-visual works of European productions, with the exception of the time dedicated to news, sports events, games, advertising, teletext and TV sales. This share is reached gradually, in accordance with the provisions of the law regulating the electronic media, taking into account the obligation of public service media to ensure the public interest through informational, educational, cultural and entertainment facilities. Program content older than five years may make at the most a half of whole content. Program content of independent productions are selected on the basis of open competition. The process and criteria for selecting first mentioned program content shall be determined by the general act of public service media. Criteria for selection of first mentioned program content must be non-discriminatory and in accordance with program obligations under the law.

Advertising for the public service broadcaster is regulated by law that regulates the electronic media and advertising area. The public service broadcaster has the right to refuse publication of advertisements for content that is contrary to the programming obligations established by law, other rules and regulations governing advertising.

Establishment of Institutions of public service media

Chapter III establishes the institutions of public service media. RTS and RTV have legal status as legal entities. RTS provides media services at least two television programs and at least three radio programs on the territory of the Republic of Serbia. RTV provides media services at least two television programs and at least three radio programs on the territory of the Autonomous Province of Vojvodina. RTS and RTV offer media services like electronic publication on the internet. At least one television and one radio program of public service must provide general media services.

Public broadcaster can start providing new media services of radio or television broadcasting, television or audio or audio-visual media services on demand, if its overall impact on the market justified by the additional value in terms of fulfilling the democratic, social and cultural needs of the society and the curriculum requirements prescribed in the provisions of Article 7 LPSM. New media services, in terms of this LPSM, are services that are significantly different from the services that the institution of the public media service already provides in terms of content, approach, or a group of users who are assigned. Existing media service shall be deemed to new media service if it is modified to meet the criteria described in the preceding section.

Managing director of public service media determines the proposal for the introduction of new media services, which provides a clear and complete description of the new media services and justification for its introduction, technical conditions, an indication the group of users that is intended, a description of the funding and evaluation of the potential impact on competition in the relevant market for electronic media.

The proposal for the introduction of new media services is delivered to the Regulator for opinion in relation to the possible impact of new media services on competition in the relevant market. The controller analyses the potential impact of new media services on the relevant market in cooperation with the competent competition authorities. Regulator delivers the opinion to the public service broadcaster with a report on the analysis within 90 days of the submission of the proposal. Public media service organizes and conducts a public hearing on the proposal for the introduction of new media services that cannot be shorter than 30 days. After a public hearing, the Management Board of the public service broadcaster makes the decision on the introduction of new media services.

Public media service provides media services through operators of electronic communications networks for terrestrial broadcasting as well as through other operators providing service media content distribution. Conditions are governed by the distribution agreement.

Public media service is entitled to be provided, by the operator of electronic communications networks for terrestrial broadcasting, a good quality reception of analogue signals for at least 90% of the population and digital signals for at least 95% of the population in the area where the service is provided as a public service broadcaster and to provide capacity for multiplexes broadcasting and distribution of programs, technical requirements for broadcasting in standard and high-resolution images and

technical support to other technical and technological, program and service improvements with a payment service operator of electronic communications networks for distribution and broadcasting, in accordance with the contract. Public broadcaster acquires the right to provide media services directly under this Act and is not required to obtain a license for the provision of media services in accordance with the law regulating the electronic media.

The organs of public service media are the Management Board, Managing Director and Program Council.

Universal service obligations and other public rights and obligations

Public service Obligations

Concept and scope

Chapter X regulates the universal service. Article 55 defines the universal service. So, the basic universal services are:

1) access to a public communications network and publicly available telephone services at a fixed location, including data service that provides functional access to the Internet;

2) access to information and public telephone directories;

3) the use of public payphones;

4) free calls to emergency services;

5) special measures for persons with disabilities and socially disadvantaged users provide equal opportunities for access to publicly available telephone services, including making calls to emergency services, public service announcements and telephone directories.

Universal services are provided in a technologically neutral basis, with specified quality and at affordable prices, and to people with disabilities and socially disadvantaged users at affordable prices. Ministry, at the proposal of the Agency (with which the Agency shall provide an analysis of the provision of universal service in the Republic of Serbia, including the quality and cost of providing such services) shall prescribe the scope, geographic coverage and quality of universal service, as well as the requirements in terms of providing equal opportunities to use services to persons with disabilities, taking into account the level of development of public communications networks and the availability of publicly available electronic communications services in Serbia.

Designation of operators

The Agency shall designate one or more operators designated to provide some or all of the universal service, on the part or on the whole of the territory of the Republic of Serbia, in order to ensure coverage of the whole territory of the Republic of Serbia universal services. The operators are defined in an objective, transparent and

non-discriminatory manner, so as to ensure efficiency and effectiveness in the delivery of universal service and to the extent determined by the obligation which is not an excessive burden on the operators. These operators are required to make publicly available updated information about their services of universal service, including in particular data on the geographic availability, pricing, conditions of access and use (including limitations) and quality. The Agency shall specify the level of detail and manner of publication of such data.

Costing and financing of universal service obligation

The Agency is authorized to order the operator adjusting the offered price or conditions of use of the universal service in a manner that is transparent and non-discriminatory, in the case of the interest of providing equal opportunities for the use of persons with disabilities, and providing accessibility for vulnerable users. Agency verifies treatment operator with respect to certain obligations and analyses the provision of universal service in the Republic of Serbia, including the quality and cost of providing those services, at least once during a period of three years starting from the date of the act, and in accordance with established state decisions regarding the obligations of operators and proposing amendments act referred to in Article 55, paragraph 3 of the LEC. The aforementioned analysis is published on the Agency's website.

In order to protect LEC prescribes the determination of the excess costs of providing universal service. (Article 57). Operators that are designated for universal service providers are required to submit a report on the provision of universal service, no later than the end of the first quarter of the current year for the previous year. This report may contain a request for reimbursement of the excess costs of providing universal service (hereinafter referred to as excessive costs), along with documentation of costs that are excessive burden. The Agency shall specify the method of documenting the excessive costs and standards for the exercise of the right to compensation for excessive costs. Agency within three months from the date of receipt of the application operator and documents in accordance with the said act, shall issue a decision determining the amount of the excess costs.

Funds for reimbursement of excess costs shall be provided from funds that operators pay to fund the universal service on a separate account maintained by the Agency. Agency determines by the decision the amount of funds that operators pay to fund the universal service in the previous reporting period, in a way that is least damaging for market and to leverage market and in proportion to the operator on it, while the total amount of payments for all operators must match the total amount of excess costs determined solutions referred to in Article 57, paragraph 4 of the Law.

Protection of rights and subscribers broadcasting

This matter is regulated by chapter XV of LEC. The contract between the operator and the user is provided in art.105 of LEC. The mutual rights and obligations of operators and users shall be governed by the agreement, which is to be concluded

in writing. This contract, in addition to the elements provided by the law governing contractual relations, contains the following elements:

1) the specification of services (package contents), including in particular information about the possibility to make calls to emergency services, the conditions for access to and use of services (including limitations), the minimum level of service delivery and measures applied to prevent excessive network load, the time required for the commencement of service, the services offered maintenance and support, as well as limitations in the use of terminal equipment;

2) provisions on the treatment of personal data (especially in relation to public telephone directories), traffic data and location data, during and after the termination of the contractual relationship**;**

3) information on prices and tariffs, as well as the ways in which you can get current information about all applied tariffs, maintenance costs, as well as payment and additional costs related to the offered payment methods;

4) The term of the contract, and the conditions under which the contract is extended or terminated, including in particular the terms of services offered in connection with promotional benefits, fees associated with the transfer number, temporary suspension or permanent termination of services, or the termination of the contractual relationship, with and without the payment of expenses in connection with the termination (particularly with respect to terminal equipment);

5) Fees and conditions for the return of funds in the event of non-compliance with the agreed level of service quality;

6) the method for filing and resolving complaints;

7) the measures that the operator can be applied to maintain the security and integrity of their networks and services, as well as control of illegal content. These elements are contained also in the contract between the user and the operator (carrier) which doesn't provide access to an electronic communications network. The operator (carrier) is obliged to offer its services in a way that consumers are clearly and unequivocally informed of the terms of the contract (Article 106), and in particular the elements referred to in Article 105, paragraph 2 of LEC. Price list, depending on the types of services offered, includes: amount of one-off connection fees, the monthly fee for access to an electronic communications network or service, unit of account and tariff interval, description of the specific conditions for access to protected content and value added services, notification maintenance and service packages available, information about discounts and other terms specific to a particular service. The operator is obliged to make publicly available contract conditions and prices, in a convenient manner. The operator is obliged to without delay inform the subscribers about contract terms and conditions and prices, as well as any changes thereof in an appropriate manner and submit them to the Agency no later than the date of their entry into force.

Change of terms of the contract is stipulated by Art.107. The operator is obliged to, at least one month in advance; notify the subscribers of the intention of unilateral changes to the contract terms in appropriate manner, as well about the subscriber's right to terminate the contract before the expiration of the period for which it was

concluded. The subscriber shall be entitled, upon receipt of the notice, to terminate the contract without the obligation to pay the costs associated with the termination, if the announced unilateral changes significantly alter the conditions under which the contract was concluded, in a way that is not for the benefit of subscribers, especially as regards the specification of services (content package) and conditions for the use of services in connection with promotional benefits offered. The Agency may prescribe the content of notices under this section.

Operator (carrier) of services with added value is required to pre-publish a detailed description and cost of the overall service, and all of its component parts. The Agency shall specify the obligations of operators, particularly with regard to advertising services, methods of billing and collection services, methods of processing of personal data, traffic data and location data, control of illegal contents and resolving complaints, taking special care to protect the interests of users.

The Agency is, in order to ensure quality in the provision of publicly available electronic communications services and protect the interests of users, authorized to (art.109):

1) closely prescribe quality parameters of certain publicly available services, as well as a way to inform consumers about the quality of services offered;

2) determine the minimum quality of certain services for operator of a public communication network.

Operators of publicly available electronic communications services shall, within their technical capabilities, ensure equal access to their services for people with disabilities (art.110). The Agency may impose specific obligations to the Operator in terms of ensuring the availability of certain electronic communications services to persons with disabilities.

The Agency shall keep up to date database of prices, terms and conditions for access and use (including limitations), as well as the quality of public communications networks and services. Agency publishes and updates the information on its website with a comprehensive search capability.

Accounts with detailed specification broadcasting.

The operator is obliged to subscribers, upon request, to issue an invoice containing detailed specification of the services provided to the calculation of charges for each service, for easy verification and control costs of the services provided (art.112). The data do not include information about calls that are free, calls to emergency services, as well as information that is incompatible with the provisions of the law governing the protection of personal data.

Objection of subscriber to operator (carrier) (art.113) broadcasting

Subscriber may submit in writing a complaint to the operator the amount charged for the service or the quality of services provided, as well as to seek damages pursuant to the provisions of the contract on the provision of services with lower quality than agreed. Deadline for filing objections is 30 days from the date of obligation due from

the account for the service, in the case of an objection to the bill, which is 30 days from the date of service, in the case of an objection to the quality of service. Subscriber shall pay the undisputed portion of the bill, and if challenged the entire bill, he shall pay the monthly average price for the last three months preceding the period to which the complaint relates. Operator is not liable for damages if the quality of service provided is less than the prescribed or agreed due to objective reasons that could not be predicted, avoided or removed (*vis maior*), as well as the timely efforts of maintenance work, networks and services in terms appropriate circumstances. The operator shall, within 15 days of the filing of the complaint to the subscriber submit a response in writing, which will be set up to accept a claim for damages pursuant to the provisions of the contract on the provision of services with lower quality than the agreed or to refuse allegations in the complaint, stating the facts and evidence on basis of which the amount owed for services rendered or determined by the quality of services provided.

A subscriber whose objection is denied may apply to the Agency or another body to mediate in resolving the dispute out of court or initiate civil proceedings before the competent court within 15 days from receipt of the operator's response to the complaint, or within 15 days of the expiration of the period within which the operator was obliged to comment on the complaint. To subscriber who filed the complaint and orderly conducted obligation of payment, the operator shall not suspend service call receiving, calling emergency services, as well as to exclude the terminal equipment of the subscriber from its network, up until the deadline for the launch of extra-judicial or judicial proceedings or until the completion of extra-judicial or judicial proceedings.

Operator of publicly available telephone services shall, in accordance with its technical capabilities, to enable the subscriber, the easy way and free of charge:

1) To prohibit outgoing calls and sending e-mails when the monthly cost of such services exceeds a predetermined amount;

2) the prohibition of certain types of outgoing calls as well as calls or sending emails to certain types of numbers.

Operator offering Caller Line Identification (Call ID) is required to provide to the prevention of showing identification of individual outgoing call, a subscriber for all outgoing calls, in easy way and without compensation. This applies to outgoing international calls but does not apply to calls that are sent to emergency services. Operator has the right to temporarily suspend the previously mentioned ability to detect and prevent malicious or disturbing calls.

Operator offering Call ID is required to enable the subscriber off identifying incoming calls in a simple way and without charge for reasonable use of these opportunities; this also applies to international incoming calls. Operator offering Call ID is required to subscribers with an easy way to reject incoming calls with hidden identification, as previously this also applies to international incoming calls. Operator that provides service identification of established lines is required to enable the subscriber switching off of displaying caller identification established lines in a simple way and without compensation. Of course, this refers also to the international incoming calls.

Operator that provides service to Caller ID or established lines is obliged to publish information on the possibilities and limitations of this article.

Malicious or harassing calls broadcasting

Operator of publicly available telephone services to whom the subscriber in writing sends the compliant and describes the manner and content, a tentative date and time, about malicious or harassing calls, shall record and maintain records of the identification of the incoming call, the date and time of the call or call attempt (article 116). If the operator determines, on the basis of a compliant that malicious or harassing call has come from the number of its subscribers, it shall issue a warning to the subscriber or, in the case of repeated harassment and take other appropriate measures to prevent further harassment. If the operator determines, on the basis of an application that malicious or harassing call has come from the subscriber number of another operator's network, the operator shall forward a report of a disturbance to the operator whose subscriber has made it and that operator will send a warning or, in the case of repeated harassment, will take other appropriate action to prevent further harassment. Operators of publicly available telephone services are obliged to cooperate in order to monitor and detect malicious or disturbing calls, especially for the exchange of information and acting on complaints forwarded.

Stopping of automatic call divert broadcasting

The operator is required to enable the subscriber, in a simple manner and without charge, to stop automatic call divert, performed by the third party, to the terminal equipment of the subscriber.

Unsolicited messages broadcasting

The use of automated calling system and communication without human intervention, sending of fax, electronic mail or other electronic messages for direct advertising is permitted only with prior consent of the user or subscriber (recipient). So, according to art.118 of LEC, in force in Serbia is in the Opt-in system. If a natural or legal entity, when selling their products or services has obtained directly from the recipient – contact information and consent to the use of data for purposes of direct advertising, then it has the right to use them in order to direct their advertising similar products or services, provided that the recipient provide an opportunity for objection to such use of the contact data in a simple way and without compensation.

It is prohibited direct advertising which shows the incorrect or conceals the identity of the sender of electronic mail or other electronic messages, as well as direct advertising that does not contain the specified e-mail address or phone number through which the recipient can request, with no charge, to prevent further sending of advertising messages.

The operator is required to enable the subscriber filtering of unwanted and harmful e-mails, as well as an easy way to configure or disable the filter. Operator shall publish the e-mail address to complain of unwanted and harmful emails. Operator shall, upon receipt of proof of unsolicited and harmful messages that have been sent by its subscribers, establish the facts and, depending on the degree of abuse, warn subscribers or temporarily disable the use of the service and promptly inform subscribers of that. Operator has the right, in case of repeated abuses subscriber to permanently disable the use of the Services, or terminate the service agreement.

Personal data in the public telephone directory

Service providers of public telephone directories shall, with no charge, inform subscribers about the intention of including of their personal data in the publicly available telephone book in printed or electronic form, about the purpose of the book, the availability of personal data across service announcements, as well as possibilities for the search of personal data by the third parties via the search function in e-book form (Article 120). The subscriber shall be entitled, upon receipt of the notification, to refuse to consent on the inclusion of personal data in a publicly accessible directory. These obligations apply also to legal entities to the extent that they are not bound to make their phone number available to the public.

Service providers of public telephone directories shall facilitate to the subscriber, whose personal data are stored in a publicly accessible directory, means or ways to check on or update data, and provide the possibility of withdrawal of approval date, or to delete personal information from publicly available telephone directories, in a simple way and without compensation. These obligations apply to legal entities to the extent that they are not bound to their phone number is available to the public

Service providers of public telephone directory are required to obtain additional consent of the subscriber before enabling the use of data from the public directory for purposes other than to contact the subscriber via a personal name, or the name of the subscriber or the minimum of his other identity markers. This obligation applies to legal entities without restrictions

The availability of data in the public telephone directory

Operator that provides publicly available telephone services shall:

1) create and keep up to date public phone book (directory) with the data of its subscribers;

2) provide its customers access to information and public telephone directories.

The operator is obliged to meet all reasonable requests for access to information (referred to in paragraph 1, item 1) under conditions that are objective, non-discriminatory, in accordance with the provisions of this law and the law governing the protection of personal data. This obligation applies in particular to the requirements of providers of public telephone directory, which consists of comprehensive publicly available directories containing data on all subscribers of publicly available telephone services in the Republic of Serbia.

The Agency shall prescribe the requirements with respect to access to and use of this information.

Processing of traffic and location data

Operator of public communication networks and operator of publicly available electronic communications services, which processes and stores the data traffic of subscribers and users, is obliged to erase data or make unrecognizable person to whom the information relates, when the data traffic is no longer necessary for the transfer of communication, with the exception of (art.122):

1) data that is required for creating an account for services or interconnection, which can be processed until the expiration of the time limit prescribed by the law for claims or debt collection;

2) data which operator uses for advertising and sales services, with the prior consent of the person to whom the data relate, and also to provide added-value services, the time and extent necessary for those purposes;

3) The data to be retained in accordance with the provisions of LEC.

The operator shall, prior to commencement of processing of traffic data from point 1) of Article 122, as well as prior to obtaining consent from point 2) of this Article, inform the subscriber or user of the types of data to be processed, as well as the duration of treatment. A person who has given consent to the processing of data from point 2) of this Article shall have the right to revoke consent at any time. Processing of traffic data must be performed only by persons for purposes of the operator performing tasks of issuing bills, managing network traffic, answering customer questions, detecting fraud, advertising, and sales of electronic communications services, as well as providing added-value services, to the extent necessary for the performance the activities.

Described provisions do not apply to the ability of the Agency and other competent state authorities to make insight into the details of network traffic that are relevant to the determination of disputes, especially regarding bills for services or interconnection.

Operator of public communications networks and publicly available electronic communications service may process the data on the location of the user, which are not data traffic, only when the parties to whom the data relate so are made unrecognizable or with their prior consent for the purpose of providing added-value services, in the extent and the time required for this purpose (art.123). This provision does not refer to the location information to be retained in accordance with the provisions of this Act. Operator shall, before obtaining the consent of users and subscribers, inform them about the types of location data that will be processed, the purpose and duration of the processing and whether the data will be sent to third parties for the purpose of providing added-value services.

A person who has given consent to the processing of data has the right to revoke consent at any time. The operator is obliged to provide to the person, who has given consent to the processing of data, the opportunity to temporary refuse a location information procession every time they connect to a network or transmission of communication, in a simple way and without compensation. Processing of such data described on the site must be performed only by persons authorized operator, or authorized persons of the third party providing the value added services, to the extent necessary for the provision of value added services.

Security and integrity of online public communication network services

Chapter XVI handles the security and integrity of public communications networks and services. The operator shall, for the purpose of ensuring the security and integrity of public electronic communication networks and services, confidentiality of communications, and protection of personal data, traffic and location data, the application of

appropriate technical and organizational measures appropriate to the existing risks, particularly measures to prevent and minimize the impact security incidents on users and interconnected networks, as well as measures to ensure the continuity of public communication networks and services. If the operator provides the service using an electronic communications network, associated facilities or services of another operator, it is obliged to cooperate with that operator in ensuring the security and integrity of public communications networks and services. When there is a particular risk of security breaches and integrity of public communications networks and services (unauthorized access to significant data loss, jeopardizing the confidentiality of communications, the security of personal data, etc.), the operator is obliged to notify subscribers of that risk and if that risk is beyond the scope of measures that the operator is obliged to enforce, inform subscribers about possible security measures and costs in connection with the implementation of these measures (art.124).

The operators are obliged to inform the Agency of any violation of the security and integrity of public communications networks and services, which has a significant impact on their work, particularly on breaches that had resulted in violation of the protection of personal data, or privacy of a subscriber or user. The Agency is authorized to inform the public about security breaches and integrity, or ask the operator to do it itself, when the Agency assesses that the disclosure of such information in the public interest (art.125).

Privacy of communication electronic and lawful interception and retention of data

Chapter XVIII handles the confidentiality of electronic communications, lawful interception and data retention. Confidentiality of electronic communication is treated by art.126. Interception of electronic communication that reveals the content of the communication is not permitted without the consent of the user, except for a limited time and order of the court, if it is necessary to conduct criminal proceedings or protect the security of the Republic of Serbia, in the manner provided by law. This provision shall not prevent the recording of communications and related traffic data, which is performed for evidence of commercial transactions or other business relationship, in which both parties are aware or ought to be aware of, or are expressly cautioned that the communication can be recorded. Use of electronic communications networks and services for storage, or accessing data stored in the terminal equipment of a subscriber or user, is permitted provided that the subscriber or user is given clear and complete notice of the purpose of collecting and processing data in accordance with the law governing the protection of data personality, and that he was given the opportunity to refuse such processing. This does not prevent technical storage or access to data in order to ensure communication within the electronic communication networks or services that the subscriber or user has explicitly requested.

The operator is obliged to provide lawful interception of electronic communications prescribed in Article 126, paragraph 1 of the LEC (art.127). The competent national authority in charge of affairs of lawful interception shall keep records of intercepted electronic communications, which specifically includes determining of

act which constitutes a legal basis for carrying out the interception, date and time of intercept, and this track is kept as a secret, in accordance with the law governing the confidentiality of data. When the competent authority conducting the affairs of lawful interception is not able to carry out lawful interception of electronic communications without access to the premises, electronic communications networks, associated facilities and electronic communications equipment operator, the operator (referred to in paragraph 1 of this Article of LEC) shall keep record about received requests for interception of electronic communication, which specifically includes the identification of the authorized person who performed the interception, determination of the act which provided the legal basis for carrying out the interception, date and time of intercept, and that this record is kept secret, in accordance with the law governing the confidentiality of data. The operator is obliged, in order to achieve this commitment, at its own expense to provide the necessary technical and organizational requirements (equipment and software), as well as evidence thereof to the Agency, in accordance with the provisions of LEC.

Ministry, after obtaining the opinion of the ministry of Justice, Ministry of Internal Affairs, the Ministry of Defence, Security and Intelligence agencies and bodies responsible for the protection of personal data, shall prescribe requirements for devices and software referred to in paragraph 4 of this Article as well as the technical requirements for the fulfillment of obligations retention of Art. 128 and 129 of LEC.

Administrative Charges

Article 29 of LEC determines fees for use. The fee is payable for:

1) The use of numbering;

2) The use of radio frequencies;

3) The performance of electronic communications;

4) Provision of the services of the Agency.

The amount of the fee is determined by the MB of the Agency. This document must be approved by the Government. This act is always published on the Agency's website.

The fee for the use of numbering is determined depending on the type of service provided using the assigned numbering or purpose for which is used the assigned numbering and special technical requirements relevant to its use (internal numbering, addressing in electronic communication networks, the commercial exploitation of the assigned numbers and also, keeping in mind the need to ensure introduction of new services, market competition and rational use of numbers. Fee for the use of numbering is paid by the operator, or the holder of a license for numbering use, in the amount determined on an annual basis, by a decision by the Agency and which determines the manner of payment of such fees.

The fee for the use of electronic communication shall amount to a maximum of 0.5% of the operator's revenue from the activity of electronic communications, according to the type of electronic communications networks or services in accordance

with the financial plan of the Agency. Compensation for the performance of electronic communications is paid by the operator, and the amount is determined on an annual basis, through a decision by the Agency and on the manner of payment of such fees.

Fees for the provision of the Agency shall be determined by the type of services provided by the Agency in accordance with LEC (issuance and renewal of licenses for the use of numbering and individual licenses for use of radio frequencies, conformity assessment, technical inspection), taking into account the costs of the Agency to provide these services.

REGULATION OF COMPETITION IN THE ICT MARKET

Application of competition law to the ICT market

In this area there has been for a while at force Law on protection of competition (LPC) published in "Official Gazette of the RS", no. 51/2009 and 95/2013[20]. It is prescribed by that law regulates and is applied to all natural and legal entities who, directly or indirectly, permanently, temporary or on one-term basis participate in trade of goods and services, regardless of their legal status, ownership, citizenship or state affiliation. Also, this law shall be applied to acts and practices performed on the territory of the Republic of Serbia, as well as on acts and practices performed outside of its territory that affect or could affect the competition on the territory of the Republic of Serbia. LPC therefore must be implemented at ICT market. Only specificity is area of implementation, so the pocedure for all stakeholders and consumers would be the same, but acting authority must account the specific rules of trade. It is defined by LPC what can be considered as Affiliated undertakings, and relevant market by articles 5 and 6. The main definition of this law is competition infringement and it (article 9) shall include acts or actions of undertakings that as their purpose or effect have or may have a significant restriction, distortion, or prevention of competition. It also provides restrictive agreements definition and prohibition of restrictive agreement (provides also Conditions for exemption from the prohibition art.11- 14). Institutes also tackled by this law include: definition of the dominant position on the market (art. 15), concentration of undertakings (art.17) exceptions of concentration of undertakings abuse of a dominant position (art.16), permissibility of concentration[21]. In special LPC introduces and regulates activities and powers, competencies commission for protection of competition. It also gives procedures for the process at the commission (ex officio acting, acting by the request of a party, summary procedure), decisions enacted by the commission. LPC proscribes obligations for various parties in implementing the law such as: obligation to provide requested information (art. 48), cooperation of state authorities and organizations (art. 49) cooperation with the police is separately stipulated (art.50) and it is predicted in a form of assistance.

Special provisions on procedure related to competition infringement are introduced by LPC: authorizations in inspections (art.52), dawn raid (art.53), entering the premises (art. 54), temporary seizure of documents and belongings (art. 55). Commission is powered by taking interim measures (art. 56), administrative measures (art. 57), and measures for removal of competition infringement (art. 59).

[20] It is accessible in English at http://www.kzk.gov.rs/kzk/wp-content/uploads/2011/07/law-on-protection-of-competition2.pdf.

[21] Further regulation of this area is done by regulation on the content and manner of submitting notification on concentration "Official gazette of the RS", no. 5, January 25, 2016. Can be accessed at http://www.kzk.gov.rs/kzk/wp-content/uploads/2016/11/01-Regulation-on-the-content-and-manner-of-submitting-notification-on-concentration-20161.pdf last time accessed 17.02.2018.

LPC provides measure for protection of competition and relief from measure for protection of competition and even procedural penalty measures (art. 68, 69, 70).

Against the final decision of the Commission LPC proscribes Judicial review of decisions of the Commission (art. 71) a claim may be submitted before the court within 30 days from the date of service of the decision to the party, competence of the Administrative Court as a court of appeal.

Operators with significant Market Power

Markets eligible to prior regulation and obligations of operators with significant market power

Introduction

Chapter XI of LEC prescribes markets susceptible to ex ante regulation and obligations of operators with significant market power (OCMP). Determination of markets susceptible to ex ante regulation is defined in Article 59. Market subject to ex ante regulation is that one where there are structural, regulatory and other permanent barriers that prevent the entry of new competitors, where it is not possible to ensure development of effective competition without regulation and where the deficiencies can't be remedied only by the application of the competition rules (hereinafter: the relevant market). The Agency determines the relevant market with the implementation of relevant recommendations of the European Union's markets susceptible to ex ante regulation.

Agency at least once every three years, performs an analysis of the relevant market (hereinafter referred to as market analysis), and if necessary, additional markets, with the implementation of relevant recommendations of the European Union on market analysis and the determination of significant market power OCMP. In the process of market analysis agency cooperates with the agency responsible for the protection of competition. Agency publishes on its website this Report on market analysis.

The criteria for the determination of operators with significant market power (OCMP) are regulated by Article 61 of the Law. Operator has significant market power in the relevant market, if you own or together with other operators in a dominant position, or a position that allows it to significantly behave independently of its competitors, its subscribers and ultimately consumers. In determining individual significant market power in particular are taken in account:

1) the size of the operator and its competitors, particularly in terms of number of customers and revenues in the relevant market;

2) control of the infrastructure of which the volume can't easily be replicated;

3) technological advantage of the operator that enables superior position in the market;

4) lack of or low level of bargaining power of buyers;

5) easy or privileged access to capital markets or financial resources;

6) the degree of diversification of products or services (e.g. Related products or services);

7) economies of range;
8) economies of scale;
9) the degree of vertical integration;
10) a high degree of distribution and sales network;
11) lack of potential competition;
12) the existence of barriers to the spread.

In determining the common market power, in particular it is taken into account:
1) saturation of the market;
2) stagnant or moderate growth in demand;
3) low elasticity of demand;
4) the homogeneity of the product;
5) the similarity of the cost structure;
6) the similarity of market share;
7) lack of technical innovations and technologies developed;
8) lack of excess capacity;
9) high barriers to entry;
10) lack of bargaining power of buyers;
11) lack of potential competition;
12) the existence of various informal or other links between operators;
13) the possibility of applying countermeasures;
14) lack of or limited space for price competition.

In the determination of significant market power on the relevant market for particular operator there can be determined its significant market power even on the closely related market, if the links between these markets are such that power from one market can be transmitted to the closely related market in a way that strengthens the market power of the operator.

The process of operators with significant market power determination is defined in Article 62. When the Agency, based on previously conducted market analysis, is to determine the absence of effective competition in the relevant market (as well as the closely related market), by the decision determines the operator which, individually or together with other operators, in this market has significant market power. Through this decision of the Agency when determines operator with OCMP also determines at least one obligation under Article 63 of this Law, taking into account the type and nature of the deficiencies identified in the market, previous investments, encouraging further investment and opportunities for return on investment at a reasonable rate considering the associated risks. In the process of making the decision Agency invites all interested parties to provide their views of the importance of determining the obligations of operators with OCMP and, if necessary, seeks the opinion of the authority responsible for the protection of competition. The Agency shall monitor the implementation of obligations under the operator with OCMP and ex officio review is a decision for at least a period of three years from the date of, and in accordance with established state decisions regarding the obligations of operators with OCMP.

This Decision shall expire on the date of entry into force of the Act on the Agency's determination of the relevant market, if by that decision is not determined to be subject to ex ante regulation of markets in which the operator has previously been declared as an operator with OCMP.

Duties of operators with significant market power

Obligations of operators with significant market power are defined by Article 63. The actual decision of Agency determines the operator with OCMP, also determines obligations for it in:

1) publication of certain data;
2) non-discriminatory treatment;
3) accounting separation;
4) facilitating access to and use of network elements and associated facilities;
5) price control and cost accounting application;
6) providing a basic set of leased lines;
7) providing opportunities for the selection and pre-selection operators;
8) the provision of retail services under certain conditions.

The obligation to publish certain information (Article 64.) specifically refers to the accounting information, technical specifications, network characteristics, conditions of supply and use (including limitations), period of validity of offers and prices in relation to interconnection and access services. Operator with OCMP to which is determined by decision obligation of non-discriminatory treatment, shall, at the request of the Agency, within 60 days of receiving the request, prepare and publish a reference offer for interconnection and access. Operator with OCMP in the relevant wholesale market when accessing to network elements and associated resources, shall, at the request of the Agency, within 60 days of receiving the request, prepare and publish a reference offer for unbundled access to the local loop. The standard offer, which contains the previously described, shall be made in accordance with the needs of the market and includes a description, technical and commercial conditions for interconnection and access and unbundled access to the local loop. Standard Offer must be broken down into individual components to an extent that allows to the interested operator selection between specific components offers, with no obligation to accept the other components of the offer, which does not need to provide a service that is the subject of interconnection and access.

The Agency shall prescribe the minimum content, level of detail and manner of publication of the standard offer. If the operator fails to comply with the Agency's request or if the Agency determines that the standard offer is not made in accordance with the said Act, the Agency shall provide and publish a reference offer for interconnection and access and unbundled access to the local loop.

Nondiscriminatory action obligation

An obligation of non-discriminatory treatment is defined in Article 65 LEC. Obligation of non-discriminatory treatment refers to the equal treatment of operators with

OCMP in the provision of interconnection services and access in comparable circumstances. Operator with OCMP shall, in accordance with its obligation under paragraph 1 of Article 65, provide services to other operators under the same conditions and with the same quality as it does for its own purposes, or for purposes related entities or partners.

Article 66 defines what is meant by the obligation of accounting separation. Obligation of accounting separation refers to the separate accounting of the business activities of operators with OCMP in relation to the provision of interconnection services and access. Way of applying separate accounting shall be determined by the decision of determining operators with OCMP. The Agency is authorized to request from the operator with OCMP, and its related entities, to publish their wholesale and internal transfer prices, in particular for the fulfilment of obligations of non-discriminatory treatment and prevention of undue cross-subsidization. The Agency is authorized to, especially in order to check the fulfilment of the obligation to publish certain data and non-discriminatory treatment, ask from the operator access to the concluded contracts, accounting data, including data on revenues earned in the market, and that the information revealed, if it would contribute to the development of effective competition, ensuring that important not to jeopardize business operators.

Obligation to provide access to and use of network elements and associated facilities is defined in Article 67 LEC. Obligation to provide access to and use of network elements and associated facilities related to the compliance with the reasonable requests of other operators for access to and use of specific network elements and associated facilities operators with OCMP. This obligation is determined especially if it is established that the denial of access, undue conditionality or similar restriction of the operator with OCMP, would prevent the development of competition at the retail level, or would jeopardize the interests of end users. In determining liability, the operator with OCMP may be ordered to:

1) allow another operator access to specific network elements and associated facilities, including access to passive network elements and unbundled access to the local loop, particularly to enable the selection and pre-selection and offering of services provided through the local loop;

2) negotiate in good faith with the operator who requires access;

3) don't negate already granted access to network elements and associated infrastructure;

4) to provide certain services to other operators under wholesale terms;

5) Allow free access to technical interfaces, or other key technologies needed to ensure interoperability of services or virtual network services;

6) provide collocation or other form of joint use of related assets;

7) provide the services needed to ensure interoperability of services to connect end-users, including intelligent network services or roaming on mobile networks;

8) provide access to operational support systems or similar software systems, to ensure fair competition in the provision of electronic communications services;

9) provide interconnection networks and associated facilities;

10) provide access to related services, such as services based on information about the identity, location and availability of the user.

These measures may be supplemented by additional requirements in terms of good faith, fairness and timeliness. In determining the measures specifically takes into account the proportionality of commitments, in particular the price:

1) the technical and economic viability of using or installing assets of another operator, in terms of market development and the nature of interconnection and access, including the viability of other means of providing access, such as the use of conductive pipes and channels;

2) the feasibility of allowing the proposed approach, compared to the available capacity;

3) the initial investment of the owner of assets, taking into account the investment from the budget and the associated risks;

4) The need for long-term protection of competition, particularly economically effective competition on the level of infrastructure;

5) protection of intellectual property rights;

6) obligations under the relevant international agreements.

In determining the obligations, the Agency may provide technical and organizational requirements on the OCMP operator and operators seeking access from it and use of the network elements and associated facilities, when necessary to ensure the smooth functioning of the network.

The obligation of price control and the application of cost accounting (Article 68) refer to the application of the prescribed mechanism for reimbursement of costs and price control operators with OCMP, including the obligation of cost price grounding and application of cost accounting in relation to interconnection and access services. This obligation is determined especially if it is found that the absence of effective competition provides the operator with OCMP to maintain unreasonably high prices or low prices squeeze out competitors to the detriment of end users. In determining liability, the operator with OCMP can be ordered:

1) the application of a specific mechanism for reimbursement or methodology for determining the price, in a manner that ensures efficiency, sustainable competition and consumer welfare, while it can take into account prices on comparable markets, as well as the retail prices of operators with OCMP;

2) adjusting the price of services;

3) The obligation to apply cost accounting in order to control the price.

In determining the measures, particular attention is paid on previous investments of operators with OCMP, encouraging further investment opportunities and return on investment at a reasonable rate considering the associated risks.

Operator with OCMP bears the burden of proving that the price of its services resulting from the costs, including return on investment at a reasonable rate, and shall, at the request of the Agency, submit a detailed justification of its price.

In determining the cost-effective provision of services, the agency may apply a different methodology of cost accounting from those applied by the operator with OCMP.

If for the operator with OCMP is determined obligation by agency's decision of the cost accounting application in order to control prices, the Agency shall determine and publish the manner of application of cost accounting, which contain at least the main

groups of costs and rules of distribution of these costs, and hire an independent auditor to annually verify OCMP operator`s compliance for cost accounting with prescribed method of application of cost accounting. Auditor's report is published on the Agency's website.

The obligation to provide minimum set of leased lines (Article 69) refers to the duty of operators with OCMP in the relevant market for leased lines to provide to other operators lease of the part or all of the basic set of leased lines, on the part or on the whole of the territory of the Republic of Serbia.

The Agency shall define the scope and content of the minimum set of leased lines. In determining liability, the operator with OCMP establishes the method of providing minimum set of leased lines, so that in particular is ensured non-discriminatory provision of services, cost price foundation, as well as disclosure of information on the technical, pricing and other terms of supply and use.

The obligation to provide opportunities for the selection and pre-selection operators (Article 70) refers to the duty of operators with OCMP in the relevant market access to the public telephone network at a fixed location, to its subscribers with access to the services of any interconnected operator of publicly available telephone services, and on the following manner:

1) providing a choice of operators, using the prefix choice operator during each call;

2) providing a pre-selection, with the possibility of circumventing a pre-dialing prefix choice operator during each call.

In determining liability, the operator with OCMP can be obliged:

1) The obligation of the cost price of services being based interconnection and access, which are a function of service selection and pre-selection;

2) adjusting the level of direct costs related to the subscriber using the service selection and pre-selection, so there are disincentives for the use of these services.

The obligation to provide retail services under certain conditions (art.71) refers to the duty of operators with OCMP in the relevant retail market, to provide retail services under the prescribed conditions. This obligation is determined when it is estimated that the determination of other obligations under Article 63 of this law would not be effective. In determining this obligation, given the nature of the lack of the relevant market, and the need to protect the interests of end-users and encourage effective competition, the operator with OCMP can be obliged:

1) prohibition of calculating excessive fees, prohibition of interference with market entry or restrict competition too high or low prices, a ban on giving an unfair advantage to certain end users or prohibition of unjust binding of certain services;

2) limiting the amount of retail price, determination of control measures individual tariffs, as well as the obligation of establishing prices on the cost of providing services or prices on comparable markets.

If to the operator with OCMP is determined some of the retail price control obligations, the Agency also establishes the obligation of the application of cost accounting in order to control the cost, with also established and published way of the application of cost accounting, and Agency also hires an independent auditor to annually verify compliance cost accounting of the OCMP operator with prescribed method of application of cost accounting. Auditor's report is published on the Agency's website.

LEGAL STATUS OF OUT-OF-COURT DISPUTE SETTLEMENT IN THE ICT SECTOR

Those procedures are provided firstly by Law on obligations, and of course Law on civil procedure. But more theoretically this matter is stipulated by Law on mediation (Official gazette of RS no. 18/2005) and it is tackling it by areas. Area of pre-trial situation through articles 8-10, and those after complaint filed and by court accepted in articles 12-16. In Article 17 it deals with this area but also refers to secondary implementation of Law on obligations and Law on civil procedure.

LEGAL STATUS OF STANDARDIZATION

The first form of institutionalized standardization activities in the former Kingdom of Yugoslavia was established in 1939.

Throughout the history the Institute for Standardization of Serbia (ISS) has changed its legal status and official name on several occasions. In this regard, the Institute for Standardization of Serbia is the legal successor of the Institution for Standardization (2006-2003), Federal Institution for Standardization (2003-1978), Yugoslav Institute of Standardization (1978-1962) and the Federal Commission for Standardization (1962-1946).

Pursuant to the **Law on Standardization** („Official Gazette of the Republic of Serbia"No. 36/2009) and the **Decision on Amending of the Founding Act of the Institute for Standardization of Serbia** („Official Gazette of the Republic of Serbia" No. 88/2009) the Institute for Standardization of Serbia is the only recognized national standards body in the Republic of Serbia, a legal entity which operates in accordance with the regulations governing the legal status of public services. The founder of the Institute is the Government of the Republic of Serbia.

The Institute represents the interests of the Republic of Serbia in the following international and European organizations for standardization:

- International Organization for Standardization (ISO), where ISS is a full member since 1950;
- International Electrotechnical Commission (IEC), where ISS is a full member since 1953;
- Worldwide System for Conformity Testing and Certification of Electrotechnical Equipment and Components (IECEE), where ISS is a full member since 1965;
- European Committee for Standardization (CEN), where ISS is s a full member since January 1, 2017;
- European Committee for Electrotechnical Standardization (CENELEC), where ISS is s a full member since January 1, 2017;
- European Telecommunications Standards Institute (ETSI).

In addition, the Institute is also engaged in activities regarding the accession of Serbia to WTO.

Institute for standardization of Serbia has a status of National organization for standardization in European Telecommunications Standards Institute (ETSI). In that sense ISS has the obligation of implementing of European standards published by ETSI. In the monthly bulletin of ISS there is a section in which are published standards previously published in ETSI, in order for all national organizations for standardizations to take them and publish in their own countries.

PART II

PROTECTION OF INTELLECTUAL PROPERTY IN THE ICT SECTOR

APPLICATION OF COPYRIGHT IN THE AREA OF ICT

General Statement

At the international level, this matter is governed by the Berne Convention (for the Protection of Literary and Artistic Works)[1] of 1886. Changes were made in Paris in 1896 and Berlin in 1908. First completed in Bern in 1914, the Convention was revised in Rome 1928.god. Brussels in 1948. Stockholm in 1967 and in Paris in 1971 up to in 1979 when it was changed by amendments. And as one of the major shortcomings of the Convention were its unregulated Internet and information and communication technologies, which resulted in the adoption of the WIPO (The World Intellectual Property Organization Copyright Treaty) in 1996. The World Trade Organization as one of the conditions for membership requirements of the future Member States is obliging to adopt the provisions of the Berne Convention and that they are an integral part of the Agreement on Trade-Related Aspects of Intellectual Property Rights. In addition to the Berne relevant to the matter also is Rome Convention on the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, which was opened for signature on 26 October 1961. when it was adopted by members of BIRPI[2] – WIPO[3] predecessor. Also of importance in this area is the Geneva Convention on the Protection of Producers of Phonograms against Unauthorized Duplication of 1971 on the treatment of copyright protection in respect of sound recordings. This Convention has given the opportunity and the power to take action against imports of piracy in the form of unauthorized created music recordings as well as people who distribute them and resell. WIPO administers 24 Conventions, agreements and protocols of which Serbia is a signatory to all. UN has included the organization as a specialized international organization within the UN. This organization has confirmed its importance and expanded the scope of its importance by signing an agreement in 1996 with the World Trade Organization (WTO).

Intellectual property and copyright

The development of information technology, internet, digital world and cyberspace brought many challenges traditional concepts in many areas of the law, to that even the intellectual property and copyright are not an exception.

[1] Since 2008 this Convention has164 signatories. Text of the Convention is accessible on internet address: http://www.wipo.int/treaties/en/ip/berne/index.html last timeaccessed 25.01.2014.

[2] United International Bureaux for the Protection of Intellectual Property, more at stable internet address: http://en.wikipedia.org/wiki/BIRPI poslednji put pristupljeno 24.01.2012

[3] Convention Establishing the World Intellectual Property Organization signed in Stockholm 14. July 1967. Stable Internet address : http://www.wipo.int/treaties/en/convention/trtdocs_wo029.html , 25.01.2014

The term "intellectual property" is defined in the convention establishing the world intellectual property organization. The convention was adopted 1967 and later amended in 1979. article two of the convention provides the definition of intellectual property rights as related to: — literary, artistic and scientific works, — the interpretation of artists and performers, phonograms and radio and TV broadcasts, — inventions in all fields of human activity — scientific discoveries, - industrial design — factory, trade and service marks, and trade names and trademarks — protection against unfair competition and all other rights relating to intellectual activity in the industrial, scientific, literary and artistic fields."[4]

The term intellectual property refers to creations of the mind, by which this term primarily includes inventions, literary and artistic works, symbols, names and images used in commerce. Intellectual property is not a concrete, material ownership of an object, but the right and set the powers of the legal system of the country recognized to the holder of intellectual property rights. These rights are powers of the authors, inventors and other intellectual property holders. Intellectual property is unique, as it is the result of personal creativity and innovation. it can be any activity in any field of life: the invention in any field of technology, the name under which the product is sold or offered services, poem, painting, film, and the like. In almost every single case, intellectual property stimulates progress, transforming society and adding value to our lives.[5]

Intellectual property is divided into two categories: industrial property and copyright. Industrial property includes patents for inventions, trademarks, industrial designs and geographical indications and designations of origin and topography of integrated circuits. Copyright as a concept arose in the 18th century with an idea to protect the rights of authors, because the books were reprinted without the author's consent and without payment of compensation to the authors. Copyright was first protected in the printing industry, and later expanded to all the other works of authorship. Within the intellectual property, some authors singled out the database as a new sui generis field of intellectual property.[6] Today, the concept of copyright does include copyright and related rights.

Copyright and Related Rights

The term author's right is characteristic of European law. In common law uses the term copyright (copyright). The main difference between the two terms is that copyright is essentially a personal right of the author based on the relationship between the author and his work, and the copyright strictly refers to the work as such. authors right includes, but is not limited to literary works (such as novels, poems and dramas),

[4] *Convention establishing the world intellectual property organization*, internet address: http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?doc_id=131054&file_id=190032#p50_1504 , last accessed 22.11.2020.

[5] *Protection of Intellectual property in Serbia*, internet address: http://www.scribd.com/doc/56780927/zasitita-intelektualnesvojine, last accessed 20.02.2014.

[6] Koumantas Georges, *Reflections on the concept of intellectual property*, in: intellectual property and Information Law, Kluwer, 1998, pp. 41. Jehoram Tobias Cohen, *Copyright in non-original writings past - present - future?*, in: Intellectual Property and Information Law, Kluwer, 1998, pp. 108.

scholarly works (monographs, articles, lectures), films, musical works, artistic works (such as drawings, paintings, photographs, choreography, sculpture, etc..), reference works, newspapers, advertisements, maps, technical drawings, computer programs, databases and work of architecture.

Laws in some countries define author's right as a right of authors of literary, scientific, professional and artistic works.[7] In addition to the author's first, there are rights related to copyright or author's right. it can be referred as — copyright law related rights are the rights and scope of the legal protection of artistic expression, and the protection of organizational, business, and financial investment in the construction, manufacturing, distribution and broadcasting of copyright works, and include:

- the rights of performing artists on their performance;
- the rights of producers of phonograms on their phonograms;
- the rights of film producers (manufacturers videogram) on their videograms;
- the rights of broadcasting organizations on their programs;
- the rights of publishers on their publications;
- the rights of database producers on their databases.

Law on Copyright and Related Rights (LCRR) in Serbia under related rights includes "the right of performers, producers of phonograms the right film producer (manufacturer of videograms), the right of broadcast, the right of database producers, and the right of publishers that includes two basic rights: right the first publisher (part of which is in the public domain, which has not previously been issued) and the right publisher of printed editions of the special compensation."[8] Copyright and related rights are essential to human creativity, the authors provide an incentive in the form of recognition and monetary compensation, on the other hand provide them with a level of security that their work can be distributed without fear of unauthorized copying or piracy, and if this occurs, they are certain that they were determined to copyright.

Holders of copyright and related rights

The copyright holders (of author right) are called creators of works protected by copyright, and their heirs and successors. Copyright holder is a natural person–the author – who has created an original intellectual creation (copyright act), which has originality and a certain form. Author is entitled to a copyright on his work, the act of creating the work without complying with any formalities such as registration or deposit works. The author is considered to be a person whose name, pseudonym or mark in the usual manner is put on copies of the work until the contrary is proved. If there are multiple authors participated in the development works it is a work of authorship. If the work was done so as indivisible whole, the co-authors who participated in the creation of works of his creative contribution, have a joint copyright on the created part. If two or more authors compile their work for their common use, each author retains the copyright on his works.

[7] *LCRR*, Official gazette of RS nr. 104/2009, 99/2011 i 119/2012.
[8] Ibidem.

Holder of related rights may be any natural or legal entity, other than the rights of performers, which, by its nature, belongs to the natural person to perform the work of a literary or artistic fields or expressions of folklore.

User related rights can be: a performer (actor or musician) for performance of his work, the producer of sound recordings (on cassette tapes, compact disks, etc.) for their recordings, and broadcasting organizations in their radio and TV programs, film producer, the producer database, and so on.

Contents copyright

Contents of author's rights is usually determined by national legislation in this area, and it is usually the law on author's rights (copyright) and related rights.[9] Based on this law, "copyright holders" shall have the exclusive right to use or authorize others to use the work under agreed conditions. Carriers (carriers) of the right to work (or object of the author right) can prohibit or authorize: its reproduction in all formats, including print and audio clips; his public performance and communication to the public; its broadcasting; its translation into other languages; and its adaptation, such as the novel, which transposes the script for the film. Many types of works are protected under the Law on copyright and related rights, require mass distribution, communication, and serious financial investment for their successful dissemination and marketing (for example, publications, sound recordings and films), so authors often cede rights to their works to companies that will best be able to develop and place the work in the market, asking in return benefits in the form of payments and / or royalties (fees based on a percentage of income that brings work, or lump-sum compensation).

Copyright or author's right is consisting of:

- moral rights - protecting the personal and spiritual connection the author with his work,
- economic rights - protecting the property interests of authors regarding the use of his work,
- other authors' rights - protecting the interests of the other authors in terms of his work.

The moral rights of authors include:

- The right of publication - the author has the right to decide when and how his work is to become accessible to the public,
- The right to authorship - the author has the right to be recognized and identified as the author of a work (paternity right), and any person who publicly uses a copyrighted work is required to adequately indicate the author of the work (for example on the graphics published works on the program of the concert performance parts, etc..), unless the author has stated in writing that he would not be listed.
- Right to respect the author's work and honor or reputation of the author – the author has the right to object to any distortion, mutilation or other modification

[9] Ibidem.

of his work (right of integrity),[10]2 and any use of the part prejudicial to his honor or reputation (the right to reputation),

- Right to repentance – the author has the right to revoke the right to use the work and to prevent its further use with compensation to such right, if further use of harm to his honour or reputation. This takes into account the fact that the work was a reflection of the author's personality, which means that the author is provided with a legal possibility to specifically affect the future use of their already published or order parts. Right of repent lasts through the author's life and he (or she) cannot give up of that.[11]

Property rights are the exclusive rights of authors, because the author can authorize or prohibit the use of his work in any way. This confirms the absoluteness (acting towards everyone) economic rights, which include in particular the right of reproduction, distribution rights (trafficking), the right of communication to the public and the right to change. It includes all forms of exploitation of works copyright in which is expressed the need to protect the property interests of authors. Property rights of author's rights are manifested in particular as:

- the right of reproduction (right of multiplication) – the right of making copyright work in one or more copies, in whole or in part, directly or indirectly, temporarily or permanently, by any means or in any form.
- distribution rights (the right of trafficking)[12] and rental – the right to distribute is the exclusive right to put into trafficking the original or copy of the work by sale or otherwise. Rent means lending the original or copies of a work for a limited period, in order to achieve direct or indirect economic or commercial advantage, and the right administration of the copies of the lease.
- the right of communication of copyright works to the public include:
- the right of public performance (e.g. performing live at the event or concert, reciting or playing and singing)
- the right of public presentation of stage works (e.g. stage performance of dramatic works in the theatre)
- the right of public transmission performance or presentation (e.g., when the piece of music that is publicly performed live in a concert hall, at the same time communicate to the public outside of the hall by the speaker or on your screen)
- the right of public communication of a fixed part (e.g. playing music from CDs through music and CD player),
- the right of public presentation,

[10] 1) to object to any change of his (or her) work by unauthorized persons; 2) to object to public interpretation of his (or her) work in changed form or uncompleted form, minding concrete technical form of interpretation and good business practice; 3) to give permission for changing his (or her) work. (art.17).

[11] In LCRR these rights are enumerated as following: right of paternity, right of assigning author's name, right of publishing, right of protecting the integrity of art work (consisting of three rights – prohibition of changing, confronting and objecting to public interpretation of work in changed or incomplete form, permission to change the work of intellectual property) right to object on immoral exploitation of work, (endangering of honor and reputation of the author), while right to repentance is not prescribed within articles related to moral rights, but in a part related to publishing contract.

[12] This right of trafficking is incorporating: 1. Right of offering in order to sell. 2. right of storing specimens of work in order to trafficking.

- the right of radio diffusion broadcasting
- the right of radio diffusion retransmission (when the act in which the primary broadcast of one of broadcasting organizations both in full and unaltered is re-broadcasted via cable networks or by other broadcasting organizations),
- the right of public communication radio diffusion broadcasting (cases of public broadcast such as when in public catering establishment music is played from the radio or television without entry fee)
- the right of making available to the public (right of communication to the public via the Internet or other similar global digital network).
- the right of change - the exclusive right to translate, adapt, music processing, or any other modification to the author's work.

The so-called rights of the author towards the Owner of copyright works are rights that carry resemblance both to the economic and moral rights, and cannot be classified into any of these categories. These include the right of succession (the right of author on the appropriate share of the purchase price, for each time the resale of his original art works that followed after the first selling of works by the author, under certain conditions) and other authors' rights (the right of access to work, right to ban the public display of works – copy of a work of fine art, as well as pre-emptive right of modification of a work of architecture, the authors' right to remuneration for the lending).

The copyright owner has the exclusive right to reproduce the copyrighted work, to process it and on that ground create a new copyrighted work, to distribute copies of copyright works, to perform the work of authorship, or represent him in public. Any person who uses any of these rights, without permission, violates the copyright of the author, except in cases where it can be qualified as fair use of copyright works, or in cases where the copyright has expired and the author's work became public domain.[13]

Works of authors (Copyright)

Copyright work is an original intellectual creation in the literary, scientific and artistic domain, which has an individual character, regardless of the manner or form of expression, type, value or purpose. Thus, the essential characteristics in order to be considered an act of copyright are:

- intellectual originality (creative) achievements or achievements of the human spirit of creativity - originality (originality) in terms of copyright law does not require absolute novelty, but it is required so called subjective originality (originality), or a novelty in a subjective sense. Work is considered to be subjective if the original author does not imitate other work he knows and which carries a "personal touch" of the author.
- literary, scientific, artistic or professional work area - above phrase is the copyright considerably wider meaning than in the theory of literature mean literary works, and art history of art.

[13] Overbeck Wayne, Belmas Genelle, Major Principles of Media Law, Stamford: Cengage Learning, 2011, p. 238.

Copyright protection is ensured to the expressions, including visible form of some ideas that can be achieved by using different means of expression, such as written or spoken word, body movement, and sound, as a different two-dimensional or three-dimensional form.

Copyright works are in particular:

- linguistic work (written work, voice work, computer programs) - e.g. novels, poems, manuals, newspaper articles;
- musical works, with or without words;
- drama and drama-musical works;
- choreographic and pantomime works;
- Fine art (the fields of painting, sculpture and graphics), regardless of the material they are made, and other works of fine art;
- works of architecture;
- works of applied art and industrial design;
- photographic works and works produced by a process analogous to photography;
- audiovisual works (cinematographic works and works created in a manner similar to cinematographic creation) - Usually films;
- cartographic works;
- Reviews of scientific or technical nature, such as drawings, plans, drawings, tables, etc...

Translations, adaptations, musical arrangements and other alterations of works which are original intellectual creations of individual character, are protected as independent works.

Translations of official texts in the domain of legislation, administration and judiciary are protected unless made for the purpose of officially informing the public as such.

Collections of independent works, data or other materials such as encyclopedias, collections, anthologies, electronic databases and the like, that by the selection or arrangement of their constituent elements make their own intellectual creation of their author, are also protected as such.

Folk literary and artistic creations in their original form are not subject to copyright, but their communication to the public remunerative as the communication to the public of protected copyright works.

What is that that defines author's work in any national legislation in particular, in Serbia law system, according the Law on Copyright and Related Rights "original intellectual creation, expressed in some form, regardless of its artistic, scientific or other value, its purpose, size, content and as a way of expressing the permissibility of public communication of its contents."[14]

This law particularly stated that as works of authorship are considered:

- written work (books, brochures, articles, translation, computer program, in any form of their expression, including the preparatory materials for their production, etc..)

[14] *LCRR, art.2.*

- voice work (lectures, speeches, sermons, etc..)
- drama, drama-musical, choreographic and pantomimic, as well as works that originate from folklore;
- a piece of music, with or without words;
- filmmaking (cinema and television);
- the work of fine art (paintings, drawings, sketches, prints, sculptures, etc..)
- work of architecture, applied art and industrial design;
- cartographic work (geographic and topographic maps);
- plan, sketches, models and photographs; and
- theatre directory.[15]

Importing of specimens of work

Copyright restrictions

In the case of any form of exploitation of copyright works under the provisions of this law on the restriction of copyright it must be front stated: the author's name and the source from which the work is taken (publisher of the work, year and place of publication, magazine, newspaper, television or radio station where the act or section works originally published or directly taken, etc..).

In each case, the extent of the exclusive rights must not be in conflict with a normal exploitation of the work or not unreasonably prejudice the legitimate interests of the author. There are cases of suspension of exclusive rights and rights to compensation. Without permission and without paying copyright royalties published work can be copied and publicly disclosed for the purpose of proceeding before a court or other governmental agencies or for the purpose of ensuring public safety.

Also, it is permissible, under reporting to the public through the press, radio, television and other media on current events, to the extent appropriate for the purpose and manner of reporting on current events, without permission and without paying royalties:

1) reproduction of copies of published works that appear as part of the current event that is being reported on; and applies to all forms of public communication of these acts;

2) the preparation and reproduction of short extracts or summaries of newspaper and other similar articles in the press reviews;

3) multiplication of political, religious and other speeches at public meetings held in public bodies, religious institutions or in national or religious ceremony;

4) free use of daily information and news that are of the nature of a newspaper report.

It is allowed without the author's permission and without paying royalties for non-commercial purposes of instruction:

[15] *Ibidem.*

1) public performance or presentation of published works in the form of direct teaching in the classroom;

2) public performance or presentation of published works on school events, provided that the performers receive remuneration for their performance and not be charged an entrance fee;

3) public disclosure of school shows broadcast by technical devices within an educational institution.

It is allowed without the author's permission and without paying any fees to reproduce works by public libraries, educational establishments, museums and archives, for their archival purposes, if the work is multiplied from your own copies and if such duplication of these institutions does not intend to exercise direct or indirect material gain.

With the described it is allowed to a natural person without the author's permission and without paying royalties to reproduce copies of the published work for personal non-commercial purposes, which does not exclude the application of Article 208, paragraph 1, items 4 and 5 of LCRR.

The copies may not be sold or used for any other form of public communication. This does not apply to:

1) shooting (filming) performance, presentation and display of the work;

2) three-dimensional realization of plans for works of fine art;

3) the construction works of architecture;

4) construction of new buildings modelled on the existing building, which is the copyrighted work;

5) computer programs and electronic databases;

6) reproduction of written works in the scope of the whole book, unless copies of the book sold out for at least two years;

7) reproduction of music sheet with written music in notes other than manually rewriting.

The authors have compensation, under the provisions of Article 39 LCRR, for use of the work in the manner specified in fore mentioned lines.

If the work was a computer program, a person who has lawfully obtained a copy of a computer program that, for their own usual use, it is allowed to, without permission and without paying royalties:

1) place the program in the memory of a computer and run the program;

2) to eliminate errors in the program, and to make other necessary changes in it that are consistent with its purpose, unless the contract provides otherwise;

3) to make one backup copy of the program on a physical carrier;

4) make a decompilation of the program solely in order to obtain information necessary to achieve interoperability of the program with other independently created software or some hardware, provided that the information was not otherwise available, and that decompilation is limited only to that part of the program, which is necessary to achieve interoperability.

Data obtained from Section 4 shall not be disclosed to others or used for other purposes, in particular for producing or selling another computer program that would

infringe the copyright in the first. This action may be made directly to the person who has lawfully obtained a copy of a computer program or other qualified person acting on his orders.

It is allowed, without the author's permission and without paying royalties, to temporary reproduce of copyright works under the following conditions, if:

1) reproduction is transient or incidental;

2) multiplication is an integral and essential part of the technological process;

3) the purpose of reproduction is to enable data transmission in a network between two or more persons through an intermediary, or to allow the legal use of copyright works and

4) there is no duplication of independent economic significance.

It is allowed without the author's permission and without paying royalties to reproduce, as well as other forms of public communication of short excerpts of the author's work (the right of quotation), or individual short works of authorship, under the following conditions:

1) that the work is published;

2) that the said parts or short work, without modification, are integrated into other work if it is necessary for purposes of illustration, certificates or references, along with a clear indication that this is a quotation in accordance with fair practice;

3) to a suitable location specify who is quoted author, the title of the cited work, when and where he cited work published or issued, if the data is known.

Broadcasting organization which has a broadcasting license for the part is permitted without the author's permission and without paying royalties to record work with its own funds to on media for storing image or sound and media for storing both images and sound in order to broadcast that in its own show. This clip of work of copyrighted material must be removed no later than 90 days after the broadcast works. The recording can be saved in the official public archives, if it has a documentary value.

Work recorded in accordance with the descriptive circumstances cannot be rebroadcast without permission of the author.

It is allowed without the author's permission and without paying royalties making a two-dimensional reproduction, distribution of the copies in that manner produced, and other like forms of public communication, which are permanently on display in the streets, squares and other public places.

For the purpose of public exhibition catalogues or public sale it is permitted, without the author's permission and without paying royalties, to do proper reproduction of exhibited works and the trafficking of copies made in that way.

In shops, fairs and other places where there it is held demonstration of equipment for recording, playback and transmission of sound and images, is permitted without the author's permission and without paying any fees to reproduce works on a sound and pictures, public presentation of works from the tray, and presentation of the broadcasted work, but only to the extent necessary to demonstrate the operation of the device. Recording made in this way must be promptly deleted.

For persons with disabilities, it is allowed without the author's permission and without paying royalties, reproduction and circulation of the author's work, if the work does not exist in the form requested, if its use is directly related to the disability of the person and to the extent that requires certain type of disability, and if copying and circulation has been done in order to achieve direct or indirect financial gain.

It is allowed free processing (in sense of changing it) of the published work of authorship if it is: 1) a parody or caricature, if it does not create confusion or may not lead to confusion regarding the source of the work;

2) processing part for personal purposes and which was not intended for and is not available to the public;

3) processing in conjunction with the permitted use of the work, which is caused by the nature or manner of such use.

Authorized user of a database or its amplified copies may freely reproduce or processing of this database, if it is necessary for access to its content and the regular use of such content. If the user is authorized only for a part of the database, he (or she) is allowed to copy and alter only the portion for which authorization is. Contract provisions that are contrary to the above conditions are null and void.

Published works that are not important ingredient in relation to the main work in which they are involved, or in relation to the main thing with which they are used together, are in the free use of the exploitation of such capital work or thing like that.

Without permission and with obligation for payment of royalties, is permitted to make reproduction on paper or a similar medium, photocopying or any other form of photographic or similar techniques that give similar results, in the form of a collection intended for teaching, examination, or scientific research, excerpts of published authors acts of individual short published works of authorship in science, literature and music, or disclosed individual works of photography, fine art, architecture, applied art, industrial and graphic design and cartography in the case of public works of several authors, unless the author explicitly does not prohibit that. This does not apply to music sheet, notes on paper.

Without permission and with obligation of royalties' payment, it is permitted reproduction, distribution of copies in the mass media, as well as other forms of public communication of articles that have been published in other media, provided that these articles refer to the current economic political or religious issues, and the author didn't explicitly prohibit.

Without permission and against payment of royalties, it is allowed to make the three-dimensional reproduction of works that are permanently displayed in the streets, squares and other public places, as well as the circulation of such copies, unless:

1) the copy of a sculpture gets a casting from the original mold, from which the copy that will be permanently displayed at an open public place or from a mold made by casting the sculpture;

2) If a building is modeled on the existing building;

3) The product is formed on a work of applied art.

Copyright infringement in cyberspace

Peer to peer file sharing

File sharing in cyberspace today is the most common threat to copyright. Known case of "Napster" in 2000 is famous now. Napster is a "peer to peer" service for sharing music files, it has allowed millions of users to share mostly copyrighted music files. This of course led to numerous court cases, Napster went bankrupt, but the number of such services in cyberspace has increased to unimaginable proportions. These services even today offer not only music files, but also all other files, the files of music tracks, video clips, movies, and all files to various kinds of software and computer programs.

The company Apple has in 2003, in an agreement with the companies in the music industry and with respect for copyrights, sat up its own service for sharing music files "iTune" intended for users of its products su as: "iPod" - music player, "iPhone" - a mobile phone, and today "iPads "- tablet computers.

Google has organized a digital library of books in which there is a huge number of digitized books, but the company did not have the approval of a number of authors for digitization of their books, so in dispute of leading publishers against Google in 2011 the court ruled that Google is obliged to reimburse the authors.[16]

Digital Rights Management

Digital rights management (Digital rights management, DRM) is a term used to describe technologies that control access to information in the digital world by publishers or copyright owners to narrow use of digital content. It's just another form of copyright protection and is a digital lock of intellectual property that would not be stolen. A typical practical example of digital rights management is iTunes software, property of American company Apple. This type of digital asset management is supported by a number of international legal instruments. In technological terms, digital rights management provides control over the use of digital media by restricting access, copying or conversion to other formats by end users. Opponents of the concept of digital rights management argue that this aspect of digital control prevents users from doing something which is entirely in accordance with the law: e.g. making copies of CDs or DVDs for personal needs, that access works in the public domain, to use the material for research and educational purposes, in accordance with fair use. These arguments go along with the thesis that the digital rights management is in violation of applicable copyright laws.

It is important to emphasize the difference between analogue and digital recordings. Analogue audio or video recordings on vinyl, magnetic tape, audio or video tapes stored signal as a continuous wave as opposed to a digital signal (either an audio or video signal) that is used today, which actually consists of data as a kind of combination of numbers: ones and zeroes.

In the case of analogue recording, it is a physical recording of the medium (the board or tape), and in the case of digital recording is about writing data in some form of computer memory. analogue media can't be copied without loss of quality, and quality

[16] Overbeck Wayne, Belmas Genelle, *Major Principles of Media Law*, Stamford: Cengage Learning, 2011, p. 281.

of the analogue media is lost even by ordinary normal usage, and the digital material can be copied without loss of quality, and they do not lose quality due to use. Analogue recordings can be converted to digital images by a simple method by everyday computer user.

Digital rights management technologies are used primarily in the entertainment industry (music, video, e-books, computer games, TV and radio broadcasting, etc...). This technology is based on contracts with a limited license on which users must agree in order to have access to a web site or to download the appropriate software. This technology is to control access to and reproduction of information online, and even copying for personal use.

Public Domain

Question of the public domain or public ownership is one of the commonly argued issues related to intellectual property. Today public domain means public ownership of intellectual property. It's a legal institute of common law and indicates the knowledge and innovation in relation to which no person or other legal entity can't (or will not) to establish or maintain proprietary interests, and these authors' works and innovations are part of the common cultural and intellectual heritage of humanity that, in principle, anyone can use or exploit. In historical sense the public domain is preceded protection of intellectual property. At first all of cultural and scientific works presented the public domain, so that only the development of the printing industry and market made laws on the protection of copyright. The concept of public domain is shaped by the end of the 19th century. Victor Hugo, French writer, in 1878 determined by two main features of the public domain: first the work after it was revealed by author is not anymore only his property but belongs to the human spirit, becomes a social public good, and second that is for sure the fate of intellectual work is that one day it will become a public good. The Berne Convention of 1886 calls on the public domain to which belongs works that have no copyright protection of law.[17] Public domain as argument is often used by many critics of the current system of intellectual property protection. The issue of public good is also dealt within the World Intellectual Property Organization, as well as many politicians and governments. Many projects of digitization of cultural heritage are based on public domain.[18] No permit is required to copy, use or distribute material that is part of the public property regardless of the purpose or purposes no matter private or commercial (industrial). This is what you can do for free, without obligation, permanent or temporary rental license and the like. The public domain can be defined as the opposite of other forms of intellectual property, public domain, stands opposite trademarks (currently accepted term "trademark"), patents and the like. For the material under "public property" there is no law that keeps it from use by members of the society. It can be argued that material that is the subject of public property serves as the basis for new creative work.

In defining the concept of public property it can be said that this is what belongs to all people. When using the work, which is part of the public domain, one does not

[17] Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet address: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr. pdf, 6.11.2010.
[18] *Ibidem.*

have the obligation of referring to the original author, although it is considered polite and fair relationship. However, it should be borne in mind that although the permitted use of creative works in the public domain, as well as his, alteration, improvement and/or incorporation into other works, this does not mean that the new work that may occur on this occasion is a public property, it may contain parts that fall within the domain of copyright law, it may be the property of the author who created it, and if it is not clearly stated that this new work the author put into the public domain should be assumed that there are some rights reserved. In the story of Copyright the central attention is given to the exploitation of labour, but they never regulate access to and use of the work while in the public domain in the forefront is the possibility of intellectual access to works in the public domain.[19] Copyright should achieve a fair balance between the rights of authors to control the dissemination of their work and the public interest that the work is more spread and be available to as many people.[20]

A public good is generally defined as a material that is not subject to copyright, or materials for which the copyright has expired, ceased to exist. Public ownership refers to the complete absence of copyright protection works or intellectual property that is not controlled by anyone. Materials, labour declared as public domain or the property, can be considered as a part of the "public cultural heritage," every member of society is encouraged to use it for any purpose, including copying, modifying, improving, even it can be sold or used for commercial purposes. Copyright work becomes part of the public domain, either when the original author of the work has put it at the disposal of society, when consciously, voluntarily and irrevocably waives right to it, which as the author of works deserve, or more often when the right to copy and use any part expires, or when the work of intellectual property reaches a certain age, or when the original author or owner of the rights does not extend the right or give them up. Copyright works and innovations can be found in the public domain in a variety of ways:

1. Absence of legal protection because they were creative works that were created before the enactment of legislation in this area (of William Shakespeare, Ludwig van Beethoven, Archimedes inventions, etc..), meaning the protection of work of intellectual propriety; folk proverbs, traditional folklore; works which cannot be determined who the author is, uncreative works which because of a lack of creativity do not fall under the protection of copyright law (mathematical formulas, judicial decisions, legislation, intuitively organized collection of data, alphabetical lists, search results, etc..).

2. Upon the expiration of the legal protection. Most of copyrights have a shelf life and when it comes to pass that limit – work or patent enters the public domain. When it comes to patent that term is usually 20 years and for the copyright it is needed to fulfil several conditions. These conditions are that the work is published before 1.1.1923. or at least 95 years before January 1 of the current year, that the copyright owner has died at least 70 years before January 1 of the current year, that no state party to the Berne Convention on copyright law did not set a permanent copyright on a particular work, or that the United States and the EU are not brought a legal act to extend the duration of copyright.

[19] *Ibidem.*

[20] Dworkin Gerald, Judicial Control of Copyright on Public Policy Grounds, in: Intellectual Property and Information Law, Kluwer, 1998, pp. 137.

3. Waving of legal protection. By the Copyright law, the United States puts all work created by the United States Government to be placed in the public domain. Some institutions and authors can give up of legal protection and transfer its work to the public domain using the example of the GNU Free Documentation License, free software license, "copy left" license or "Creative Common 0" license. In case where the author of the work consciously, voluntarily and irrevocably puts his work into the public domain, by that he (or she) waived any right he had over that work and can't later (in the case of an estimate otherwise) revoke or restore the rights of the respective part. This means that at the time of placing the work he (or she) was aware that his work could (and is going to) be used without any compensation from anyone and in any manner. For example, the authors of the works which have put their works into the public domain before 20-30 years probably could not even assume that their work could be used in a medium such as the Internet and in the ways and purposes for which they are used. UNESCO Recommendation of 2003 relating to universal access to cyberspace within the definition of the public domain are included the public data and official information generated by governments and international organizations and with that they voluntarily allow access to all.[21] Practically, it can be said that material declared as a "public good" is actually a material with zero license. Waiver of present and future copyright can be based on legal regulations of the American legislation, which regulates the "public domain". Under Serbian law, such a possibility as the transfer of copyright or waiver of all copyright does not exist.[22] The significance of the public domain has a large number of reasons: education, democratic, economic and free competition. This role is of equal importance as the role of the existence of copyright, as it allows cultural diversity, freedom of creation, innovation, culture, and science. Powerful and strong public domain of culture and science facilitates to the creation of the cultural heritage of mankind and the availability of this wealth to everyone. That is the main driver of social and economic development and protects against privatization, encroachment and a balance in relation to the existence of exclusivity of intellectual property.[23]

Great threat to the public domain represent attempts to create a monopoly by using digital technology methods of restricting access to digital content. Digital rights management is a term that covers several different systems and mechanisms for global control of content. In other words, DRM is supposed to provide legislative foundation to control systems that allow complete control of digital content, any use that is in question. An early example of a DRM –encrypted DVD content as encoded by a specific encryption key which is owned by the DVD Forum and kept in secret, and manufacturers of DVD players must sign certain contracts to be able to play encrypted DVD content. This is just one example of how DRM laws hinder the free exchange of contents, so you can often hear that the abbreviation DRM supposed to mean Digital Restrictions Management.[24]

[21] *Ibidem*.

[22] Creative Commons, Internet address: http://creativecommons.org.rs/faq. 6.11.2010.

[23] Dworkin Gerald, Judicial Control of Copyright on Public Policy Grounds, in: Intellectual Property and Information Law, Kluwer, 1998.

[24] Jelić Ivan, Zajednica u savremenom informatičkom društvu, 2006, Internet address: http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf , 4.11.2010.

Copyright Works in Cyberspace

Written works of art - author copyright in cyberspace, novels, books and similar work of art, Literature and related works

"The written works are... the works of authorship, expressed in the language of writing."[25] This simple definition gains in importance nowadays and is further complicated when it comes to written works in electronic form, those who are eligible to be published and/or interpreted in whole or in part in a digital environment. Electronic publishing of copyright works is imprecise and unclear term, but may involve a range of diverse activities that lead to the same goal - the presentation of an author's work to a wider audience, in digitized (electronic) form. Some of these activities are producing, selling, renting or making available otherwise physical objects that contain the copyrighted work in digitized form; transmission of copyright works in digitized form via electronic communication (e.g. downloading from the Internet, e-mail communication, etc.) and transmission of copyright works by means of electronic communication.[26] Of course, each of these activities can be done with the knowledge and permission of the author, or without it (illegal). Written works are no exception to this practice – while the legal descriptions of activities are called electronic publishing, other illegal option is one of a kind "piracy". According to Article 2 of the Berne Convention, the term "literary and artistic works" shall include all creations in the literary, scientific and artistic fields, regardless of the manner of their expression. Literary works are thus classified into one of the main categories of creativity and those works that are protected by the copyright regime. Among the literary forms – accurate to say written – works specifically mentioned books, pamphlets and other writings, other works of the same nature. The term "literary and scientific works" is not precise enough. Also, literary works definitely can be scientific. Many forms of written expression do not have to be literary – talks and discussions from the above examples. Finally, there are forms of literary and scientific expression which surely enjoy copyright protection and are not listed – they are for example computer programs, which will be discussed later, as well as a variety of other forms of research and research results. On the other hand, the newly posted member 2bis of Berne Convention leaves the possibility for States to explicitly deprive copyright protection to certain forms of written expression – political speeches, and submissions made during court proceedings. They may be part of the written work if it were published or made public in writing, but may be the sermons, orally presented work. In connection with the article 10bis of the Convention, which does not take away the possibility of copyright protection of works that deal with the current economic, political or religious matters, but allows for the possibility that such acts of transfer, in example citation by other publications (including electronic) without the express permission of the author, or something like that will be possible only if the author didn't expressly forbid that. And this is the logical consequence of the purpose of creation of such written works - all these works that deal with the current

[25] Vidoje Ž. Spasić, Autorska dela u digitalnom okruženju, Niš, 2011, p. 83.
[26] David Bainbridge, Introduction to Computer Law, Pearson Education Limited, London, 2000, p. 74.

socio-political issues have emerged that the analyses and conclusions expressed in them as efficiently and mass transfer.

Berne Convention also allows two exceptions, typical for written works. In fact, it is possible to cite a written work without the express permission of the author if such a practice is common and if it is consistent with the objective to be achieved; also, it is possible without special permission from the author to use his written works in the teaching process. Of course, in both cases it is necessary to explicitly specify that the work in question is copyrighted, as well as the author of the cited work - so, those citing rules must be consistently followed.[27] Although these exceptions are logical and desirable, the question arises whether the usual practice involves specifying copyrighted works (with proper citation), also to the works that are published electronically, or on the internet? It seems that the answer must be yes, and practice clearly indicates it. The purpose of the exception is scientific training, scientific research, and education – the means which lead to the desired goal (electronic or traditional) are not and cannot be subject to a special regime if it is already allowed such a use of written works. In addition to these previously clarified exceptions, articles 11bis – 12 of the Convention are quite explicit: the authors of written works alone have the right to approve (or not) any reproduction of their works, including electronic versions of the work, performed in whole or in part, as also any modifications, adaptations, and the processing (changing) of these works (this is usually the general regime applicable to all copyright works unless applied some exceptions). What is also particularly important in relation to the analysis of cinematographic works is that the authors of written works shall enjoy the exclusive right of authorizing adaptations of their works in cinematic purposes.[28] LCRR in Article 2, paragraph 2, item 1 states that as a form of copyright works and written works, and among them particularly stands out (but are not limited) books, pamphlets, articles, translations, computer programs in any form of their expression, including the preparatory material for the preparation of these written works. Thus, the LCRR is more modern than the text of the Berne Convention and it recognizes computer programs as a form of written works of authorship. In Section 6 of the LCRR elaborates the solution for in Article 2bis. Berne Convention, so as to specifically deprive the copyright status of the work: laws, rules and regulations; Official materials of state authorities and bodies performing a public function; Official translations of regulations and official materials of state authorities and bodies performing a public function; pleadings and other documents in administrative or judicial proceedings. Interesting is also the first paragraph of this article, according to which the protection of copyright shall not apply to general ideas, procedures, methods of operation or mathematical concepts as such, as well as the principles, the principles and guidelines contained in the work of authorship (they refer to each author's work, but it is quite obvious given the nature of the exception that it will first be included in the written works of authorship). The law further in Sections 28-30 establishes the basic elements of the general regime of copyright works from unauthorized broadcasting, which according to refer to the written works. Of importance is also Article 33, which gives the author the right "to prohibit or allow to publicly present his work which was recorded

[27] Art 10. of the Bern Convention.
[28] Ibidem, article 14.

on a sound or motion picture carrier (compact disc, audio cassette, video tape, film tape, optical disc, slide) with the means of technical devices (for the reproduction of sound or images)." It is obvious that this situation includes any electronic transmission or reproduction of written works of authorship. The authors of those acts for which, due to their nature, can be expected to be reproduced for personal non-commercial use of the audio, video and text (literature, music, film, etc..) are entitled to special compensation from the importation or sale of technical devices and blank audio, images and text that can reasonably be assumed to be used for such reproduction.[29] In the case of reproduction of copyright works by photocopying or similar technique, in addition to the right to compensation under paragraph 1 of this Article, the author is entitled to reimbursement from of legal or natural person who provides photocopying services for a fee.[30] Such a legal regime that is in practice faces different critics due to the size of fees and relative inconsistency, apparently it is possible to implement it to the written works of authorship, particularly in the copying or other forms of reproduction. However, it should be noted that this provision applies to those who provide photocopying services for a fee – that is, if they deal with this at its profit activity – and that as such solution can't be applied to colleges and other educational and scientific institutions which are photocopying materials from various authors in the educational and research purposes, and especially when LCRR allows it.[31] In support of this special regime says, and Article 49 of the LCRR, according to which the proper use of the cited works whose excerpt, extract is used as an illustration, a confirmation or reference does not have to pay royalties or obtain licenses from authors (this corresponds to described solution referred to in Article 10 of the Berne Convention). The decision referred to in Article 10bis of the Berne Convention is also elaborated in the statutory text. Thus, it is possible without permission and without payment of royalties, in the mass media – reproduction, distribution of copies, as well as other forms of public communication of articles that have been published in other media, provided that these articles refer to current economic, political or religious issues, and also that the author does not explicitly prohibits it. Compensation payment will not be if this purposes in the view of the various comments or articles, does exploit only short excerpts from reviews or articles.[32] Written works can therefore be under more or less similar conditions compared to other species and forms of copyrighted works, available in electronic form and use as well as in printed form. In this sense, the differences that Serbian legislation has are minimal and the principles of copyright are consistently enforced, regardless of the form in which it is written copyrighted work is used.

[29] Such article isn't unusual in many countries around the world. In elaboration on that in court practice, of case law in USA L.Lessig makes parallel between videorecorders and guns: Courts in USA got to the stand that any seller of VCR could be considered accountable for infringing copyrights that is done by byer of that product, by letting him (or her) obtain the means for criminal act of counterfeiting and infringing; that is the same accountability as gun sellers have. (Lawrence Lessig, Free Culture, New York, 2004, p.160). Probably realizing extremity and no logical thinking in this way lawmaker in USA started to "preventively sanction" sellers of the similar technologies, which can be used in infringing copyright with obligation to pay certain taxes.

[30] Article 39 sections 1 i 5of LCRR.

[31] In that sense all uncertainties is settled by art. 55 of Law, which says: "without consent of the author and with obligation of fee payment to him (or her), it is allowed to copy on paper or similar carrier parts of published work by photographical or similar technique with similar results in state agencies, educational facilities, public libraries, in order for use in education or scientific research".

[32] Article 56 of LCRR.

LEGAL PROTECTION OF SOFTWARE

General Statement

Definition of protection of Software is not easy to make. On one side, we have a living thing. Spasić criticizes the definition of computer programs from an old legal document from United States, according to which they are a "set of instructions or orders to be used directly or indirectly in a computer to achieve a particular effect."[33] Today, by most people computer programs are perceived as a final product that enables them to easily perform certain tasks, or some sort of entertainment (e.g. games). However, computer programs are in essentially exactly what this definition reveals – a series of commands and instructions written in a computer language that the computer recognizes and follows. What the user has identified as a computer program through the user interface, presents only the end result of this series of commands executed by the computer.

Subject Matter of Protection

As noted above, Article 2 of the LCRR, computer programs are defined as a kind of written works of authorship, regardless of their form of appearance (as stated in the Act, "regardless of the form of expression") – in this sense is equally punishable any kind of unauthorized disposition of a script computer program, as well as physically copying CD/DVD on which this program is recorded in electronic form.[34] Law is still stingy when it comes to special provisions that would refer only to computer programs. Article 47 lists some of the specifics that are related to the nature of the use of computer programs. Thus, there is said that a person who is "lawfully obtained a copy of a computer program that, can for their own usual use, without permission and without paying royalties:

1. store program in the memory of a computer and run the program; remove bugs and to make other necessary changes in it that are consistent with its purpose, unless the contract provides otherwise; make one backup copy of the program on a physical carrier; Decompile the program solely in order to obtain information necessary to achieve interoperability of the program with other independently created software or some hardware, provided that the information was not otherwise available, and that decompilation is limited only to that part of the program that is necessary to achieve

[33] Spasić Ž Vidoje, opus ciatust, p. 69. In the said paper Spasić, very accurate differs between computer program as written code and software as wider term – which is consisted of software and other different documents like manual instructions, package, software description.

[34] Putting software or computer programs in written works of art is not special only for Serbian law (LCRR) – similar solution has since mid-eighties of last century (USA, Japan, UK, Germany, France and some years later Spain) while EU in 1991 has issued directive which has put equal sign between computer software and written works of art, in sense of Berne Convention. Spasić Ž Vidoje, *op.cit*, p. 70.

interoperability." These are common activities that users of computer programs can (must) performed to use them; in the case of the last of these actions, the LCRR expressly provides that the information obtained in this way must not be disclosed to others or used for other purposes, in particular for producing or selling another computer program that would infringe the copyright in the first, and that such actions may made directly to the person who has lawfully obtained a copy of a computer program or other qualified person acting on his orders.

In addition to computer programs that fall into default – legal regime of copyright protection, there are licenses that permit a variety of different modes of use and the processing (changing) of computer programs - it's so called. "Open-source software" (a free software). These issues have already been discussed above.[35]

Musical work of art in cyberspace

According to Article 2 of the Berne Convention, the term "literary and artistic works" shall include all creations in the literary, scientific and artistic fields, regardless of the manner of their expression, and, among other works there are stated musical compositions with or without words. LCRR in Article 2 into the meaning of term the copyright work, in accordance with the Berne Convention, includes "musical works with or without words." Berne Convention in Article 2, point 3 specifically prescribes protection for adaptation and musical arrangements. The Berne Convention and in LCRR in particular were singled musical drama works. Musical drama works are different from the music works in that part of the music drama music is what makes the whole drama part and it is a part of the performance. Music copyright works are original works of authorship composers, lyricists, arrangers, and all those who are in the creation of musical works enter their intellectual creativity. When considering music works it is necessary to differentiate between musical composition and recording musical works. Musical composition is comprised of the composition and text of composition (a piece of music can be a combination of music and lyrics, or the music itself). So in it we have as authors composer, lyricist, arranger, and of course all the others who have made a visible and measurable contribution to the creation of a musical work of authorship. The author of a musical work, in addition to the rights that all other authors have, has the right to reproduce their artwork, to create a derived work of art, to distribute their music work and to publicly perform their musical act. The right to reproduce a musical work includes the right to record on tape, compact disc or as a digital file of one of music formats (analogue and digital). There should be noted that the advancement of technology today allows easily conversion of analogue to digital format and very simple and almost completely free copying and distribution of musical acts in cyberspace. Right of distribution of musical works includes the right to make and sell copies of musical works. This right may be transferred to the publisher or manufacturer for example CDs. From this derives the right to ban anyone else without the consent of the author of a musical work distribution of his (or her) copyrighted work. The most common form of violation of the rights of authors of musical works

[35] Licence of open content and Creative Commons Licence.

today is unauthorized distribution of musical works. Every day in cyberspace without authorization are set up many musical works in digital formats (mp3 etc.) on various websites and it is allowed to download it by an unlimited number of Internet users. As a special right of the author of a musical work is the right of public performance or interpretation of musical copyright works in concerts and other public events, broadcasting of music copyright works in radio, television, cable and satellite broadcasting. Musical work shall not be publicly performed without the consent of the author or authors of music associations (organizations for collective management of rights). Article 8 of the WIPO Copyright Treaty[36] [(1)] provides that the authors of musical works, and authors of literary and artistic works shall enjoy the exclusive right of authorizing any communication to the public of their works, by wire or wireless means, including the making available to the public of their works being carried out in such a way that members of the public may access these works from a place and at a time individually chosen by them, or over the Internet. International legislation WIPO Performances and Phonograms Treaty[(2)] specifically protects the rights of performers (interpreters) and producers of phonograms. This act as "interpreters" defines actors, singers, musicians, dancers, and other persons, who act, sing, deliver, speak, play in, interpret or otherwise perform literary or artistic works or expressions of folklore. Performers shall enjoy the exclusive right of authorizing, as regards their performances, broadcasting and public communication of their unrecorded performances except where the performance is already a broadcast and recording their unrecorded performances. They have the right to copy, to distribute, lease and right of making available of recorded performances. Phonogram producers, where term "phonogram" means the recording of performance sounds or other sounds, or the representations of sounds other than in the form of a recording incorporated in a cinematographic or other audio-visual work, have a right to reproduce, right to distribute, the right to lease and the right of publicly making available of their phonograms wired and wirelessly, in a way that allows the public may access them from a place and at a time individually chosen by them.[37]

[(1)] Law on ratification of Berne Convention for protection of literary and works of art, Official Gazette of SFRY, nr. 14/75 and Official Gazette of SFRY, – International treaties nr. 4/86.

[(2).] Law on ratification of *WIPO treaty of copyrights*, Official gazette of FRY – international contracts, nr. 13/2002.

Audio/visual work of art in cyberspace

Cinematographic works in narrow sense

Berne Convention for the already cited article 2 as a category of works states "cinematographic works to which are equaled works expressed by a process analogous to cinematography." Later in the text of the Convention are set cinematographic works within in the general framework of copyright law, with some exceptions that are understandable due to their specificity, while copyright holders are determined by

[36] Law on ratification of Berne Convention for protection of literary and works of art, Official Gazette of SFRY, nr. 14/75 and Official Gazette of SFRY, – International treaties nr. 4/86.

[37] Ibid.

the law of the country where the cinematographic work came from.[38] LCRR states as a type of copyright works the film work, and divide its forms on cinema and television. Hence the Spasić quite right when notes that there is some confusion between the terms "cinematographic work" and "filmmaking", since it was the first in the beginning included the content of authorship, and the film was just a medium, the carrier of the contents.[39] Today, in the age of electronic communications and electronic records of practically all works of authorship, this distinction loses its significance. However, the common name of the film works remained as a generic, and includes a wide range of films, documentaries and animated films and television shows copyright character. Films like the equivalent narrow meaning of the term cinematography or film work, specifically the product that contains more artistic elements, and therefore many types of copyrighted works, which have been incorporated into the whole. Thus, in the film can clearly separate the scenario as written works, musical component as a separate work of authorship, as well as a separate image element. It is possible to have other authors' works are incorporated in this unit – in example special dance choreography, etc… Hence films occupy attention of lawmakers, and even Serbian law is no exception. In Article 11 of LCRR expressly provides that as the filmmakers are considered a screenwriter, director and director of photography. If music is an important element of the film, or if it is a so-called musical film, and composed exclusively for the purpose of creating a film, then composer of film will be considered as co-author. If it's a cartoon or animated movie or cartoon or animations are essential elements of a film, then the main animator will be considered the co-author of a film. Although it is possible by a Film contract to assign property rights to the work of a film producer, screenwriter and composer of film music, film co-authors retain the right to exploit their work independently, apart from a film, unless the film contract provided otherwise.[3] Film works are suitable for digitization, and is thus a work of film included solutions from Articles 33 and 39 of the Act. Article 33 established the exclusive right of authors to prohibit or allow publicly disseminate his work, which is recorded on a sound or picture carrier (compact disc, audio cassette, video tape, film tape, optical disk, and slide) with the help of technical devices for the reproduction of sound or images. Furthermore, Article 39 establishes the same regime for film work on which was discussed in the analysis of regulations for literary and related offenses, and that is extremely relevant when it comes to the digitization of film work, "authors of works, which, due to their nature can be expected to be reproduced for personal non-commercial use of the audio, video and text (literature, music, film, etc..) are entitled to special compensation from the importation and sale of technical devices and blank audio, images and text that can reasonably be assumed to be used for such reproduction."[40] This provision, which as noted above is present (and criticized) in many comparable jurisdictions, is more efficient when it comes to film work primarily because the major film studios, mainly located in in the United States, lead the most extreme campaign against the freedom of the Internet and internet communication, which may be misused for copyright infringement filmmakers. Under the Act, filmmaker and producer videogame only has the authority to allow (or not allow) copying and distribution of film. However, the

[38] Spasić Ž Vidoje, op.cit, pp. 79-80.
[39] Law on ratification of *WIPO treaty of copyrights*, Official gazette of FRY – international contracts, nr. 13/2002.
[40] Articles 88 and 89 of LCRR.

development of modern technology and communication has made it possible that they can be effectively reproduced in any household, and obtain unauthorized copies on the Internet. Therefore, the issue of the so-called. "Piracy" is given much attention in the film and music industries, as well as the manufacturers of computer programs. As already explained, each bridging protection which have carriers of these works provided, their unauthorized copying and placing on the market or making available to third parties in any way, constitute an offense, or an offense in the laws of most states.

Television and radio programs

The Berne Convention does not explicitly elaborate on television and radio programs such copyright works, but uses a broad concept of "works expressed by a process analogous to cinematography," which could definitely be recognized television shows, regardless of whether the recorded programs or program that is broadcasted live. Unlike the text, the television works are explicitly mentioned in the LCRR[41] television and radio programs in each case must be considered copyright works - the fact that the radio programs is not specifically mentioned when listing the specific copyrighted works, does not take away this characteristic. This problem largely dismissed by Article 28 of the LCRR, which establishes exclusive copyright to allow (or prohibit) the broadcast of authorship, and thereby broadcasting is defined as "public dissemination of a wired or wireless transmission of radio or television program signals intended for public reception (broadcasting and cable broadcasting)." Radio and television program is therefore seen as a way of expression of another author's work, thereby not excluding the possibility that the radio emission is observed as a separate copyright works if they meet the criteria of originality, which are required for other types of works of authorship.[42] Analogy to the rights of film producers at film work, the Act provides a right of producer of the broadcast, which is related to electrical, electromagnetic or other signal converted into a sound, visual or audio-visual content that is broadcasted for the purpose of communicating to the public. In these rights are included licenses for the retransmission of broadcast, recording broadcast on a sound and / or images, copy length, etc... This definitely round out the system of copyright for a television and radio programs and particular attention should be paid to one of the rights of broadcast – interactive facilitating available to the public its emissions by wire or wireless means. The right of show producer among other things includes a license for web casting, broadcasting programs over the Internet and in real time – live when the show airs on radio/television or broadcast of programs (delayed versions) at a later time.[43] This is one of the basic ways of use, and possible misuse or unauthorized broadcasting, television and radio material - talk shows - on the Internet. However, the concept of broadcast is important with internet radio stations that broadcast their programs only through the Internet.[44] Internet radio has its obvious advantages, because it

[41] Art. 39, section 1 of LCRR.
[42] Art 2. Of LCRR.
[43] We can disclose this from art. 29 of LCRR.
[44] Other manners could be considered as copyright infringement on other works / in example transmitting or facilitating availability by other means of a film work taken over from a TV station or recorded other way.

can be broadcast to the world, no matter where the listener is a number of broadcasters is not limited by the number of available frequencies, and so on. It is estimated that one-fifth of US citizens listen online radio stations, while in 2004 the total number of users on a worldwide basis was $ 80 million, and in the last few years there has been an increase of almost 50% per year. It must be noted that the copyright laws which apply to the general regime, remain identical when it comes to radio and TV as the exclusive internet phenomenon – that is, everything that has been said about the "regular media" in a way that viewers and listeners are accustomed to traditional consume them, true to their internet versions – copyright in the internet world are still protected and any unauthorized downloading, or in any way unauthorized distribution is prohibited and punishable.

LEGAL PROTECTION OF DATABASES

Berne Convention for the already cited Section 2 within the expression "literary and artistic works" shall include lectures, speeches, sermons and other works of the same nature. Within the Bern Convention, greater attention was paid when it comes to voice work, only political speeches and speeches held in during the court hearings. Article 2bis is left to national legislation to partially or totally exclude it from protection predicted in Article 2 of the Berne Convention, political speeches and speeches delivered in the course of court hearings. National legislation is left to determine the conditions under which the teaching sermons and other works of the same nature which are exposed on the public will be able to be reproduced by print, broadcast through radio broadcasting communicated to the public through the wire and be subject to public interpretation unless such use is justified by the objective of achieved notice. However, in these cases, it is left to the author the exclusive right to compile their works. LCRR in Article 2, point 2 of authorship, in accordance with the Berne Convention, includes voice work (lectures, speeches, sermons, etc...). For voice work are provided the same moral and economic rights of authors, as well as any other literary and artistic works. Of course, the voice part can be converted to digital form, and then, the authors retain all their rights under the legislation and only they can approve an conversion to digital format, distribution or public communication of their digital voice work of authorship, except in cases where it is otherwise regulated in political speeches and speeches delivered in the course of court hearings. Prerequisite of originality is assumed with speech acts, so that some authors believe that the lectures are held in the classroom, and are based on strict adherence to certain literature do not represent original intellectual creations and not considered to be copyright works.[45]

Compilation of copyright and data in cyberspace

Berne Convention for the Protection of Literary and Artistic Works in Article 2, point 5 provides a special form of protection for the collection of literary or artistic works, such as encyclopedias and anthologies which, according to the choice and arrangement of the contents constitute intellectual creations, of course, this protection should not produce any damage to the copyright to any of these acts are an integral part of these collections. LCRR in Article 5 sets out in more detail situation in which the collection is considered copyright act. These are the cases when it comes to reference books, journals, anthologies, selected works, musical collections, and collections of photos, graphic works, exhibitions and the like, provided that it is the original spiritual creation of the author. As authorship is also considered a collection of folk literary and artistic creations, as well as a collection of documents, court decisions and similar materials, databases, whether in machine readable or other form, that given the choice and

[45] Spasić Ž. Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011, p. 71.

arrangement of the components meet the condition they represent original intellectual creation of the author. In our LCRR, in accordance with the Berne Convention for the Protection of Literary and Artistic Works, is provided that collection shall not in any way limit the rights of authors of works that are part of the collection. Usually, as the author is considered the collection editor, therefore to him (or her) does belong proprietary and moral rights under copyright? "However, if the collection consists of works of authorship that are within the duration of legal protection, a collection of the author where the collector is not the author of some works, then from it arises relationship analogous to the relationship between the original and derivative work, with all the legal consequences that come along. Hence authors of works (constituent elements of the collection) have their own separate authority, independent of the rights of the authors of the collection. In this sense, the author of the collection must, above all, to seek the consent of the author constituents. Moreover, the authors of component parts have the right to request that their names are specified when using collection. Moreover, the author of the part which is an integral part of the collection may exercise his (or her) authority to protect the integrity of the work, oppose to improper utilization of parts, as well as the right of repent."[46] All kinds of collections of copyright works can be digitalized and subject to the terms of exercise of rights related to everything already mentioned for the protection of all other works in cyberspace. The simplest definition of a database is that they are organized sets (collections) of data. Creating a database is aimed to facilitate ease of use, viewing, searching, transferring, comparing, sorting, and editing data. Nowadays most of databases are fully digitized and available in cyberspace. Digitalized databases are made up of a number of records, and each record is composed of a set of elements (data). One of the essential characteristics of a database is that they include information, materials and/or parts that make up the collection, and so are selected, connected and arranged to make the intellectual creation and a new work of authorship.[47] Legal protection of databases is possible within the legal regulations *sui generis*, in the framework of regulations that protect copyright and similar rights in the framework of the regulations governing the issue of unfair competition. *Sui generis* rules are rules that are made when there is a special situation that cannot be subsumed under existing regulations. Databases are rich in specifics and therefore many believe that they are not protectable by use of existing legal institutions and that there is a need to pass special legislation - *sui generis* legislation to protect the website database. One such legal document was adopted by the European Union, the European Union Directive 96/9/EC on the legal protection of databases. It is defined in Article 1 that the database is "a collection of independent works, data or other materials arranged in a systematic or methodical way, which is individually accessible by electronic or other means."[48] The exclusive rights of the author under Directive 96/9/EC were 1. temporary or permanent reproduction by any means or in any form, in whole or in part; 2. translation, adaptation, arrangement and any other alteration; 3. any form of distribution to the public database or a copy; 4. any kind of communication, public display or public performance; and 4 reproductions, distribution, or any form of communication, public display or public performance of translated, adapted, or prepared in

[46] Spasić Ž Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011, p. 63.
[47] Drakulić, M. Računarsko pravo, Beograd.
[48] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal L 077 , 27/03/1996, p. 24.

any way changed the database. Article 7 of Directive 96/9/EC provides a *sui generis* right website database in terms of preventing the extraction and/or re-utilization of the whole or a substantial part of the database in qualitative and/or quantitative terms. Under the "extraction" should be considered as permanent or temporary transfer of the entire database or a substantial portion of a database to another medium by any means, in any form. By "re-use" will be regarded any form of facilitating of a public access to all base or a substantial of its parts, distribution, rental of on-line or other form of transfer. This article of the Directive 96/9/EC Paragraph 4 provides that this type of protection is on regardless of the suitability of the content of the database to be protected as a copyrighted work. Article 9 provides for the possibility that national legislation determine exceptions on the application of *sui generis* rules in the following cases: 1 extraction for private purposes of the contents which is not an electronic database; 2, in the case of extraction for the purposes of an illustration of teaching or scientific research, provided the source and to the extent that is necessary for the non-commercial purpose of use; and 3 in the case of extraction or re-use of public safety, administrative or judicial proceedings. In addition to protection through regulations that protect copyright and neighboring rights and *sui generis* legislation by the authors of the database can be protected by national regulations relating to unfair competition. These regulations do not replace the aforementioned two types of regulations, but supplement these regulations and allow the authors of databases specific form of protection in cases of unauthorized extracting of a larger or smaller part of the contents of the database in order to achieve competitive advantage in the market.

OTHER INTELLECTUAL PROPERTY RIGHTS IN THE ICT SECTOR

Generally

Article 2 of the Berne Convention states works of drawing, painting, architecture, sculpture, engraving and lithography as copyright works of art that have the document protected under the general regime of copyright. When it comes to these works in cyberspace and in digital form, it is certain that the subject of copyright can be only their reproductions, and photos, and not by itself. Hence, it is of importance article 11bis of The Berne Convention, which leaves authors the exclusive right to consent to, among other things, "broadcasting of their works or their communication to the public by any means of wireless diffusion of signs, sounds or images" or "the public communication by loudspeaker or any other similar device transmission of signs, sounds or images works "... Although outdated and obsolete when it comes to electronic communications and cyberspace, this formulation is analogous to the use of modern technology communication". In Article 2, paragraph 2, point 6 of the LCRR, works of fine art are also explicitly defined as works of authorship. What is so specific in terms of the group of works of authorship is the eventual manner of their expression in electronic form - it cannot be such that it represents the original, because it does not have the three-dimensional shape nor the ability to at any time replace (accidentally or intentionally) the original work. In these cases, there is only one original that has artistic value, a copy or display (images, 3D model) of such acts will be just - only a copy of the electronic, digital form.[49] More or less faithful to the original, perhaps even identical, copies will not have any special artistic value. That's the difference between, for example part of film, theatre and music in relation to this specific category. Music tracks can be faithfully transmitted in electronic form and cannot be discussed as to whether the original recording has a higher or lower value of electronic copies that are unlawful exchange on the Internet – the original and the copy are identical in substantive terms. In a work of fine art is not, nor it can be the case. However, what is common to these works in cyberspace with virtually all other copyright works is the possibility that it is illegal to show to big – virtually unlimited – number of people. For many, it will be enough from the comfort of their home to examine and to look to perfect reproduction of an image in high resolution, but to pay a ticket for a gallery to exhibit work. In this sense, these works may not apply the provisions of Article 37 of the LCRR, according to which the author is able to prohibit the presentation of its work of art - unless he (or she) has sold it, and that he has not explicitly insisted on such a ban. On the other hand, in cyberspace, far greater relevance has the provision of Article 46 of the same Act, which prevents the commercial use of multiplied copies of the published work - that is, the exclusive authorized personal (not public!) and non-commercial use. Hence, the unauthorized use of any work of art in cyberspace,

[49] Compare: Bainbridge D., op.cit, p. 83; Vidoje Ž. Spasić, op.cit, p. 83.

which is by its nature open to the public, constitute a violation of copyright to which the author may require damages from the violator.

Legal Protection of Multimedia Works

Works of architecture, applied arts, industrial design in cyberspace

Works of architecture, applied art and industrial designs under the Berne Convention are also works of authorship, protected by copyright. Article 2 of the Berne Convention explicitly cites works in the field of architecture, applied art, plans, sketches and three-dimensional works relating to architecture. In Serbia, the LCRR, Article 2 as works of authorship (as copyrighted material) are expressly stated in item 7 as architecture, applied art and industrial design, and in point 9, plans, drawings, and models. Article 51 of LCRR provides that it is allowed without permission of the author and without paying royalties – two-dimensional reproduction, distribution of such copies, and some other forms of public dissemination, which are permanently on display in the streets, squares and other public open spaces. According to article 57 of the same Act, without the author's permission and against payment of remuneration, shall be allowed a three-dimensional reproduction of works that are permanently displayed in the streets, squares and other public places, as well as the circulation of such copies, unless a copy of a sculpture receives casting from the original model from which the copy that will be permanently displayed at an open public place or from a model made by casting the sculpture; If a building is modelled on the existing building; product formed after a work of applied art. When it comes to works of architecture that means that it is only the original author's works, which means must that it have an original design and a minimal degree of creativity. "Not every building or architectural work is copyrighted work. On the contrary, only a small number of facilities will be considered part of the architecture and will enjoy copyright protection."[50] Although some authors believe that the work of architecture cannot be subject to interpretation and cannot be converted to digital form that would have utility value and practical application[51] that is not quite precisely because it is already possible to create three-dimensional models of objects and provide a virtual tour of the facilities, or even facilitate stay of the virtual personality in these facilities, and of course, plans, sketches and models of architectural work are already digitalized and often used in cyberspace without permission of the author and although that violates the rights of the authors of architectural works. Works of applied art are works of art (original works) which are applied, and can be manually produced or manufactured by industry. Practical application, items for personal use, posters, labels, or other objects in fact distinguishes these artworks from other types of artworks, with other works of art binds them together in creativity and artistic merit. Works of applied art and industrial drawings and models have their own specificity, as they often are not only works of art but also manufactured goods. Berne Convention in Article 2, item 7 leaves national Legislation to establish the field of application of the law relating to works of applied art and industrial drawings

[50] Spasić Ž. Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011, p. 83.
[51] Ibidem, p. 84.

and models, as well as the conditions under which such acts, drawings and models are to be protected. For works that are protected only as drawings and models in the country of origin, it may be possible in another country to seek a special protection recognized in this country to a drawings and models; however, if such special protection is not recognized in this country, the work will be protected as artwork. In terms of the content of authors' rights in relation to works of applied art, they have all the rights that other works of authorship enjoy, and may have protection under other legislation relating to industrial property or rules relating to unfair competition. Works of applied art because of their nature, they are far more susceptible to digital piratery than architecture.

Cartographic works in cyberspace

Cartographic works are defined as two-dimensional representations of surface land, or part thereof, the space objects and the sky in a less scale, or in a certain proportion. The Berne Convention states cartographic works in earlier repeatedly mentioned article 2, paragraph 1, as one of the forms of literary and artistic works, hereinafter referred to in this document do not contain any provision which would more closely determine their legal status. LCRR, in Article 2, paragraph 2, item 8 also outlines the geographic and topographic maps as a kind of copyrighted works, but there is no word in the text more about them. Given these circumstances, one would conclude that these authors' works are under the general regime, which was established in the legal system, and that to them are applied all the provisions that are most general character and established for all copyright works in its entirety. When it comes to computer programs that appear in the cyber environment in connection with cartographic works, by far the most attention so far is drawn to the Google applications: Google Maps and Google Earth. These are user programs in specific way make closer geographic information to individuals who use them. Google Maps is the name of the user program that serves to the presentation of map data, maps of virtually all places on the planet. This program primarily serves as orientation in urban areas, showing roads and buildings (as well as their distance, shortest and/or fastest times, means of public transport, etc..), combining in this way virtually all functions of GPS systems and maps. The system itself is free of charge, but suffers from some limitations. However, this popular program has become widely accepted primarily because of the non-commercial aspects (use free of charge), because of the possibility to combine its various properties (in example it is possible to review the field in the mode of the plan, but also in mode of geophysical maps using satellite imagery territory) as well as versions which also can be used for free on mobile phones and tablet computers. Google is the owner of the copyright on the maps that display, or leased their use in a specified time period from the copyright holders.[52] Google Maps application is free for users, but the commercial component of its use can be seen in the existence of various internet ads, which is a distinctive way of the various products of Google. If we analyses the terms of the program, it can be concluded that it falls under the non-commercial license, which is free to use but is not allowed for commercial purposes, or for further processing and upgrading both software and base images. Terms of use fall under the

[52] Only country in the world which wasn't up until recently covered by this system was People Republic of Korea.

jurisdiction of the legal system of the United States. When it comes to the use of maps for other purposes, Google has set up two main limitations: You cannot use any of the final product of Google Maps (that is, a folder or a portion thereof, in any format, resolution and proportion, scale) for commercial purposes (further resale, use in a variety of publications[53] or other computer programs); second limitation concerns commercial use - in this case it is necessary to reflect on the map stamp, logo or watermark, which will clearly indicate the origin of the photographs, i.e. maps. For certain applications Google have a different license, which can offer professional users to integrate Google Maps into their programs (commercial) websites (Google Maps API).

Photos, plans, sketches and models in cyberspace

General rules of copyright apply to, under the Berne Convention, according to Article 2 also to the works of photography to which are assimilated works expressed by a process analogous to photography.

LCRR has predicted also by Article 2, item 9 a copyrighted work plans, drawings, models and photographs. When it comes to photography, it is necessary to distinguish between images as a work of art that protects the LCRR and the common photos that have protection on the basis of the general principles of civil law and regulations governing unfair competition. Photography as art must have some degree of originality and creativity that separates it from the ordinary photos and must have a certain artistic value. In order to have some degree of originality and that it could be argued that a photograph a work of art, it is necessary that it is the result of intellectual, creative activity which is so original that two people, independently of each other, it is reasonable to assume couldn't create exactly the same result. Of course, in practice, is not always easy to distinguish between these two types of images. Progress of technology facilitated possibility to easily convert analogue photos to digital photography, by scanning or photographing with a digital camera or mobile phone, and even their procession and changing is very simple. Today, most of images are produced and remain in digital form. Because of that specificity of the photos, they are extremely susceptible to abuses within the cyber space. Plans, sketches and models can also be copyright works if they meet the necessary criteria of originality and creativity. "These are the author's creations in various fields of science or art that are expressed in two-dimensional (plans and drawings) or three-dimensional form (plastic parts, models, etc.)."[54] Of course that the plans, drawings, and models also can be found in digital form in cyberspace where they are subject to the same types of protection, as well as other works of authorship.

Drama, choreographic and pantomime works in cyberspace

Drama, choreographic and pantomime works are collectively known as "theatrical works".[55] Their main characteristic is that these are part of the intended performance of

[53] Unless it is scientific research work where product is used as side element, utility if visuelisation.
[54] Spasić Ž. Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011, p. 87.
[55] Spasić Ž. Vidoje, op.cit, p. 71.

the stage in which intertwines several elements of expression – music, movement, text, game. Vidoje Spasic is consistently supporting the domestic legal provision, and as a special category of these acts notes also folklore acts.[56] Under the Berne Convention, dramatic, choreographic and pantomime works fall under the general definition of "literary and artistic works."[57] Authors of drama, musical-drama and musical works shall enjoy the exclusive right of authorizing the public performance of their works, assuming public performance by any means or methods, as well as to the public of any means of display and presentation of their work.[58] This provision logically assumes transfer, or reproduction in whole or in part, the performance of dramatic, choreographic and pantomimic acts in cyberspace. Also, according to Articles 12 and 14 of the Convention, the authors shall enjoy the exclusive right of authorizing adaptations, arrangements and other alterations of their works. This would mean that such acts, as well as other analyzed products and intellectual copyrighted work may not be used without authorization in any form – for posting or making available in its original form – as well as for further development, processing, or any other processing of the original work (and the subsequent setting up of such acts in cyberspace). Neither these works, as well as others that have been discussed above, will not enjoy copyright protection if they become public property (Article 18 of the Convention). When it comes to drama and musical-drama works, these are works that contain both text and music, which are designed (or adapted) for stage performance. When it comes to the area of copyright, it should be noted that each music track, regardless of the text that may be spoken in the work, is regarded as a copyright work, but they are jointly covered by the right to broadcast or display part, which belongs to the author works as a whole. In cyberspace, we can talk about a few aspects of copyright in relation to these works: transmission or reproduction of works, publication of text and music, in part or in whole, or individual music tracks, any audio or video recordings of these works regardless of the way and modality of their performance.[59] All the rights belong to the copyright holder of the work as a whole, and can be realized only with his (or her) permission. The same applies to the reproduction and distribution of works as a whole, or its aforementioned segments. Choreographic and pantomime works are specific to the group of so-called "theatrical works" primarily because they do not necessarily have to perform on stage, and are therefore commonly isolated in comparable regulations as a special kind of copyrighted works. While pantomime works executed movement with possible background music, choreographic works are diverse and they are, except that ballet is the most common form of these works considered a folk, folk dances and games. In ballet there is a synthesis of text; movement and music in a work of authorship, while in others generally combine music and movement. As in the previous cases, these works are protected from any kind of reproduction and/or adaptation without permission from the author, in cyberspace, using audio-video recordings, as well as the other theatre works.

[56] Ibidem.

[57] Article 2, section 1 of Convention. It is the same according to article 2, section 2, point 3 of LCRR.

[58] Article 11 of Convention.

[59] For example it will be considered as infringement uploading on the internet of the recording of official interpretation of work that was allowed (but there is no allowance for further transfer and distribution) or uploading on the internet of that recording in private manner.

INTERNET DOMAIN NAME REGISTRATION

Background

Period in which the owner of the company, or trademark, could use this right is different in different countries. In Serbia, it is permanent, as long as the registration of the mark and such domains are sometimes called "protected domains" – this name shouldn't be literally taken, because it derived from the name of "trademark". Trademark, as the basis of visual recognition of a company, is copyrighted – no one should use some trademark without the permission of its owner. Hence, according to the Serbian decision, anyone who has a trademark has the right to a domain that will contain the name of the registered company. This also applies to individuals – that is it is not necessary to have a company that is a registered trademark and thereby acquire the right to use the same internet domain.[60] In addition to these situations, the domain registration is valid right of way at the time – who first applies for registration of a particular domain will be able to lease it.[61] According to Article 16 of the arbitration proceedings to resolve disputes regarding the registration of .rs domain,[62] the arbitrary tribunal may decide on the termination or transfer of the disputed Internet domain with the registrant (the person who purchased the domain) to the plaintiff, if it satisfies the following:[63]

- that the disputed domain name is identical or substantially similar to law protected trademarks, business or trade name of the plaintiff for the same or similar goods or services, or if the similarity can create confusion and mislead users;
- the registrant has no legitimate interest and right to use the disputed domain name – this is a situation where a registrant hasn't bought a domain name with the intention of using it for business purposes, but for other reasons, especially because of subsequent resale, or just to prevent another person to use it;
- the registrant has registered a domain and use contrary to the principle of good faith, honesty and good business practices – this will happen if someone leases a domain that resembles the name of the competing company and it publishes false information about its operations, supply, etc.; This situation will exist especially when the domain is leased to use the company, trademark which are similar to a protected mark in order to attract customers and create confusion about the origin of the goods in question.

Problems continue in cases of global internet domains. Trademark and company are usually registered at the national level; internet on the other hand has no national

[60] In Serbia about this is in charge Register of national Internet domain of Serbia – RNIDS. Internet address: http://www.nic.rs, last accessed on 01.08.2014.

[61] In Serbia internet domains are leased for a period lasting from one to ten years, and after that period it can be again registered the same domain, of course always former registrant has the first right. Cited from: Prlja Dragan, Reljanović Mario, op.cit, p. 142.

[62] Manuscript of proceedings can be found on Internet address: http://www.nic.rs/files/list0031.pdf, 01.06. 2012.

[63] Look at article nr. 17. Proceedings.

boundaries. Here the story is spread from Internet domain names and gets in the area of advertising - different companies may have the same or similar marks registered in different countries, and advertise their products throughout the world through newspapers, satellite television, and the like. Then it is quite reasonable to expect that potential customers will not understand that there are different companies that beyond a common name, company and/or trademark - that is, the visual impression created by clients or consumers do not really have anything in common. How G.J.H. Smith observes, very correctly, this problem is not new but is now placed in a new, far more complicated context, considering that with the advent of the Internet, particular advertising can be made currently available to all countries of the world, 24 hours a day, potentially unlimited number of users, and there would be no physical manifestations, or physical form, and commercials whose traffic could be prohibited or at least limited for the countries in which it violates the right to use a registered trademark.[64] One of the solutions, which is quite logical, is the registration of the company and trademark, which would include more countries at the same time. Second solution of this problem would be that in practice could be applied only by large and wealthy companies, and it is to register trademarks and/or firms in all countries of the world individually. It is interesting that even this author doesn't have a definitive answer to the question of how could we provide most efficiently complete protection to a company or trademark, and proposes smaller companies focus on the most important markets for their business, where they would be better protected. This should in practice lead to the company that develops and conquer new markets, and it potentially would have in the future on all markets to appear with a new name and visual identity because the original is not protected at the time, which is quite inconvenient and not conducive to companies that seek to create a world-known brands.

The Registration Procedure

General Considerations

National Register of Internet Domain Names of Serbia (RNIDS) is a professional, non-governmental, non-profit foundation formed to manage the national internet domains .RS and .SRB, in providing the general interest of all citizens of Serbia, through respect of the principle of quality, efficiency, independence and transparency.

Constituent Assembly of RNIDS was held on July 8, 2006 and this day is celebrated as the Day of RNIDS. Until 28 May 2011 RNIDS worked as a fund, and then, in accordance with the law, he became the Foundation. Authorities RNIDS are: conference of co-founders, Board of Directors and CEO. Co-founder of RNIDS can become any domestic legal entity or an entrepreneur which pays an annual fee, signs a contract and delegate their authorized representatives to the Conference of Co-founders of RNIDS.

RNIDS manages the register of National Internet Domain Names of Serbia .RS accordance with the decision of ICANN on 11.09.2007. ICANN has accepted the

[64] Graham J.H. Smith, op.cit, London, 2002, p. 74.

proposal RNIDS on November 8, 2010, to mark .SRB a Cyrillic domain of Serbia and awarded this designation to our country for the second national domain on the Internet. Serbian Internet Domain Day is celebrated on 10 March 2008, the date when began the official registration of .RS domain. Connecting Yugoslavia in global electronic networks began in the late eighties of the 20th century. Then in Europe was operating the European Academic Research Network (EARN). In 1988 the Faculty of Physics in Belgrade[65] suggested that our universities join the EARN. University of Belgrade became the hub of EARN in 1989, when the first international academic network connections between Belgrade and Linz was established.[66]

Since simplicity of TCP/IP protocol family caused the rapid development of ARPANET (which later grew into the Internet), soon it was needed to establish a "bridge" for the exchange of electronic mail and data between the Yugoslav academic network (based on VAX servers connected to DECNET network and X.400 test platform) and the ARPANET. In order to achieve this connection, Yugoslavia got its Internet top-level domain (TLD) - yu.

Project to develop an academic network for Socialist Federative Republic of Yugoslavia functioned as part of the project for the development of scientific and technological information (SNTIJ), and alongside with the University of Maribor, a project led by the Institute "Jozef Stefan", from Ljubljana, and these institutions took over the organization of the first register yu domain, between 1990 and 1991.[67]

Evolution of Domain Name's

The beginnings

When in 1992 the UN imposed sanctions on Yugoslavia, network traffic with foreign countries was suspended, and our country is formally excluded from the international academic exchange. With the disintegration of the country also ceased to exist SNTIJ project, but the .yu domain remained in Slovenia. After Slovenia gained its national TLD (.si), members of the Commission for SNTIJ from Serbia sent a letter to their colleagues in Ljubljana, with a request to transfer .yu register competence. Since on the sent letter there was no reply for months, Ms. Mirjana Tasic from the Faculty of Physics in Belgrade required assistance from international and European institutions that deal with managing of the basic Internet services. Letters were sent to the address of John Postel (IANA, the Internet Assigned Numbers Authority), and colleagues from the organization RIPE (Résaux IP Européens). The correspondence lasted until the spring of 1994, when John Postel finally ruled in favor of the Federal Republic of Yugoslavia. Since then, the management of .yu TLD registry was entrusted Ms. Mirjana Tasic and a group of enthusiasts from University of Belgrade (professor. Bozidar Radenkovic from Faculty of Organizational Sciences – FON, prof.

[65] Significant support the initial establishment .yu domain gave the scientific diaspora - professors, researchers and PhD students at various Universities, who then agreed to administer second-level domains within yu TLD.

[66] The capacity of this link was initially 4,800 bit / s, but was later doubled to 9,600 bit / s.

[67] The first official administrator yu TLD was YUNAC registered to the address of the University of Maribor.

dr. George Paunovic with Electronic engineering faculty –ETF, Berislav Todorovic, Nenad Krajnović the ETF and others), which were functioning under title YU NIC - Yugoslav Network Information Centre.

The establishment of the first primary DNS server for .yu TLD was not easy, because Yugoslavia was under sanctions and foreign companies were forbidden to establish any links with Yugoslav firms and academic institutions. At the request of YU NIC and courtesy of the staff of the Internet service provider MCS.com, domain yu was "hosted" out of the country, provided that MCS wasn't responsible for the maintenance of Yugoslav domains. To this limitation to be overcome, it was decided to make a second-level domain .co.yu and .ac.yu which should have been directed towards other Internet servers whose administrators would be willing to maintain a .co. yu i. ac.yu domain.[68] The situation was functioning in this way until 1995, when they re-established international telecommunications relations. The primary DNS server for .yu TLD then migrated to servers EUnet in the Netherlands, and soon after to the server ETF and FON in Belgrade. National .yu domain was located on servers at ETF where remained until the departure from the Internet in March 2010.

As might be anticipated from the story of the struggle for the assumption of jurisdiction over yu domain, the official institutions of the nineties didn't show much interest in support the efforts of enthusiasts from YU NIC. Minimal financial support necessary for the functioning of these groups dried up in 1995, and YU NIC had to adapt to a "temporary situation that has become a permanent state of things.[69]2 The first consequence of this adjustment was limiting the opportunities for .yu domain registration only to legal entity's (companies, entrepreneurs, civic associations, political parties, etc.). In addition, we have introduced the restriction that each entity may have only one domain. These limits are somewhat mitigated by the decision of YU NIC not to charge a service of domain name registration. The rapid development of the Internet in our country has led the current mode of operation YU NIC to the breaking point. The number of requests for registration of domain names, in spite of all the limitations, grew to over 200 a day, while time of waiting for the activation of domain extended to approximately 20 days.

Reform initiatives

Since 2000, there were initiated a series of processes that are aimed at reforming modes of operating of YU NIC. In mid-2001 was formed a working group within the Federal Office for Information Technology, which created the first draft of the new Regulations on the Registration yu domain and the Statute of YU NIC. In late 2002, the Working Group within the Republican Agency for Information Technology and the Internet has made the second draft of the Regulations on the Registration yu domain and the draft Agreement on domain registration.[70]

[68] Significant support the initial establishment .yu domain gave the scientific diaspora - professors, researchers and PhD students at various Universities, who then agreed to administer second-level domains within yu TLD.

[69] Urgent costs, such as failures of computer and network equipment necessary for the operation of the registry, mostly covered by the School of Electrical Engineering and the Faculty of Organizational Sciences.

[70] www.internodium.org/node/1824.

At the initiative of Mrs. Mirjana Tasic, in early 2005 formed the ad hoc working group with the aim of making the founding documents of the organization that is supposed to take over the management of .yu domain. Group included, in addition to the current administrator yu registry, the national Internet service provider, Telecom, Ministry of Science and Environmental Protection, NGOs, etc.. This group drafted the Statute of National Register of Internet Domain Names of Serbia (RNIDS). Public consultations on the draft Statute RNIDS lasted from 20 March to 3 April 2006.[71]

In those years, in the framework of the working groups and the broader Internet community it was agreed that it is necessary to provide at least the following:

Establish a non-profit (but cost-recovery) organization, which will act in the common interest (RNIDS will be served by fees (charging) for registration of domains in the central register).

Representation of all relevant interests in the process of developing and implementing organizational policies.

Domain registration in registry-registrar model (RNIDS will maintain a central registry of domains, while domain registrars enter into a RNIDS at the request of end-users).

The abolition of existing restrictions on the registration of the domain (citizens and organizations will be able to register an unlimited number of domains)

Establishment of fair rules for mediation in resolving disputes over domain names

Establishment of RNIDS

The working group in May 2006 agreed on the final text of the draft Statute RNIDS, and the Constituent Assembly of the new organization was held on 8 July 2006 and it was attended by 34 companies and organizations. The Steering Committee RNIDS, was also elected, who worked on creating the organizational, technical and financial requirements for responsible and reliable maintenance of central .yu domain. The process of negotiating the transfer of competences between the NIC, State, ICANN and RNIDS was completed. Treaty of establishing RNIDS was signed on 18th December 2006, by 17 companies and organizations that have in that way acquired the status of a founding member. RNIDS was on 12 February 2007, registered as a fund in the Ministry of Culture, which officially initiated its operation.

ICANN on 11 September 2007 has issued a decision by which RNIDS was entrusted with the management of existing and future YU register Register of National Internet Domain Names of Serbia and .RS domain has become visible on the Internet on 25 September 2007.

In 2007, with the Montenegrin register RNIDS signed the Agreement on Transition domain names and subdomains registered under the domain .yu .rs and .me Domains.

[71] www.elitesecurity.org/forum/230.

Representatives RNIDS participate in work of ICANN (Internet Corporation for Assigned Names and Numbers)[72] and CENTR (Council of European National TLD registries).[73]

Getting Started .RS domain

Official registration .RS domain began on 10 March 2008 at 12.00 hours, while more than 27 companies that are authorized for performing domain registration tasks. On the first day of 7000 registered the domain. In the next six months to 10 September, the owners of the old .yu domain had given priority to register the same domain with the .rs. Old .yu domain was about 40,000, of which about half were still active. RNIDS, in order to ease the transition, he founded the Committee for the transition, which is addressed by the registration of the transition in cases where .YU domain registrant is no longer an active entity.

The main objective of RNIDS is to organize the management of the register of National Internet Domain Names. RNIDS operates five address spaces in both national domain (.rs .co.rs, .org.rs, .edu.rs and .in.rs and .srb, .pr.srb, .org.srb, .obr.srb and .od. srb) managing of address spaces .ac.rs and .ak.srb is left to the academic network of Serbia, a .gov.rs and .upr.srb left to the Administration for Joint Services of the Republic Bodies.

Additional objectives of RNIDS are:

1) Increase the number of co-founders RNIDS and participation of the general community in his work;

2) To promote the Internet as a public good, available to all citizens;

3) Increase Internet content on Serbian and minority languages.

RNIDS performs the following primary activities:

1) Technical and administrative management of the Central Register of domains within the national TLD and IDN assigned by ICANN to the state of Serbia;

2) Maintenance of the main DNS servers for ccTLD and IDN;

3) Management of the publicly available WHOIS server for the national domain;

4) Establishment of principles and procedures for the operations of registrars;

5) The collection and publication of data on the development of the national Internet (in terms of its scope and in accordance with the objectives RNIDS);

6) Developing and promoting of policies for dealing with registrars in accordance with best practice, using the experiences of other national registries;

7) Assistance in settling disputes over allocation of domain names;

8) Cooperation with similar regional and international organizations;

9) Promotion of the .rs and .srb domains.

RNIDS also performs the following additional activities:

1) Organizing professional conferences, public hearings and other meetings;

[72] www.icann.org.

[73] www.centr.org.

2) Supports the registrars within the national domain;

3) Collaborates with other national and international organizations in accordance with the objectives and activities of RNIDS;

4) Other activities consistent with the objectives of RNIDS.

RNIDS is a member of CENTR (Council of European National TLD registries), and cooperates with ICANN (Internet Corporation for Assigned Names and Numbers).

The birth of .SRB domain

In early 2010 RNIDS started the procedure for the introduction of Internet top-level domain (IDN ccTLD) in the Serbian language and Cyrillic script. On November 8, 2010, ICANN stated that the proposal of RNIDS was accepted to mark .SRB as a Cyrillic domain to Serbia and awarded this designation to our country for the second national domain on the Internet.

Cyrillic domain .SRB became visible on the Internet on May 3, 2011, and on 11 May 2011 was engaged into operation a new official website RNIDS and also became the first local site in a new national Cyrillic domain, at рнидс.срб.

At the session of the Assembly RNIDS held on 28 May 2011 adopted legislation governing the registration .srb domain, and the passing of the Statute which RNIDS became the Foundation, in accordance with the law, and the Assembly was renamed the conference co-founders.

RNIDS

The Registrar is a legal entity or an entrepreneur based in Serbia, which has the authority RNIDS to register the names and .srb rs domains in the ccTLD registry. RNIDS is responsible for managing the central register rs and .srb domain, while the jobs name registration rs and .srb domains for end-users (registrants) performed by registrars. Registrars are economic entities in the field of IT, which meet the technical requirements of RNIDS and have signed a contract with RNIDS.

Privacy Protection

Jobs national domain name registration includes:

- registration of domain names
- changing data for the domain name
- renewal of the registration of the domain name
- transfer domain names between Registrars
- transfer of the domain name registration
- the activation of the contact information for the domain name
- termination (deletion) of the domain

It is possible to file a complaint regarding the register. Any interested person may file a complaint about the violation of laws on the registration of the domain name. Comments should be submitted in writing to the office RNIDS and must include: information about the identity and contact the applicant, a detailed description of the circumstances that led to the violation of laws on the registration of the domain name or the work of the Registrar and other evidence to support the claim that there was an alleged violation of. For more information, read the Regulations on the establishment and work of the Commission for determining violations of provisions of legislation on the registration of the domain name.

ICT CONTRACTS

Represents the field of ICT area which should be regulated maybe through separate legal provisions, one or structurally formed branch of legal acts. Nevertheless, in Serbia those rights and freedoms are partially regulated through various norms within the most of in this work presented laws and provision under law, such as by-laws. Generally, all of those norms are scattered all over the legal system, of which the most are in the sector of electronic laws and media laws, and general principles of obligation law are implemented within. We have tried to describe situation here with general remarks pointing out where they are discussed in text. General principles of civil law – regulated with law on obligation[1] are here also implemented. So the situation is following under the general principles of obligations and contractual liability and accountability this area is regulated thoroughly through this text in Chapter 1. Regulatory Framework of the Telecommunications Sector, in titles: Costing and financing of universal service obligation, Markets eligible to prior regulation and obligations of operators with significant market power, Duties of operators with significant market power. Also, it is partially regulated through Chapter dealing with Radio spectrum radio frequency, where it is tackled in title: Rights of use for the Radio-Electric Public Domain, Specific responsibilities of providing access, and especially around: Protection of rights and subscribers, Contracts and changes of terms, Value added services, Quality of service, Objection of subscriber to operator (carrier), Cost Control and other duties. Also, with this issue is dealt within the Chapter 3 Law on public information and media, where it is covered by Due Diligence. Then after all mentioned it is covered by Chapter on Law on electronic media – Electronic Media Law, especially in title Sponsorship and Responsibility for Content. With Chapter Protection of Intellectual Property in the ICT Sector, this area covered Legal Protection of Software and by presenting different various forms of copyright and related rights in cyberspace and their protection with bearing in mind that protection goes after contracting for copyright and related rights.

Also contractual area is covered by Part IV. Electronic Transactions and within that Chapter on this issue are focusing titles: Legal Status of Electronic Transactions, Defining term of electronic commerce, E-business in cyberspace, Legal issues of electronic business, Regulations on electronic business in Serbia. Area of consumer protection besides special provisions within different laws is covered by The Law

[1] "Official gazette of Socialist Federal Republic of Yugoslavia", br. 29/78, 39/85, 45/89 – Decision of Constitutional Court of SFRY and 57/89, "Official gazette of Federal Republic of Yugoslavia", br. 31/93 i "Official gazette of State Union of Serbia and Montenegro", br. 1/2003 – Constitutional charter. Especially Chapter II Part 1 Titled Contract Section I Contract conclusion articles 26- 45. Section III of the contract objective, articles 46-50, Section III titled causality articles 51-53, Section IV Capability for contracting articles 54-59, Contractual Will is covered by Section V articles 60-66, Form of contracts is dealt with in Section VI art.67-73, Contractual conditions are dealt with in Section VII. Terms and dues are within Section VIII and fore paying and contract breaking are within section IX. Chapter III is all about contractual obligations enforcement. Part II Titled Contracts within Chapter VII deals with different named and other contracts and obligations deriving from them.

on consumer's protection and even for the duty of prior notification by e-commerce. Future draft laws are presented in this work so The Future law on payment services (draft law) even deals with Submission of information in the pre-contractual stage and Amendments to the framework agreement on the proposal of payment service providers.

PART III

ELECTRONIC TRANSACTIONS

LEGAL STATUS OF ELECTRONIC TRANSACTIONS

Generally

Electronic commerce (e-commerce) has been developed in parallel with the development of information and communication technologies. During the seventies world started with electronic payments. During the eighties world has developed electronic communication. During the nineties it appeared the notion of e-commerce in general use to indicate the performance of various types of business transactions electronically. Internet trade is shorter term and it's not a synonym for electronic commerce. Broader concept of e-commerce and Internet commerce is the concept of "e-business" which can be defined as the performance of business operations using modern electronic technology. The term "electronic (digital) business" includes on-line communication, business transactions, commerce, service provision and financial services, and all other actions and activities that follow the business for which realization is necessary computer network, for example the Internet. This form of business is able to eliminate the problem of time differences and geographical distance between trading partners related to the ordering, delivery and payment of goods or services. In addition, the operational boundaries extend to goods and services that did not exist before the emergence of this type of business, or the electronic goods and services. Electronic business transaction generally can be divided into those between two entities (business to business, B2B) and those between legal entities and individuals (business to individuals, B2I). No matter who is in these transactions in the role of seller and buyer, he (she or it) can expect improvement of their status in relation to traditional business. Goods and service providers are creating strategy performance based on e-business strategy to create a global performance which will lead to lower costs, increase of competitiveness, and better customization of goods to customer needs, which should all lead to an increase in the total capacity of business. On the other hand, consumers choose quality goods tailored to their needs at lower prices by increasing the standard of service. Some authors believe that e-business can be classified into several areas: e-commerce, electronic payments, electronic communications, electronic manufacturing and electronic distribution.[1] Start of e-commerce is linked to the end of the seventies, when there was first the idea of on-line shopping. In the early eighties they first started selling the use of computer networks – that were to B2B networks in the UK and the USA. However, a milestone in the popularization of electronic purchasing and deploying B2I as the dominant form was the emergence of the first Web browser in 1994. It was Netscape Navigator, which allowed any Internet user to search the first commercial websites and presentations. It is interesting that for that first version of the software had SSL encryption and fraud protection system. Large retail chains have quickly embraced this visionary idea and started two new types of

[1] Bjelić Predrag, Elektronsko trgovanje – elektronsko poslovanje u međunarodnoj trgovini, Beograd, Institut za međunarodnu trgovinu i privredu, 2000, p. 4

activities – online banking and e-commerce. Pizza Hut, a chain of pizzerias, was the first to allow the sale of products over the Internet. After it followed other industrial and retail chains, and e-commerce soon was not limited to large corporations, on the contrary – some of the first ideas on-line sales have local scope and related to the sale of flowers and a subscription to the electronic editions of different newspapers. During the same year, there were rapidly evolving businesses and models of cars were sold over the Internet, as well as the porn industry. The following year have begun to work two Internet radio stations and also started the work of one of the biggest sites when it comes to e-business in general eBay. Since then, until now, e-commerce world is recording constant annual growth. The use of digital devices in e-commerce enables classical business abuses such as fraud, financial fraud or tax evasion in a new way, which is necessary to be regulated separately, and to incriminate new forms of actions, because the rules and control mechanisms of classical operations cannot be applied.[2] Meanwhile, system protection and monitoring of shipments which were ordered over the Internet has evolved considerably, making it possible and delete any limitations of on-line purchase of the world – and Serbia are slowly but surely moving towards the group of countries in which is possible delivery of goods purchased on-line anywhere in the world.[3] E-business does not recognize state borders, which complicates the collection of taxes and revenues in many countries around the world. When we add to this the so-called "electronic cash", which is the main form of payment for this business problem becomes very complex, since technical capabilities allow almost instantaneous transfer of cash from one account to another, from one country to another without recording the transfer. In addition, many buyers and sellers do business only with their e-mail addresses that are on free servers and do not contain information about their physical addresses. As electronic commerce brought some products that do not have physical characteristics (e.g., software) which are available only in electronic form on the e-mail to it we can address the question which arises – how they can be taxed.

Legal Framework

Introduction

The expansion of electronic commerce has opened a number of new issues that should be legally regulated. Conclusions of electronic contracts require a precise definition of determining the authenticity of electronic messages and authentication of electronic communications, and also require the definition of procedural rules at the conclusion of electronic contracts. Many misuses of electronic data, misrepresentation of the Internet, electronic fraud, electronic sabotage, carrying viruses into computer

[2] Dimitrijević, Predrag, Pravo informacione tehnologije - osnovi kompjuterskog prava, SVEN, Niš, 2009, p. 177.

[3] This road for Serbia would be much shorter and simpler if our country wasn't famous for mass usage of stolen data about payment cards, especially in period of massive usage of computers and internet at the end of nineties of the last century and in the beginning of 21st century. Multinational companies which deal with online transactions, as for instance PayPal system, because of that didn't wont to come to Serbia officialy and thus make possible electronic payment to residents of Serbia under the same conditions as everywhere in the world, while big websites specialized for for online sale denied Serbia place among other countries with possible delievery, or charged for delievery enormous amounts of money much bigger than orders.

systems, unauthorized changes to electronic data, linking without prior permission, and many other illegal acts in electronic commerce demanded to be legally regulated. Non-delivery of ordered goods over the network, poor quality of delivered goods, and many other ways to harm consumers in electronic commerce demanded that legal norms in the best possible way protect the growing number of consumers who purchase goods through virtual stores, and payments which were made electronically. Particularly important issues are the protection of patents, trade secrets, matters of taxes and jurisdictional issues in the conduct of proceedings, and of course, it must be legally regulated under national legislation, as well as internationally. The first steps in the field of legal regulation of electronic commerce have made international organizations, especially the United Nations and the European Union.[4] After the international organization have established bases of legal regulation and national levels have begun to bring any legislation on issues of e-commerce. In addition to legislation that directly regulates issues relating to electronic commerce issues such as: electronic signatures, electronic contracts, electronic documents, etc... For the area of e-business is of great importance and other legislation governing the issue of intellectual property protection, data protection, privacy, consumer protection, revenue, etc...[5]

Types of payment services are prescribed by Article 4 NZPU. According to it, payment services include:

1) services enabling payment of cash to the payment account, as well as all the services required for opening, maintaining and closing of that account;

2) services that enable the payment of cash from the account, as well as all the services required for opening, maintaining and closing of that account;

3) a transfer of funds from the payment account and to the payment account, as follows:

(1) transfer approval

(2) direct debit, including one-off direct debit,

(3) using a credit card or similar device;

4) service of execution of payment transactions where the funds have been secured by the loan to the payment service user, as follows:

(1) transfer approval

(2) direct debit, including one-off direct debit,

(3) using a credit card or similar device;

5) issuing payment instruments and/or acceptance of these instruments on the basis of which the payment service provider of the recipient of payment enables the execution of payment transactions initiated by the payer using a particular payment instrument;

6) a performance of remittances in which the payment service provider of the payer receives funds without opening a payment account of the payer or the recipient of the payment, only to place those resources at the disposal of the recipient to pay or

[4] United Nations Commission on International Trade Law (UNCITRAL) adopted the model law regulating electronic commerce of 1996; a Model Law on Electronic Signature 2001 The European Union in 1997 adopted the "European initiative in the field of electronic commerce", in 1999 adopted the Directive on Electronic Signatures, and in 2000 adopted the Directive on electronic commerce.

[5] Efraim Turban, at all, Electronic Commerce : A Managerial Perspective, New Jersey, 2000, p. 342.

to transfer these funds to the service recipient's payment service, which puts them at the disposal of the recipient payment;

7) a performance of transactions for which the payer approves the use of telecommunications, digital or information-technology device and the payment is made the operator of telecommunication, digital or information-technology network, which acts only as an intermediary between the payment service user and the supplier of the product or service provider.

Credit transfer is a payment service in which the payer with its payment service provider initiates the execution of one or more payment transactions, including the issuance of a permanent order.

Direct Debit is a payment service in which the recipient of the payment based on the payer's consent is to initiate the payment transaction to debit payment account. Payer may give this consent to Payee, its payment service provider or the service recipient's payment service payment.

Legal framework in Serbia

In Serbia in the previous period legislator has passed legislation on certain issues of electronic commerce. Legislation that facilitate electronic commerce: the Law on Electronic Signature[6] Law on Electronic Commerce[7] and Law on Electronic Documents.[8] By-laws that enable e-business are: Rules on Technical, procedures for creating qualified electronic signature and the criteria to be fulfilled by means of the formation of qualified electronic signatures,[9] the Regulation on detailed conditions for issuing qualified electronic certificates,[10] the Rules of Registry certification bodies for issuing qualified electronic certificates in Serbia,[11] Rules on filing tax returns electronically,[12] Decision on Electronic payment Transactions,[13] Decision on electronic signing of documents submitted by banks to the National Bank of Serbia and the Guidelines for the Implementation of Decision on Electronic payment Transactions,[14] Decision on electronic Payment[15] traffic rules for the handling of electronic bids and manner of conducting electronic auctions in public procurement procedures.[16]

Law on electronic commerce

Law on Electronic Commerce was adopted by the National Assembly of the Republic of Serbia on 29 May 2009. This Act created the legal basis for the equalization of

[6] Official gazette of RS, nr. 41/2009 i 95/2013).
[7] Official gazette of RS, nr. 51/2009.
[8] Official gazette of RS, nr. 26/2008.
[9] Official gazette of RS, nr. 26/2008.
[10] Official gazette of RS, nr. 26/2008.
[11] Official gazette of RS, nr. 127/2003.
[12] Official gazette of RS, nr. 113/2013.
[13] Official gazette of RS, nr., 28/2009 i 47/2009. And decision in Official gazette of RS, nr. 24/2007, 31/2007, 38/2010.
[14] Official gazette of RS, nr. 50/2009.
[15] Official gazette of RS, nr. 57/2004.
[16] Official gazette of RS, nr. 50/2009.

electronic business forms with classical direct form, which allows a significant competitive advantage to enterprises and state administration. The area of e-commerce has not been regulated by the law, until this law was passed, which was a major obstacle in the overall economic development of Serbia. Law on Electronic Commerce is a complete novelty in our legislation because the first regulates the legal area trade in goods and services, which are conducted through electronic networks, particularly via the Internet. The aim of the law is to provide legal certainty for all participants in electronic commerce, so as to regulate the obligations and responsibilities of participants in commercial activities that are offered on the Internet. With the aforementioned, there are laws on electronic signature and electronic payment, and that the enactment of this Act completing the legal framework for the operation of e-business in Serbia. When it comes to the business of legal entities, one of the most significant innovations introduced by law in our legal system is the legal institution of contract in electronic form, and because those present a (way) medium of concluding the contract and the conditions for its validity are crucial for any traffic that is carried over Internet. With regard to the verification of the identity of the traffic on the Internet, it is very important previously passed the Law on Electronic Signature, which may be a condition of validity of the contract in electronic form. Enrolment of the first certification bodies for issuing qualified electronic certificates, all the conditions were created for the application of electronic signatures in practice. The adoption of the Law on Electronic Commerce made a big step towards regulating the electronic commerce, and purchase goods and services through the websites of local companies that sell them on the Internet where you can pay with credit cards. Contract in electronic form was simply defined as a contract that natural and legal persons conclude, send, receive, terminate, cancel, you access and display electronically using electronic means. It is therefore a contract whose contents and form are identical to that determined by other, specific legislation. Each contract that is concluded electronically must comply with certain norms of the law to be valid and enforceable – this refers to its content (the essential elements of contracts, prohibited items contracting, etc...) and its form - the way of negotiation, offer and response to offer, and the like; In addition, the contract in electronic form is equal to the other contracts that are concluded in writing. What makes it different from "regular" contract is a way of conclusion, or means of electronic communication as exclusive tools used during the procedure of concluding the contract. In order for some entity to perform electronic sales it must be registered like any other business entity. It is possible to imagine situations, that a company as an additional method of selling their product offering e-commerce, in addition to the classical distribution, and sale of goods which is carried in stores. It is important to note that the Act, by the express provision of Article 2, applies to the protection of personal data, the activity of the notary and other related professions regarding the use of delegated public powers, restrictive agreements in terms of the competition, taxation, representation of parties and protection of their interests before the courts, nor the games of chance with cash investments, including lottery games, casino games, betting games and gambling on slot machines, a special law provides otherwise... With these questions apply regulations given in particular legal texts. When it comes to the types of contracts that may be concluded in electronic form, the Act contains a provision that excludes certain types of legal

works, which is primarily due to its particular importance, may still be concluded only in classical writing. These are contracts which relate to:

1) legal issues that transfer of ownership rights to real property or which establish other rights over immovable property;

2) statements of the parties and participants in the procedure of last will, form of last will, agreements on the transfer and distribution of assets for life, lifelong maintenance contracts and agreements in connection with inheritance, and other agreements in the field of inheritance law;

3) agreements establishing property relations between the spouses;

4) contracts for the disposal of property of persons deprived of their legal capacity;

5) gift contracts, surety and pledge;

6) other legal proceedings or actions, for which a special law or pursuant to law enacted legislation explicitly determined using handwritten signatures on paper documents or verification of handwritten signatures[17] Law on Electronic Commerce further defines the required data and information before signing the contract, the availability of the contract, confirmation of receipt, the time of conclusion of the contract, the liability of service providers, temporary and permanent storage. Since the Electronic trading is based on the principle of mass, contracts in this way conclude are the formulary contracts. They must contain sufficient information in order not to mislead the customer in the case of purchases, its properties, prices, or other essential element of legal flaws. Therefore, the seller (as service provider) shall be the potential buyer (service user), prior to the conclusion of a service contract, provide a clear, comprehensible and unambiguous data and information on the process to be applied at the conclusion of the contract, contractual provisions, general conditions (if they are an integral part of the contract), the language in which the contract can be signed, codes of conduct in accordance with that act providers and how these codes can be viewed electronically, and to provide the technical means for identifying and correcting erroneous input data in the message prior to its delivery or sending. The service provider is still required to ensure that the text of the contract and the provisions of general business conditions which are an integral part of the contracts concluded electronically made available to service users in a way that facilitates their storage, reuse and reproduction, and that without delay, electronically, by a special electronic message, acknowledge the receipt of electronic messages containing the offer or acceptance of the offer to conclude a contract.[18] These provisions apply to contracts made and entered into on-line, but not to contracts concluded by exchange of electronic mail or other form of personal communication two or more persons made electronically! This solution makes sense primarily because during the on-line purchase access is done to predefined models of contracts, with little or no room for changing them. In direct communication, people who have no intention of concluding the contract will be in the correspondence exchanging all the information that they consider relevant, and themselves affect the conditions of the contract and its contents – it is therefore that in this case where it can't be prepared

[17] Article 10. Law on Electronic Commerce.
[18] Articles 12-14 of Law.

in advance and offered a potential buyer on a “take it or leave it” basis. The time of conclusion of the contract is also one of the important elements of each legal transaction. Contract in electronic form shall be considered concluded that moment when the bidder receives an email containing a statement offered to accept the offer. The offer and acceptance of the offer, as well as other statements of will made electronically are considered received when they are sent to the person who can access it. .

REGULATION OF ELECTRONIC SIGNATURES AND CERTIFICATION SERVICES

Law on electronic signature

Electronic Signature Law was passed in 2004, and is the first rule in Serbia, which addresses some of the aspects of e-commerce, e-business, and the like. Serbia had to wait until 2009 when the most important body of law in this area was completed by passing the other two aforementioned laws. By them was regulated the use of electronic signatures in legal matters and other legal actions, operations, as well as the rights, obligations and responsibilities in relation to electronic certificates. Their provisions are applied to the intercourse of organs, communication with the parties, delivery and decision making in electronic form in the administrative, judicial or other proceeding before a state authority – if the law governing the procedure has prescribed use of electronic signatures. Potential applications of electronic signatures could cover the entire state government, local government, and the judiciary. Electronic Signature Law introduces several new concepts in the Serbian legal system:

- "Electronic document" – a document in electronic form to be used in legal matters and other legal actions, as well as administrative, judicial or other proceeding before a public authority;
- "Electronic signature" – a collection of data in electronic form which are attached to or logically associated with an electronic document and serve to identify the signatory;
- "Qualified electronic signature" – an electronic signature that reliably guarantees the identity of the signer, the integrity of electronic documents, and prevents subsequent denial of responsibility for their content, and who meets the requirements established by law;
- "Digital certificate" – an electronic document confirming the relationship between the data for electronic signature and the identity of the signer;
- "Qualified Electronic Certificate" – an electronic certificate issued by the certification authority for issuing qualified electronic certificates and contains data provided by the law;
- "User" – a legal entity, entrepreneur, state authority, territorial autonomy, local government body or natural person which has issued an electronic certificate;
- "Certification Authority" – a legal entity that issues electronic certificates.

Electronic signature, therefore, is used to identify the signer. He (she or it) must provide at least two things: to show that the person who is listed as a signatory to the signature actually placed signature and that the contents of the document are corresponding to the content that existed at the time of signing. These two problems from the very beginning accompany an electronic signature, which are directly related to

the issue of security. To better understand how the electronic signature is used, one can draw a parallel with classical cryptography from the past: it was not unusual, especially in a time of war, for confidential military contracts to be transmitted by telegraph encrypted. The party that initiates the deal would send the offer, and the other side had to agree with her in cryptic form, and thus they would conclude valid contract. Also offer and an answer to the offer were sent in the encrypted form, so that the enemy could not reveal their contents. The key to reading these messages have both sides, but not the enemy, so that they can use it to decrypt and discover the true meaning of incoming messages. The same principle, but in a far more advanced technological level, is used for electronic signatures: the signature of "encrypted" and decryption is done using electronic certificates. The "ordinary" electronic signature may be encountered in their daily work, and all PC users can make it with the help of appropriate software. It is a simple designation certifying authorship of an electronic image, text, etc.. However, this signature is easy to forge, copy, and then (mis) used. That is why the only reliable version of the electronic signature indicates "qualified electronic signature", which is in the foreign literature also referred to as "digital signature". This is a signature that was created to perform certain procedures and protocols, and the use of appropriate software. The qualified electronic signature is not physically match the signature – expression signature is used as a marker of something unique, according to what is undeniably can establish identity. Hence, in addition to the term electronic signature sometimes used the term "digital fingerprint", or classical language "coded message". The difference between reliable and unreliable electronic signature therefore is the quality of care, and the information that it carries. If viewed as a hypertext, then its authenticity can (and must) establish through deciphering. As we have shown, digital certificate is an electronic document confirming the relationship between the data for electronic signature and the identity of the signer; to be reliable, electronic certificate must be "qualified" – issued by the Certification Authority for issuing qualified electronic certificates, and contains information provided by the Law on Electronic Signatures. Qualified electronic certificate must contain: label that it is a qualified electronic certificate; set of data that uniquely identifies the entity that issued the certificate; set of data that uniquely identifies the signer; data for electronic signature verification, which correspond to the data for creation of qualified electronic signatures that are under the control of the signatory; information about the start and end of the validity of electronic certificates; identification badge of issued electronic certificate; qualified electronic signature of the certification authority that issued the qualified electronic certificate; restrictions on the use of the certificate, if any. Electronic certificates are issued by the certification body, which can be any legal entity which is in accordance with the law registered to perform these activities. The competent ministry maintains a single register of all certification bodies, and they must meet a number of technical and personal requirements that are described in more detail by the Law on Electronic Signatures (Article 18 of the Law). Certificates can be issued by government authority.

Overall, the importance of passing this law is exceptional when it comes to electronic communication. Electronic document cannot be denied validity or probative value, just because it is in electronic form, except in those cases where the law requires a signature of the required forms. This is therefore a regulation that allows for the

introduction of electronic documents in everyday legal transactions without worrying about their originality and validity.

Law on electronic document

Law on Electronic Document was adopted by the National Assembly of Serbia on July 8, 2009. This law defines the procedure for dealing with the electronic document, receipt of such documents, the issuance of a receipt and a way of keeping duplicates. The aim of the law is that such a record achieves full legal force and relevance. Prior to the enactment of the Law on Electronic Document and Law on Electronic Commerce, there was a law on electronic signature, which gave a document with an electronic signature the same status that has paper document. However, there weren't developed procedures for handling such a document, so it was necessary to adopt the Law on Electronic Document. Electronic document is a set of data consisting of letters, numbers, symbols, graphics, audio and video files in the brief, written, decision, document or any other document, which draw up legal entities and natural persons or authorities for use in legal or administrative, judicial or other proceedings before the authorities, if made electronically, digitized, sent, received, stored or archived in an electronic, magnetic, optical or other media.[19] Thus, the electronic document is considered to be the one that is written in an electronic format and signed by electronic signature, for use in legal transactions, or a procedure. Given that the office operations under the document in the classical sense as documents in paper form, in example those containing written and possibly graphic records must be immediately noted that the electronic document can be significantly wider content, such as video and sound recordings; the notion of an electronic document may be considered as other categories of records, such as computer programs. Each document in the classical form can be converted into an electronic format (e.g. Scanning, re-typing, etc...).[20] If this is done in a way that guarantees its authenticity and in accordance with legal procedures, and if the relevant law provides otherwise, classical and electronic form of a document have the same importance in legal matters and all types of proceedings before state agencies and courts. According to the Law on electronic document, electronic document cannot be used in the following legal matters:

1) legal contracts that transfer of ownership rights to immovable property or which establish other rights over immovable property;

2) statements of the parties and participants in the procedure of last will, form of last will, agreements on the transfer and distribution of assets for life, lifelong maintenance contracts and agreements in connection with inheritance, and other agreements in the field of inheritance law;

3) agreements establishing property relations between the spouses;

4) contracts for the disposal of property of persons deprived of their legal capacity;

[19] Article 2 of Law.

[20] Legal term for transferring in electronic form is digitalization – transfer of documents from other forms in digital (electronic) form (article 3, point 1.of Law).

5) gift contracts;

6) other legal proceedings or actions, for which a special law or pursuant to law enacted legislation explicitly determined using handwritten signatures on paper documents or verification of handwritten signatures.[21]

The Law on Electronic Documents incorporated the provisions on time stamp because the Regulation on office operations and because of the Law on Administrative Proceedings the time of arrival the documents it is important part of the contract. Time stamp is officially time associated with electronic document or group of electronic documents, confirming the contents of an electronic document at that time or the content of each document in the group at that time. Electronic certificates for signature of time stamp issued by the certification body registered in the register, or register with the competent authorities, in accordance with the law governing electronic signature. Time stamp joins the electronic document based on the request for the establishment of the time stamp. The request for the establishment of the time stamp contains certain information from the contents of an electronic document or electronic signature. The data structure of the time stamp contains: time stamp identifier of the issuer; serial number of the time stamp; duration of the forming of time stamp; facility for the establishment of the time stamp; electronic signature of time stamp data structure; algorithm identifier for time stamp electronic signature; identifier of the electronic certificates through which we can verify the electronic signature time stamp. Time contained in the time corresponding to the time of formation of the trademark of the mark, with a difference of less than one second, compared to UTC (Universal Time Coordinate) time scale.[22] Electronic document shall be prepared by using any accessible and useful computer technology, unless otherwise specified. This means that the electronic documents are formed by using a series of user programs that are available to any home or business computer, such as. MOWord, MOExcel, Adobe Reader, etc... The content of the file or group of files which arises in this way is not decisive for the qualification of the file or group of files as electronic documents – is important to their purpose, for which they were created and / or how they can be used. It will be regarded as any electronic documents file that for example represents the contract document, the decision of a state authority in the administrative proceedings. But the electronic document can be considered as any form of electronic information that can be used in any court proceedings, for example digital (electronic) evidence – in this case, it may be photos, various forms of electronic communication, and the like. Electronic document may be other electronic files that may arise from the product of action of a public body in the process – e.g. electronic recording (audio, video, or both) of the trial to trial. Because of all this, the law distinguishes between internal and external form of display of electronic documents internal form refers to the technical and software form of writing its contents (that is the file format – e.g. Jpeg, .doc, .mp3 and technical preconditions for the origin and reproduction – the appropriate user programs); external form refers to the perception of the content of the electronic document to the outside world - whether it comes to sound documents, video recording, a written document, graphic document, images, etc... As it was already mentioned, every electronic document may be

[21] Article 4, paragraph 3 of the Law.

[22] Articles 14-19. Of the law

the original or a copy. The original is the one that was originally created in electronic form, and a copy of a document that was created by digitizing the original document, whose form is electronic. In order for copy to has the same legal force as the original document digitization needs to be conducted by a public authority in the enforcement of its powers and authorities, or a legal person or an entrepreneur in the performance of their activities, and are identity to the original document must verify by qualified electronic signature the authorized agent of the government, or authorized person, legal person or entrepreneur. This is a completely logical solution when one takes into account the provision of security in legal matters – it's not enough to simply overwrite an original document, but it must be applied those safeguards which were mentioned in part with electronic signatures and electronic commerce. Given the importance of electronic documents, the law gives special provision to it: "In the performance of electronic documents are applied appropriate technological processes and equipment that ensure the protection of these documents in accordance with the law governing archival materials, regulations on office operations and international standards in the field of document management."[23]

[23] Article 13 of the law.

LEGAL ASPECTS OF ELECTRONIC BANKING

Future law on payment services (draft law)

Basically, in this moment there is ongoing reform in area of payment services in digital environment so it is of utmost importance to give scope of this law in order to understand its value and impact in whole payment system within market of Serbia. Law on payment services, the draft of which was presented during 2014, it is intended to regulate the conditions and the manner of payment services, electronic money, payment systems and supervision of the implementation of the provisions of this Act. For the purposes of this Law following terms shall have the following meanings:

1) payment transaction means a payment, transfer or disbursement of funds initiated by the payer or payee, and is performed regardless of the legal relationship between the payer and the recipient of the payment;

2) the payment order means an instruction of the payer or the recipient for paying its provider of payment services, which requires the execution of a payment transaction;

3) payment account means an account that is used for the execution of payment transactions, a leading provider of payment services for one or more payment service users;

4) payment instrument means any personalized agent and/or set of procedures agreed between the payment service user and the payment service providers and that the user is using to issue payment orders;

5) payment instrument for the payment of small cash value means the payment instrument, in accordance with the framework agreement on payment services, applies only to the execution of individual payment transactions whose amount is not greater than 3,000 dinars, or whose total spending limit does not exceed 15,000 dinars, or the total value of funds stored on the payment instrument at any time does not exceed 15,000 dinars;

6) The payment service provider shall mean a natural or legal person who uses or has used the canvas service as Payer and/or Payee or the provider of payment services addressed in order to use these services;

7) payer means a natural or legal person who from their wage bill has issued a payment order or giving consent to execute a payment transaction on the basis of a payment order issued by the payee, and if there is no payment account – a natural or legal person who issues a payment order;

8) payee means a natural or legal person designated as the recipient of funds which are the subject of a payment transaction;

9) consumer means a natural person who concludes a contract or payment services relating to electronic money for purposes other than its intended business or other commercial activity;

10), an entrepreneur means a natural person who is not a consumer or (business capable) natural person engaged in business to generate revenue, in accordance with the law regulating companies and other laws;

11) funds means cash, funds in the account, and electronic money;

12) cash means banknotes and coins;

13) electronic money means electronically (including magnetically) stored monetary value that makes money claim against the issuer of the money, and was issued after the receipt of funds for the execution of payment transactions, and it is accepted by the physical and/or legal person who is not the issuer of the money;

14) the holder of the electronic money means a natural or legal person to whom is issued or has been issued electronic money, or a natural or legal person who has contacted the issuer of electronic money in order to issue the money, as well as any other individual or entity that has a monetary claim from Section 13) of this paragraph;

15) business day is a day or part of a day in which payer's or recipient's payment service provider that participates in the executing of the payment transaction operates to enable the execution of payment transactions to its payment services;

16) the value date is the reference date and the reference time that the provider of payment services uses in the calculation of interest on funds charge or approve the payment account;

17) reference rate is the rate by which the computation is performed in exchange rates, which was made available to the payment service provider, or which comes from publicly available sources;

18) The reference interest rate is the rate on the basis of which the interest is calculated and publicly available and is determined independently of the unilateral will of providers and payment service users who have concluded an agreement on payment services;

19) Unique identifier means a combination of letters, numbers and/or symbols that the payment service provider shall determine for the payment service user and that is used the payment transaction for unambiguous identification of the user and/or its payment account;

20) a means of distance communication means any provider and the payment service user may use the conclusion of a payment services when they are not physically present at the same time at the same place;

21) permanent data carrier means any device that allows the user to save the data that is assigned to him (her or it), that allows access to these data and allows to reproduce in an unmodified form in the period corresponding to the purpose of storage;

22) domestic payment transaction means a payment transaction in which payers payment service provider and the payment service provider of the recipient provide service in the territory of the Republic of Serbia;

23) international payment transaction means a payment transaction in which a payment service provider offers this service on the territory of the Republic of Serbia and the other on the territory of a third country, as well as the payment transaction in which the same payment service provider of the service to a user of payment services

provided in the territory of the Republic of Serbia, and in the same or another user of payment services in the territory of a third country;

24) home state means the state in which the registered office of the legal person;

25) headquarters means a place that is registered as the seat of the legal person, and if a legal entity in accordance with the regulations of his country has no registered office – a place from which it manages its operations;

26) the host State means a State that is not a parent state in which the entity provides services through a branch or any other person or which directly provides services;

27) qualified participation exists when one person has:

(1) direct or indirect right or ability to achieve at least 10% of the voting rights in the legal person, or direct or indirect ownership of at least 10% of the assets of the entity, or

(2) the possibility of effective exercise of significant influence on the management of other legal entity;

28) controlling participation exists when one person has:

(1) direct or indirect right or ability to achieve at least 50% of the voting rights in the legal person, or direct or indirect ownership of at least 50% of the assets of the entity, or

(2) the choice and/or removal of at least half of the members of management or supervision entity of the legal person, or

(3) the possibility of effective exercise of dominant influence on the management of other legal entity;

29) the parent company of a legal person means a company which has a controlling share in the legal person;

30) Subsidiary of a legal person means a society in which the entity has a controlling participation;

31) group of companies is a group consisting of the parent company, its subsidiaries and entities in which own capital the parent company and/or its subsidiaries have a share, as well as companies that are connected by common management;

32) government-related joint control are companies that are not affiliated relationship of parent and subsidiary companies, nor share in the capital as defined in Section 31) of this paragraph, and include:

(1) companies that are managed in a uniform manner in accordance with the agreement concluded between the companies or statutory provisions or incorporation documents of these companies, or

(2) society in which the same people make up the majority of members of management or supervision;

33) a close correlation indicates the relationship between two or more legal entities and/or individuals when:

(1) one of them directly or indirectly through participation in the subsidiary has the right or ability to achieve at least 20% of the voting rights in a legal entity, or ownership of at least 20% of the capital in a legal entity,

(2) one of them has a controlling share in another legal entity,

(3) there is a permanent connection of these people with the same third party based on the controlling share;

34) bank means a bank registered in the Republic of Serbia, which has a license from the National Bank of Serbia, in accordance with the law regulating the banks;

35) an electronic money institution is a legal entity registered in the Republic of Serbia, which has a license from the National Bank of Serbia for issuing electronic money in accordance with this Law;

36) the payment institution is a legal entity registered in the Republic of Serbia, which has the license of the National Bank of Serbia for the provision of payment services as a payment institution, in accordance with the law;

37) payment system means a system for the transfer of funds among participants in this system, with a written and standardized procedures and rules for processing and netting and / or settlement of the transfer order to the payment system applicable to all participants in the system.

The provisions of the draft law on payment services (NZPU) relating to payment service users who are legal persons also apply to branches of foreign legal entities that are registered with the competent authority in the Republic of Serbia.

Exclusions are provided for in Article 3 NZPU, according to which the provisions of this Act shall not apply to:

1) payment transactions executed exclusively in cash directly from the payer and the recipient of the payment;

2) payment transactions executed through a representative authorized to negotiate or conclude contracts of sale of goods or services in the name and for the account of the payer or the recipient of the payment;

3) transport of cash, as well as its collection, processing and delivery, performing enterprises in accordance with the law;

4) payment transactions consisting of a collection and delivery of cash made by taxable persons who are not undertakings within the non-profit or charitable activity;

5) services in which the payee immediately after the execution of the payment transaction, gives cash to the payer as part of payment transactions related to the payment of goods or services, and at the express request of the payer which was given just before the execution of the payment transaction;

6) exchange operations, which include operations of buying and selling foreign cash for cash;

7) payment transactions based on any of the following documents written on paper:

(1) check in the sense that is determined by the law governing the check payments,

(2) check which is established by foreign regulations, and its contents and effect is similar to a check of sub-paragraph (1) of this clause,

(3) voucher or other certificate which enables its holder to pay for goods or services of the issuer of the voucher and the certificate or payment by another person

with whom the issuer has contracted receipt of the voucher and the certificate as a way of paying for goods or services (eg. present - vouchers, vouchers for food and other related certificates),

(4) passenger check,

(5) postal money order in accordance with the regulations governing the provision of postal services;

8) payment transactions carried out between the participants in the payment system and settlement system for financial instruments, which are in connection with participation in these systems, as well as payment transactions carried out between the participants in the payment system and payment service providers who did not participate in that system;

9) payment transactions related to the exercise of rights and fulfilment of obligations arising from financial instruments, including the payment of dividends and other payments, purchase or sale of securities - if such transactions are carried out, participants in the system for the settlement of financial instruments or other persons, in accordance with regulations, provide investment services and custody services in relation to financial instruments of clients;

10) technical services to support the provision of payment services, including processing, storage and data protection, authentication, and data entities providing services related to information technology and communications network, provision and maintenance of terminals and devices used for payment and other services - if the provider of the above services at any time does not have the funds to be transferred or to dispose of them;

11) payment transactions made on the basis of instruments that are paid in purchase of goods and services only in the premises of the issuer of the instrument or, in accordance with the agreement concluded with the issuer, with a limited network of sellers of goods and services or for a limited range of goods and services;

12) payment transactions made via the telecommunication, digital or information technology device, wherein the purchased products or services are delivered and used by the device, provided that the telecommunication, digital or information-technology operator does not act only as an intermediary between the payment services and the seller of the product or service and services;

13) payment transactions between payment service providers and payment transactions between payment service providers and their agents or branches, if carried out on their behalf;

14) payment transactions between a parent company and its subsidiary company or between subsidiaries of the same parent company, if you are running only through the payment service provider that is a member of the same group of companies;

15) a cash withdrawal at ATMs which providers are acting on behalf of and for the account of one or more issuers of credit cards, provided that the service did not conclude a framework contract for payment services with a clients who withdraw cash from the accounts and payments that do not provide another canvas service defined by this Law;

16) electronic money stored on the instruments referred to in Section 11) of this article, or to be used for the execution of payment transactions from Section 12) of this Article.

This area is governed by Article 17 of NZPU, and by it payment service provider is obliged to the payment service user, within a reasonable time prior to the conclusion of a framework agreement, to submit the information identified as mandatory elements of the contract in accordance with Article 16 NZPU, and in a manner that will enable the user to become familiar with the conditions relating to the provision of payment services, as well as to compare the offers of different providers of payment services and to determine whether these terms and services meet their needs.

Payment service provider is required also to submit to the payment service user information in a way which shall not mislead with respect to the conditions relating to the provision of payment services. Payment service provider is also obliged to submit to the payment service user information on paper or another durable medium. The provider of payment services to payment service user may submit the requested information by submitting a draft framework contract that contains this information.

Amendments to the framework agreement on the proposal of payment service providers

If the payment service provider proposes to amend the provisions of the framework agreement, it is obliged to submit to the payment service user a proposal of the amendment no later than two months prior to the proposed date of commencement of their application. After receiving the proposal, the payment service user may agree to the proposed amendments to produce legal effect prior to the proposed date of commencement of their application. By the Framework contract it can be established that it will be considered that a user of payment services agreed with the proposal, if before the date of application of the proposed amendment was not informed of payment service providers to come up with this proposal is not agreed, as the payment service provider shall inform the user payment services simultaneously with the submission of the proposal. In this case, the payment service provider is obliged to the payment service user to, simultaneously with the submission of proposals in that paragraph, make clear notice of his right to terminate the framework contract before the date of application of the proposed amendments without paying fees and other costs, if he (she or it) does not accept this proposal. Payment service provider is obliged to the payment service user to submit a proposal in writing.

Information for the Payee after the execution of individual payment transactions

Article 23 of NZPU elaborates further obligations regarding the provision of information. Payment service provider of the recipient of payment which based on the

framework agreement executed single payment transaction shall immediately upon execution of this transaction submit the following information to Payee:

1) the reference mark or other information that the recipient of payment permits the identification of individual payment transactions, as well as information on the payer and other data that are transmitted with the payment transaction in accordance with the law;

2) the amount of the payment transaction in the currency in which the payment is authorized recipient's account or payment in the currency in which the funds are made available to the recipient of the payment;

3) the amount of any fees charged to the recipient to pay for the execution of individual payment transactions, and if the provider of payment services collectively charges these fees - and the type and amount of each fee that makes the collective benefit;

4) The amount of interest payable by the payee, if such interest is paid;

5) if a currency exchange is done – rate of exchange that is in the execution of payment transactions using payment service provider of the recipient's payment and the amount of the payment transaction before replacing the currency;

6) the credit value date of the payment the beneficiary's payment or the date when the funds are made available to the recipient of the payment.

The obligation of payment service providers of recipient of payment to provide the information specified in the preceding lines is subject to the provisions of Article 22, para. 3 to 5 of NZPU.

Pre-contractual information and a framework agreement on the payment instrument for the payment of small monetary value

By article 24 attentions is drawn to the low value contracts. Notwithstanding of the Article 17, paragraph 1 of NZUP, the payment service provider shall, prior to the conclusion of a framework agreement on the payment instrument for the payment of small monetary value, to submit the payment service user the following information:

1) information on relevant characteristics and possible ways to use this payment instrument;

2) information on the responsibilities of payment service providers and payment service users for unauthorized, non-executed or incorrectly executed payment transaction;

3) information about the fees that the provider of payment services charge the payment service user;

4) information on other relevant circumstances to the payment service necessary for a decision on the conclusion of a framework agreement on the payment instrument;

5) information on where the payment service user other available information referred to in Article 17, paragraph 1 of NZPU.

Notwithstanding Article 16, para. 1 and 3 of NZPU, a framework agreement on the payment instrument for the payment of small monetary value must contain

the elements described or referred information, and does not have to be concluded in writing.

Also, as an exception to Article 18 of NZPU, by a framework agreement on the payment instrument for the payment of small monetary value can be determined that the payment service provider is not required to amend the framework agreement proposes in writing.

The duty of prior notification by e-commerce

Article 29 stipulates that the seller shall, before entering into a contract at a distance that as the subject has a sale of goods or provision of services by electronic means to inform consumers about the data referred to in Art. 16 and 28 of ZP and to provide an easy way to:

1) recognize, store and reproduce the final text of the future agreement;

2) to detect and correct errors in data entry before sending the order form;

3) electronic access to the code of conduct which obliges merchants.

Trader has the obligation to the consumer before sending the order form in a clear and understandable way to:

1) make available to the consumer to find the instruction manual for conclusion of a contract with a description of actions that the consumer needs to do in order to conclude the contract;

2) inform the consumer about the intention of storing the signed contract and the manner in which the contract can be accessed;

3) inform the consumer about the manners in which can him (or she) to spot and correct data entry errors;

4) inform the consumer about the language in which the contract can be concluded.

PROTECTION OF USERS OF ELECTRONIC SERVICES

GENERALLY

Subject

Article 1 of the Law on consumers protection (ZP) provides that it regulates the basic rights of consumers, the conditions and means of consumer protection, the rights and obligations of associations and unions whose field of action is achieving the objectives of consumer protection, establishment of a system-of-court settlement of consumer disputes, as well as the rights and obligations of public authorities in the field of consumer protection.

Basic consumer rights

Basic consumer rights, according to the ZP are (Article 2):

1) meeting basic needs - access to the most essential products and services, such as food, clothing, footwear and housing, health, education and hygiene;

2) security - the protection of goods and services which are hazardous to life, health, property or the environment or goods whose possession or use is prohibited;

3) awareness - access to accurate data that are necessary for a reasonable range of the offered goods and services;

4) choice - a choice between more goods and services at reasonable prices and with quality assurance;

5) participation - representation of consumer interests in the process of adopting and implementing policies to protect consumers and the possibility that over consumer protection associations to be represented in the process of adoption and implementation of consumer protection policies;

6) legal protection - the protection of consumer rights in the statutory procedure in case of the violation of his (or her) rights and pecuniary and non-pecuniary damage he causes a trader;

7) education - to acquire basic knowledge and skills necessary for the proper and reliable range of products and services, as well as knowledge of basic rights and duties of consumers and the manner of their implementation;

8) to a healthy and sustainable environment - living and working in an environment that is not harmful to the health and well-being of present and future generations, and access accurate information necessary to assess the risk to the environment poses to the health and welfare of the people.

Binding nature

The consumer may not waive the rights set forth in ZP. Certain provisions of the contract between the consumer and the trader which were concluded contrary to the provisions of this Act at the expense of consumers are null and void (Article 3.). Nullity of certain provisions of the contract does not involve the nullity of the whole contract if the contract may have legal effect without that provision.

The offer for the conclusion of which the consumer gives to the trader does not oblige the consumer to maintain the offer, unless otherwise provided by ZP. ZP also applies to contracts for which the purpose or as an effect was avoiding the application of its provisions.

Application

Law on consumers protection provisions governing the protection of consumers in exercising their rights under the contract at a distance and contracts concluded away from business premises does not apply to contracts concluded using the machines for the sale of goods or services, or by using the business premises that are automated and contracts for the sale of food or beverages in temporary facilities. Also, the provisions of ZP governing the protection of consumers in exercising their rights under contracts concluded away from business premises does not apply to contracts concluded away from business premises, and which as the subject have: insurance; financial services whose price depends on changes in the financial market to which a trader can not influence and which occur in the period in which the consumer has the right to terminate the contract and consumer's credit contract. Besides the above mentioned provisions of ZP governing the protection of consumers in exercising their rights under the contract of sale of goods where the trader has an obligation of delivery of the goods and services applied to goods. It is logical that the provisions of ZP governing the protection of consumers in exercising their rights under the contract of sale of goods shall apply to contracts for the supply of goods which are subject to registration and are produced. ZP provisions regarding liability of defective products manufacturers shall not apply to liability for damages caused by nuclear accidents and liability for damage which is governed by ratified international treaties. ZP provisions governing the protection of consumers in exercising their rights under the contract of tourist travel and timeshare are also applied to the contract of residence of the student or student's residence in family abroad or in another appropriate placement and regular attendance at school or college for longer than three months, or with the consent of the parties in the short term, as well as for regular attendance at specific training.

Unfair business

In Part III ZP deals with issues of unfair business. To this end, ZP Article 19 stipulates the prohibition of unfair business practices. The trader bears the burden of

proving the correctness of the information concerning the product, which is given before, during and after the conclusion of the contract. Definition of unfair business ZP provides in Article 20 Stating that the business is unfair:

1) it is contrary to the requirements of professional diligence;

2) if substantially distorts or threatens to distort the economic behavior of matter in connection with the product of the average consumer to whom it relates or to which business is exposed to and the behavior of the average member of the group, where the business relates to the Group.

Trader significantly distort the economic behavior of consumers if their operations significantly reduce the ability of consumers to reasonably decide, due to which the consumer makes an economic decision that would not otherwise be brought. Economic decisions of consumer is about whether, how and under what conditions to buy a product, to pay the price in full or in part, whether to keep or return the product, or to exercise any other right in connection with a product that has under the contract, whether to do or abstain from doing any procedure. Business which threatens to significantly undermine the economic behavior defined group of consumers, who because of their mental or physical weakness, age or frivolity particularly susceptible to this type of business or that product, provided that the trader could reasonably be expected to anticipate, assess according to the average member of that group of consumers. These provisions do not apply to the cases of normal and allowable advertising that involves giving exaggerated statements or statements that should not be taken literally. Unfair especially is considered deceptive business, invasive operations, as well as breach of duty of notification in accordance with this Law. The unfair business includes any breach of duty of informing consumers of Article 16 of the ZP, and breach of duty of informing consumers of their rights under this law, in relation to:

1) distance contracts;

2) contracts for tourist travel and timeshare;

3) the marked price;

4) contracts concluded using electronic means.

The unfair business practices also include the breach of duty of informing consumers of their rights in relation to medical products for human use; financial services at a distance; collective investment in transferable securities; brokerage of insurance; life insurance and other types of direct insurance; sale of financial instruments; prospectus to be published in the event of a public offering of securities or their admission to trading, in accordance with the laws governing these areas.

The notion of deceptive business is defined by Art. 21. And under the misleading business, in terms of this Act, shall be deemed business of the seller which states that misleads consumers to make economic decisions that would not otherwise be made, in a manner that gives false information or otherwise causes or threatens to cause the average consumer to mislead terms:

1) the existence or nature of the product;

2) the basic features of the product related to the availability, benefits, risks, method of manufacture, use of accessories that accompany the product, assistance which can help consumers provides after sales and handling of their complaints, the

method and date of manufacture or provision of services, delivery, fitness for use, usage, quantity, specification, country of manufacture and country of origin mark, the expected results of the use or the results of the conducted tests or checks;

3) the obligations of the seller and the range of the obligation, the reasons for a particular market behavior and its nature, marking or addressing the person who directly or indirectly are supporting or recommending the trader or the product;

4) the price or the manner in which it is calculated, or the existence of certain benefits in terms of cost;

5) the need for servicing, parts, replacement or repair;

6) positions, properties or rights of the trader or his agent relating to their identity or property, qualifications and status, ownership and intellectual property rights they hold, prizes or awards that they have received;

7) consumer rights, including the right to replace items, or refund, or the risks to which it may be subject.

Deceptive business includes creating an overall impression that the average consumer is led to bring economic decision that would not otherwise be made regardless of the accuracy of the notice given to him.

Deceptive business exists if a trader, taking into account all the circumstances of the case, alleges or threatens to lead that the average consumer to make an economic decision that would not otherwise be made, in a manner that:

1) advertise a product, including comparative advertising, and by that makes it difficult to distinguish the product from other products, trademarks, product names, or other marks of a competitor;

2) violates the provisions of the code of conduct to which has approached.

Omissions that deceive consumers (Article 22)

Deceptive business by merchants passing to take certain action occurs when a trader, taking into account all the circumstances of the case, the spatial and temporal limitations of the used means of communication and additional measures undertaken for the purpose of informing consumers:

1) deny consumers important information which are necessary for the average consumer's a reasonable decision, which causes or threatens to cause the average consumer to make an economic decision that would not otherwise be made;

2) conceals relevant information or provides untimely or vague, unintelligible or ambiguous manner or when it fails to highlight the business purpose of its addressing to consumers which causes or threatens to cause the average consumer to make an economic decision that would not otherwise be brought.

Invitation to Bid and Notice of features and prices of products that a merchant must submit to customer, unless something else arises from the circumstances of the case, includes:

1) the basic characteristics of the product to the extent appropriate for the product and the means of communication;

2) the name and address of the seller and, if necessary, the name and address of the trader on whose behalf it operates;

3) the price of which includes taxes and other fees and additional costs, transportation costs, postage and delivery costs;

4) the rules of payment, delivery and fulfillment of contractual obligations and the manner in which will be handled the complaints of consumers if the rules differ from the requirements of professional diligence;

5) notification of the right to unilaterally terminate the contract.

Notwithstanding paragraph 2, item 3) of this Article, if the properties of the product price or additional costs can't be calculated in advance the trader shall provide the consumer information on which prices or additional surcharges are calculated.

Forms of business that are deemed fraudulent operations are defined in Article 23 According to it, the forms of the business regardless of the circumstances of each case are considered misleading market conduct are:

1) false assertion of dealer that it complies with certain codes of conduct;

2) unauthorized emphasizing quality mark, sign of trust or similar mark by the dealer;

3) false claim that the dealer has a certain code of conduct which is approved by a state authority or an organization;

4) false assertion of dealer that its market conduct or selling of products, endorse, support, or assisted by a certain state authority or an organization or even a true statement of the same content in the event that the trader do not comply with the conditions under which it has been given approval, support or assistance;

5) Call of the dealer to the consumer to submit an offer to purchase a product at a certain price, if the trader conceals the existence of reasonable grounds for believing he wouldn't be able to deliver the product or equipment, or hire another merchant to deliver the product at a specified price, in the amount and within the time that might be expected given the type of product, the volume of advertising and the offer price;

6) Call of the dealer to the consumer to make an offer to purchase a product at a certain price, if the trader in order to instigate the consumer to purchase of another product refuses to show the consumer the product to which the ad refers to, or refuses to accept the order and deliver the product within a reasonable time or shows damaged sample product to consumer to which the advertising relates to;

7) false assertion of the dealer that the product will be available in the short term or that it will be available in the short term, under certain conditions, in order to instigate that the consumer purchase decision must be taken without delay, and to deny him the opportunity or the time required for making reasonable decisions;

8) the failure of the trader to clearly inform the consumer, before accepting the offer, that after the sale of a particular product to provide support services in a language that is not in official use in the Republic of Serbia;

9) false assertion of the dealer or creating a false impression that a particular product on the market is in accordance with applicable regulations;

10) representing of the consumers rights that are guaranteed by law as a distinct advantage that the retailer offers the consumer;

11) use of editorial space in the media to advertise a product, it is the failure of the trader to the content of the ad sounds or images emphasize that this is a paid advertising, not content backed by the editorial staff; untrue statement of the trader on the nature and significance of the risk to the consumer which exposes him(her)self or his(her) family if they do not buy a specific product;

12) advertising by the merchants of the product that mimics the product of another dealer and that the consumer is deliberately misleading to conclusion that the products were produced by the same trader;

13) the creation, management and advertising from the merchant the system of products sales in which the consumer pays a fee to the possibility of generating income that does not depend on the successful sale of a particular product, but the participation of other consumers in this system sales;

14) false assertion of the dealer that it is going to cease operating or that it is to be moved to other premises;

15) claim that a particular merchant product increases the chance of winning in games of chance;

16) false claim that a particular merchant product cures a specific disease, dysfunction or malformations;

17) Providing false information on market conditions or the possibility of buying a particular product in the market in order to instigate the consumer to acquire the product under conditions which are less favorable than normal market conditions;

18) claim that announces a competition or promotion game, without handling the promised reward or adequate substitute for it after game or competition;

19) words describing the product for gratis, free, free of charge, or other words of similar meaning, if the consumer is obliged to bear any expense other than the unavoidable cost of answering the ad and acquisitions and deliveries of products;

20) putting the invoice or similar document which requires the payment of advertising material, which the consumer creates the false impression that he has already ordered the advertised product;

21) false claim or creation of the wrong impression that the trader is not acting as part of its business, profession or trade, or false representation of consumers (representing a customer);

22) creation of a wrong impression among consumers that after the sale of a particular product related services are available on the territory of another State other than the State in which the product is sold;

23) abuse of the term "guarantee" and expressions of similar meaning in concluding a contract of sale of goods and advertising regarding the sale of the goods, if the basis of the contract of sale of goods the consumer does not acquire more rights than they have under this law.

Law on consumers protection also defines invasive operations (Article 24). Invasive operations exist there if taking into account all the circumstances of the case, the trader by harassment, coercion, including physical coercion or undue influence, disrupts or threatens to disrupt freedom of choice or behavior of the average consumer with regard to a specific product and thereby causes or threatens to coerce consumer

to make economic decisions that would not otherwise be brought. Undue influence, in terms of this Act, is an abuse of a position of power in order to exert pressure on the consumer in a way which significantly limits the consumer's ability to reasonably decide, whether used or suggest the use of physical force. The criteria for determining the existence of intrusive operations are:

1) the time, place, nature and duration of intrusive operations;

2) the use of threatening or abusive language or behavior;

3) the fact that the dealer knowingly, with intent to influence the consumer's decision with regard to the product, use an accident which occurred on the consumer or the difficult circumstances in which the customer is located, and affecting his ability to reason;

4) severe or disproportionate non-contractual barriers that merchant puts before the customer who wants to exercise their contractual rights, including the right to terminate or cancel the contract or choose another product or another trader;

5) a threat of the dealer to the consumer that it will take a specific action that is not in accordance with law.

Law on consumers protection specifically prescribes the forms of business which by law are considered invasive operations. (Article 25) Forms of business that regardless of the circumstances of the individual case are considered as invasive operations are:

1) creation of the impression that the consumer can't leave the premises until they conclude the contract;

2) visit to the consumer, in his residential area, without its prior consent, except to enforce claims in the contract;

3) multi-addressing to the consumer, against his will by telephone, fax, electronic mail or other means of distance communication, other than to enforce claims in the contract;

4) a requirement that a consumer who intends to exercise its rights under the insurance policy has to provide documents that cannot be considered important in assessing the merits of his claim or persistent failure to respond to a customer's request to deter exercise of its contractual rights;

5) directly stimulating children through ads to buy or influence the parents or other adults for them to buy a product that is the subject of advertising;

6) request the consumer to pay back or keep product whose supply is not sought, except in cases of buying at a distance;

7) explicitly informing the consumer that the business or trader existence will be endangered if the consumer does not buy a specific product or service;

8) creation of a false impression that the consumer has won or that by taking certain actions is to win a prize or other benefit or benefit when there is no any or if the taking of any action in order to win prizes or benefits conditional on the consumer to pay a certain sum of money or incurred certain costs.

In order to get more detailed regulation of the comprehensiveness of the reach of ZP it prescribes special forms of protection of certain categories of persons, including the prescribed special protection of minors Article 26. According to the provisions

of this article it is prohibited sales, service and giving alcoholic beverages, including beer and tobacco products to persons less than 18 years of age. In case of doubt, that the consumer is a person under the age of 18 years, the retailer is under no obligation to sell or serve alcoholic beverages or tobacco products, until the consumer does not show the seller a valid ID card, passport or driver's license.

The Code of Conduct is defined in Article 27. Code of Conduct is an agreement or a decision of a trader or group of traders governing rules of market conduct of traders or groups of traders. Trader or group of traders who accessed a particular code of conduct are responsible for the control of compliance with the rules of the code of conduct by traders. The ministry responsible for consumer protection (hereinafter: the Ministry) shall encourage a trader or group of traders who access a particular code of conduct to control the appearance of unfair treatment of traders or groups of traders who have access to this code. The Ministry is obliged to encourage a trader or group of traders who access a particular code of conduct to inform consumers about the existence and content of the code.

Chapter IV implies regulation to protect consumers in exercising their rights under the contract at a distance and contracts concluded away from business premises. The first form of regulation is determined by: consumer information and right of withdrawal or unilateral termination, which prescribes the duty of notification (Article 28). According to it the dealer shall, prior to the conclusion of distance contracts and contracts concluded away from business premises, in addition to the data referred to in Article 16 of this Law, the consumer, in a clear and understandable manner, notify about:

1) Requirements for unilateral termination of the contract and the proceedings in which it may exercise that right;

2) the address where the trader operates if it doesn't operate at the address where his office is settled or residence and address of the seller on whose behalf it acts to which he can refer the complaint;

3) the existence of a code of conduct which obliges the trader and the way in which it can be accessed in the code;

4) the price of the use of means of distance communication if it is not accounted for by the basic rate;

5) the fact that they were entering into a contractual relationship with the merchant and enjoy protection under the law;

6) the fact that for distance contracts shall lose the right to unilaterally terminate contract, if with the express consent of the consumer, the retailer started offering the service before the expiration of the period in which it is allowed to unilaterally terminate the contract;

7) possibility of extra-judicial settlement of disputes.

The trader shall, before entering into contracts for the provision of financial services at a distance, the consumer, in a clear and understandable manner, notify about:

1) the basic features of financial services;

2) the total cost of financial services, including taxes, fees, charges and fees, or the manner of calculating the cost if the total cost of financial services is not to be disclosed;

3) special risks relating to a financial instrument;
4) The notice of period for which data are valid;
5) the method of payment.

If the trader and the consumer enter into a contract at a distance or contracts concluded away from business premises, the described data becomes an integral part.

Protecting the rights and interests of the users of payment services and electronic money holders

This protection is treated in Article 6 NZPU, and if the payment service provider or electronic money issuer does not comply with the provisions of this Act, other regulations or general terms and conditions governing payment services and electronic money, good business practices relating to the services or contractual obligations of payment services, and contracts relating to electronic money – users of payment services and electronic money holder shall have the right to protect their rights and interests.

On the process of achieving protection of the rights and interests of users of payment services and electronic money holders, are applied provisions of the law governing the protection of users of financial services relating to the exercise of protection of rights and interests of users of financial services.

The provisions of the law governing consumer protection are applied on unfair contract terms and unfair business practices in the provision of payment services and issuing electronic money, as well as the procedure for their prohibition.

If the provision of payment services or issuing electronic money associated with the loan or overdraft account by the payment service provider or electronic money issuer that is not a bank can be in accordance with the provisions of this law to provide payment services - the consumer, the loan agreement and an agreement on overdraft accounts, as well as other rights and obligations of payment service providers and the users in connection with a loan or overdraft accounts and Consumer Protection of the loan or overdraft, the provisions of the law governing the protection of users of financial services.

The protection of the credit card holder who is a consumer, in addition to the provisions of the law governing the rights and obligations of payment service users, are applied provisions of the law governing the protection of users of financial services relating to the rights and obligations of the Bank as issuer of credit cards, contract the issuance and use of credit cards and consumer protection credit card.

Exclusion from the established requirements for the provision of payment services

With this problem deals Article 9 of NZPU. Payment services providers may provide payment services to their clients under conditions favorable for the user of the conditions imposed by the provisions of this Act.

If the payment service user is not a consumer, contract of payment services cannot exclude or limit the application of the provisions of Section II of this part NZPU, except the provisions of Art. 14 and 15, Article 16. 3 and 4, and Article 32 In cases when the payment service user is not a consumer, contract of payment services may exclude or limit the application of the provisions of Art. 37, 38, 51, 53, 54, 58, 60 and 63 NZPU.

Article 10 defines who can provide these services in the Republic of Serbia, so they can:

1) bank;

2) electronic money institutions;

3) payment institutions;

4) The National Bank of Serbia;

5) The Treasury or other public authorities in the Republic of Serbia, in accordance with its responsibilities established by law;

6) a public postal operator based in the Republic of Serbia, established in accordance with the law governing postal services (hereinafter referred to as the public postal operator).

No one other than this way defined payment service providers may not provide payment services in the Republic of Serbia.

When the National Bank of Serbia, Treasury or other public authorities in the Republic of Serbia provide payment services within the jurisdiction established by law, they do not apply the provisions of this law governing the rights and obligations of providers and users of payment services, the contract for payment services, execution of payment transaction and execution of rights and interests of the payment service user, unless it is determined by a special regulation or contract these services.

However, NZPU prescribes the payment services provided by the public postal operator, and by Article 11 the Public Postal Operator may in its own name and for its own account provide all payment services, or some of them. In addition to this certain payment services, public postal operator may provide the following services:

1) the payment of cash to consumers at the expense of accounts maintained with a bank;

2) the receipt and payment of checks current account customers.

Public postal operator mentioned payment services can be provided and the name and on behalf of the banks, and can also provide mediation services between banks and payment service user in connection with payment services, in accordance with the regulations governing banks.

Public postal operator shall, not later than one month before the start or termination of services, the National Bank of Serbia notice of intent beginning or termination of the services. This notice contains information about each service that the public postal operator intends to commence or cease to provide, as well as the planned date of commencement or termination of the services.

NZPU in article 15 also defines the types of contracts on payment services. In this sense, the contract on payment services is concluded as a framework contract for payment services (hereinafter the Framework Agreement) or a contract for a one-time

payment transaction. Framework Agreement governs the future execution of individual payment transactions. If the payment service user opens a payment account with the payment service providers, framework agreement regulates the conditions for opening, maintaining and closing the account. Agreement on a one-time payment transaction shall be governed by the execution of a certain payment transactions not covered by the framework agreement.

Defining described NZPU first regulated by the Framework Agreement, prescribing the form and content of the Framework Agreement (Article 16). The Framework Agreement contains the following mandatory elements or information:

1) information about the provider and the payment service user:

(1) the business name (title) and headquarters of payment service providers, as well as the business name and address, or the address of an agent or branch in the Republic of Serbia, through which provides payment services, and any other address where the payment service user can contact the provider of payment services, including e-mail address

(2) The name and address of the seat body responsible for oversight of the provider of payment services, its agent or branch, in connection with the provision of payment services in the Republic of Serbia,

(3) information on the register of payment institutions or registry of electronic money institutions, or of other appropriate public register of issued licenses to payment service providers and the registration number or the appropriate identification label providers of payment services in the registry,

(4) the name and domicile or residence of the payment service user - the consumer or the business name and registered office of the payment service user - the entrepreneur or legal entity;

2) The conditions for the use of payment services:

(1) the nature and description of the main characteristics of the payment service to be provided,

(2) a unique identification code or other information that the user of payment services shall state for the proper execution of the payment order,

(3) the form and manner of issuing and revoking approval for the execution of payment transactions in accordance with Art. 33, 37 and 38 of NZPU,

(4) the time when it is considered that the payment service provider received payment order pursuant to Article 35 NZPU, as well as any time for acceptance of payment orders in a given business day, after which the orders received are considered received the next business day in accordance with paragraph 4 this article

(5) The deadline for the execution of payment transactions,

(6) An indication of the spending limit in the use of the payment instrument in accordance with Article 49 NZPU if the limit agreed upon;

3) information and details on fees, interest rates and the rate of exchange:

(1) the type and amount of compensation that the provider of payment services charges the payment service user, and if they charge collectively - and the type and amount of each fee that makes the aggregate compensation

(2) if the service provider of payment services applicable interest rate and/or rate of exchange - the interest rate and the rate of exchange, or if it is used a reference interest rate and/or reference rate - the relevant date and index or other basis for determining reference interest rate and exchange rate, and the method of calculating the actual interest

(3) an indication for changes in interest rates or the rate of exchange, which are based on modifications to a reference interest rate or reference rate applicable immediately and without prior notification to payment service users about these changes in accordance with Article 19 NZPU, in which case the payment service provider shall inform the payment service user as defined in this section – if this option is agreed;

4) information on the method and means of communication between users and providers of payment services, including:

(1) the means of communication for the exchange of information and notifications in accordance with the law, including the technical requirements related to equipment users of payment services,

(2) the manner and frequency of the provision of information to the payment service provided or made available in accordance with NZPU,

(3) the language in which it would be concluded a framework agreement on which to communicate during the contractual relationship, if the user of payment services requires the conclusion of a framework agreement and the performance of the communication in a language other than Serbian,

(4) the right of the payment service user to have, during the contractual relationship, at his request, served copies of the framework agreement and the information in this article, on paper or on another durable medium;

5) information on protective and other measures related to the execution of payment transactions, including:

(1) the measures that the payment service user shall undertake to protect the payment instrument and the manner of notification of payment service providers of the loss, theft or misuse of a payment instrument in accordance with Article 47 of NZPU,

(2) the conditions under which the payment service provider has the right to block the use of the payment instrument in accordance with Article 49 of NZPU, if it is established by a framework contract,

(3) the payer's liability for unauthorized payment transactions, including the amount of the loss covered by the payer, in accordance with Article 51of NZPU,

(4) the manner and timeframe in which the payment service provider shall inform the payment service provider of non-approved, non-executed or incorrectly executed payment transaction or to require the proper execution of payment transactions, in accordance with Article 61 of NZPU,

(5) The responsibility of payment service providers for unapproved, non-executed and incorrectly executed payment transactions in accordance with Art. 50 to 59 and Article 62 NZPU,

(6) the conditions for the return of the amount approved and properly executed payment transaction to the payer, in accordance with Article 63 NZPU;

6) conditions for amendment and termination of the framework contract, as follows:

(1) an indication that the payment service user accepts the amendments to the framework contract and without giving explicit consent, and notification of the right of the user in that case, terminate this contract, in accordance with Article 18 of NZPU - if this option is agreed,

(2) The duration of the framework agreement,

(3) requirements for unilateral termination of the framework contract or invalidity of the provisions of this contract, in accordance with Art. 18, 20 and 21 of NZPU;

7) information on the protection of payment service users, including:

(1) the contractual provisions that determine which regulations apply to the framework agreement and/or jurisdiction of the court,

(2) the right to protest and complaint to the payment service user and the possibility of extra-judicial settlement of disputes in connection with the provision of payment services, in accordance with the law governing the protection of users of financial services.

If the subject of the framework contract is issuance and use of credit cards, this contract, in addition to the elements specified in paragraph 1 of this Article shall contain the mandatory elements of the agreement on the issuance and use of credit cards determined by the law governing the protection of users of financial services.

The framework contract shall be concluded in writing. Payment service provider shall provide that the payment service user receives at least one copy of the framework contract. Payment service user has the right to, during of the contractual relationship, at his request, be provided with copies of the framework agreement and information referred to in Article 17, paragraph 1 of NZPU provided in the pre-contractual stage, on paper or on another durable medium.

Termination and Nullity of a framework agreement

Termination or invalidity of a framework contract that requires users of payment services is governed by Article 20 of NZPU. Payment service user has the right at any time to terminate the framework agreement without notice, unless the framework agreement provides for the notice period, which may not be longer than one month. Payment service user has the right to terminate the framework agreement in other cases stipulated by the law governing obligations or other law. If the payment service user terminates the framework contract, he (she or it) shall pay a fee for the payment services provided up to the date of such termination, and if such a fee was paid in advance, the payment service provider is obliged to give back the payment service user the proportionate part of the consideration paid. The provider of payment services may not charge to the payment service user for the termination of the framework contract. Payment service user may require that the provisions of a framework agreement that are inconsistent with the information provided in the pre-contractual phase, in accordance with Article 17, paragraph 1 of NZPU, and the provisions relating to information

under Article 16 NZPU that were not previously submitted to the payment services – be determined as void.

If it was so specified in the framework contract, the payment service provider has the right to terminate the framework contract concluded for an indefinite period of time, with a notice period of not less than two months. Payment service provider may terminate the framework agreement and in other cases stipulated by the law governing obligations or other law. Payment service provider shall deliver the notice of termination of the framework contract to deliver payment services in writing. If the payment service provider terminates the framework contract, the obligation of the payment service user to pay a fee is pursuant to the provisions of Article 20 para. 3 and 4 of NZPU.

Payers' payment service provider shall, prior to the execution of an individual payment transaction initiated by the payer on the basis of a framework agreement, submit to the payer, at his request, accurate information about the deadline for the execution of the payment transaction and the fees that will be charged for it, and if the provider of payment services aggregate charges and fees – and the type and amount of each fee that makes the collective benefit.

Payers' provider of payment services that, based on the framework agreement, is executing a single payment transaction shall, immediately after the debt of payer's payment invoice or after receipt of the payment order if the payer does not use the payment account, submit to the payer the following information:

1) the reference mark or other information that enable identification of individual payment transactions of the payer and information relating to the recipient's payment;

2) the amount of the payment transaction in the currency in which the payer's payment account is debited or in the currency of the payee stated in the payment order;

3) the amount of any fees that are charged to the payer for the execution of individual payment transactions, and if the provider of payment services collectively charges these fees - the type and amount of each fee that makes the collective benefit;

4) the amount of interest payable by the payer, if the interest is paid;

5) if a currency exchange is done – rate of exchange that is in the execution of payment transactions using payer's provider of payment services, as well as the amount of the payment transaction after that currency exchange;

6) the date of debt closing of payments account, which is the date of receipt of the payment order.

Payers' payment service provider shall provide to the payer information described on paper or on another durable medium.

Framework contract may stipulate that the payment service provider of the payer provides information periodically, at least once a month, in the agreed manner which allows the payer to preserve this information and reproduce it in an unaltered form. Payment service provider shall submit monthly to a payer - the consumer upon request, without charge, the requested information on individual payment transactions executed in paper.

Access to data in electronic commerce (Article 30)

The trader is obliged to provide to the relevant authorities and consumers easy, always available and immediate access to the following data:

1) The name, address and e-mail of the seller;

2) the name or a title of the public register in which the trader is registered and the number of the entry, and the other data on the basis of which identification can be performed of that dealer in the registry;

3) the supervisory authority if it is to perform activities of merchants required the approval of the competent authority;

4) the name and address of the chambers or associations which the trader has joined, professional titles and a state in which it acquired title, the professional rules which oblige the trader and the way in which it can be accessed by those rules, if for a trader occupation or activity it is necessary to meet specific requirements or achieve membership in a particular chamber or association;

5) the amount and manner of payment of value added tax.

Law on consumers protection also prescribes the duty of notification of the exercise of the right to unilaterally terminate the contract in Article 31. The seller is obliged to deliver to the consumer a form of unilateral termination of the contract at a distance and contracts concluded away from business premises, and a notice of:

1) The name, address and e-mail the of the seller to the consumer where he (or she) submits the form to the unilateral termination of the contract;

2) the consumer's right to unilaterally terminate the contract in the form of a unilateral termination of the agreement on a durable medium of records (continuous medium):

(1) for contracts concluded away from business premises, within 14 days from the date the consumer signs the order form;

(2) in the case of contract at the distance, within 14 days from the date when the goods reached the possession of the consumer or a third party designated by the consumer, and that is not transporter;

(3) for contracts at the distance relating to the provision of services within 14 days from the date of conclusion of the contract unless the consumer has expressly agreed to provide services start before that deadline;

(4) in the case of contracts at the distance which is subject to the provision of financial services, within 14 days of the conclusion of the contract or the date of informing consumers about the content of the contract if the notice is received after the conclusion of the contract;

(5) in the case of contract at the distance which has the subject of life insurance within 14 days of the conclusion of the contract or the date of informing consumers about the content of the contract if the notice is received after the conclusion of the contract;

3) The method and time for return of the goods delivered and the return on money in the sales contract;

4) for e-commerce, the consumer can fill out and submit the form for termination of contract in electronic form on the website of the merchant, and that he would dealer emailed immediately confirm the receipt of the completed form for breach of contract;

5) the possibility of using the form of unilateral termination of the contract;

6) the fact that the return of goods by consumers within the time due which it can be considered as unilaterally termination of the contract.

More detailed contents of the form for unilateral termination of the agreement at a distance and contracts concluded away from business premises would be provided by the minister responsible for consumer protection (hereinafter: the Minister).

Law on consumers protection provides for the formal requirements for the conclusion of contracts away from business premises (Article 32). If a trader and a consumer have concluded contract away from business premises, information about the data under Article 28 and 31 of ZP must be legibly written on the order form, in an easy and understandable way. The contract shall be deemed concluded when the consumer signs the order form. The contract concluded away from business premises shall be deemed concluded when the consumer signs the order form; In case the order form is not in writing, when a consumer receives a printed copy of the completed purchase order; or, if the consumer has agreed to, when the consumer receives a copy of the purchase order to the permanent record carrier. Order form must contain a form of unilateral termination of the contract.

Law on consumers protection also provides for the formal requirements for the conclusion of contracts at the distance (Article 33). For distance contracts the trader shall provide the consumer or make available the notice of the particulars referred to in Article 28 and 31, prior to the conclusion of the contract in a clear and understandable manner, corresponding to the means of distance communication.

If the seller calls consumers by phone in order to conclude a distance contract, the trader shall, immediately after the start of the talk, present to the consumer his identity and that the call was made for commercial purposes. The trader shall in the case of the contract by means of communication that by its properties limits the ability of the trader to inform consumers of the mentioned data, deliver to consumer notice of the basic characteristics of the goods and the selling price. In this case, the seller is obliged to inform the consumer in writing of the information not later than the delivery of goods or commencement of the services unless that information was given to the consumer in writing prior to the conclusion of distance contracts. Notwithstanding the foregoing, the trader can inform consumers about data records on a durable medium (continuous medium) only if the customer consents on it. In the case of the previous it is established the right of consumers to unilaterally terminate the contract and also was stipulated termination deadline (Article 35 of ZP). The consumer may, within 14 days of the conclusion of distance contracts or contract concluded away from business premises, terminate the contract without giving any reason to. Through unilateral termination of the contract the consumer shall be relieved of all contractual obligations, except for direct costs of return of goods to retailer. Statement on the unilateral termination of the agreement at a distance or contract concluded away from business premises shall be deemed timely if sent to the seller in the said period or if the consumer

returned the seller the goods he (or she) had received under the contract within. Statement on the unilateral termination of the contract has legal effect from the date when it was sent to the merchant. In contracts concluded away from business premises, the period is counted from the moment when the consumer signs the order form, and in the event that the order form is not in writing – from the moment the consumer receives a copy of the completed purchase order in writing and a copy of the completed purchase order to permanently record carrier (continuous medium) if the customer agrees with that and it ends with the expiry of the last hour of the last day of the period. In the contract of sale of goods at a distance, the deadline is counted from the moment the goods are gotten into the possession of the consumer or a third party designated by the consumer and that is not the carrier and ends with the expiry of the last hour of the last day of the period. In contract to provide services at a distance term is counted from the moment of signing the contract and ends on the expiry of the last hour of the last day of the period contracted. When it comes to contracts for the provision of financial services at a distance, the period is calculated from the time of conclusion of the contract, i.e. from the moment of informing consumers about the content of the contract if notification received after the contract is concluded and ends with the expiry of the last hour of the last day of the period. Exceptionally in life insurance contracts at a distance, the consumer has the right to terminate the contract without giving reasons within 30 days. If the seller fails to inform consumers in advance about the existence of the right to unilaterally terminate the contract deadline for the termination of the contract begins to run from the moment the consumer receives notification of the right to unilaterally terminate the contract in writing or on a durable medium of records (continuous media) if a consumer agrees with. In this case, the consumer may terminate the contract at any time, including the time prior to the receipt of a late notice of the existence of the right of withdrawal or termination. The exercise of this right (to the unilateral termination of the contract) is stipulated in Article 36 of ZP. If the customer decides to terminate (cancel) the distance contract or contracts concluded away from business premises, he (or she) shall send a statement of unilateral termination of the contract to the seller in writing or on a durable medium of records (continuous medium). Consumer can make a statement on the unilateral termination of the contract in independently formulated form or to submit a statement for the seller in the form of Article 31 of ZP. Returns of goods to the seller specified in Article 35, paragraph 1 of ZP is considered timely declaration of termination. In e-commerce merchant is obliged to provide to the consumer, except for termination of the contract in the manner prescribed in paragraph 1 of this Article, a way to terminate the contract by filling out and submitting the form referred to in Article 31 ZP on the website of the dealer – in electronic form. In this case, the seller is obligated to the consumer shall send a confirmation of receipt of the statement of termination.

Legal consequences of the unilateral termination of the contract are prescribed in Article 37. The unilateral termination of the contract at a distance or contract concluded away from business premises cease the obligations of parties arising from conclusion of distance contracts, or contracts which are concluded away from business premises. The trader is obliged to immediately return to the consumer the amount the consumer paid under the contract, but not later than 30 days from the date of receipt of

the declaration of the unilateral termination of the contract. In the sales contract, which is concluded away from business premises, or at a distance, the seller is obliged to repay the customer the funds paid under the contract when it receives or takes over the goods which is based on contracts delivered to the consumer, or when it receives proof that the consumer goods are sent the seller, regardless of these actions is the consumer first taken. If before the expiration of the unilateral termination of the sales contract, which is concluded away from business premises, or at a distance, took possession of the goods the consumer or a third party designated by the consumer, the consumer shall, within 14 days from the day when he (or she) sent a statement the unilateral termination of the contract, the goods send or deliver to the seller or to a third party that is authorized dealer to receive the goods, unless the trader has offered that to take the goods from the consumer. In this case, the consumer bears only the direct costs of returning the goods to the merchant.

In contracts for the provision of financial services at a distance, the seller is obliged to immediately return to the consumer the amount paid under the contract, but not later than 30 days from the date of receipt of the declaration of the unilateral termination of the contract, unless the financial services were provided with the express consent consumer.

In the case of unilateral termination of the contract of insurance consumers cannot demand payment for services rendered.

Restriction of use of certain means of distance communication

Direct advertising is defined in Article 41. It is prohibited advertising directly by phone, fax or e-mail without prior consent of the consumer. It is forbidden to directly advertise other means of communication at a distance, without the prior consent of the consumer. If the consumer expressly consented to advertising by phone, fax or email, the trader is obliged to do so before the advertising of certain goods or services in a clear and unambiguous manner, inform the consumer about the commercial purpose of the activity.

Sending of the shipments that are not ordered (unwanted) is stipulated by Article 42 of ZP. Also, it is forbidden to send the goods or offer the provision of services to consumers with a request for payment for goods or services that the consumer has not ordered. If in this case, the consumer does not opt for goods that are delivered or the service that is provided, it is deemed that the offer has not been accepted. Sending goods or providing services that the consumer did not order can't be a source of liability (or obligation) for the consumer and is considered unconditional gift to the consumer has been made for the purpose of advertising. It will not be considered as a trader previously described in the case:

1) instead of the consumer goods and services, which was ordered to submit other goods or provides other services to the same price and quality;

2) inform the consumer that is not bound to accept the goods or services did not request, nor to bear the cost of returning the goods to the merchant.

Law on consumers protection regulates advertising through means of distance communication Article 43. A trader shall, during the advertisement by means of remote communication, notice about the nature of the message and the identity of the legal or natural person in whose name it is done advertising and to display it in a clear and understandable way. The trader is obliged that promotional games, competitions and special offers, to highlight in a clear and understandable manner and conditions of participation in the promotional game or competition or the conditions under which it applies specials to publish in a manner that allows it to be easily accessible, clear and understandable to the consumer. ZP prescribes also Consumer Protection in enforcing contracts containing unfair contractual terms in Chapter V. The first requirement is prescribed by Article 44 of the Public Contracting provision obliges the consumer if it is expressed in simple, clear and understandable language, and if it would be understood by a reasonable person of consumers knowledge and experience. The trader is bound to make familiar the consumer with the content of the contractual arrangements before the conclusion of the contract in a manner with respect to the applied method of communication provides to the consumer a real opportunity to become familiar with the content provision. Contractual provision obliges the consumer if the consumer has agreed to it. Contractual provision whose content is determined by a trader in a manner which states that the consumer has agreed to it unless he (or she) explicitly pointed out that does not accept provision, does not bind the consumer. The interpretation of contractual provisions is foreseen in Article 45 of ZP. Contentious provisions in consumer contracts must be interpreted in favor of the consumer. ZP in Article 46 provides for unfair contract term. Unfair contract terms are null and void. As unfair Contract Terms shall be deemed a contractual provision that:

1) results in a significant imbalance in the obligations of the contracting parties to the detriment of consumers;

2) The consequence is the fact that the execution of contractual obligations makes it fawl to the consumer without a valid reason;

3) The consequence is the fact that the doing the contractual obligation is significantly different from what the consumer is legitimately expected;

4) is contrary to the request of the public in the conduct of dealer;

5) is contrary to the principle of good faith.

Criteria to consider when determining whether a particular provision of the contract is unfair:

1) the nature of the goods or services to which the contract relates;

2) The circumstances under which the contract is concluded;

3) The other provisions of the same consumer contract or other agreement with which the consumer contract is linked;

4) The manner in which was reached consensus on the content of the agreement and the way it was, with regard to the application of the public, consumer informed about the content of the contract.

Contractual provisions that are considered Unfair Contract Terms are defined in Article 47. According to the same contractual arrangements regardless of the circumstances of the individual case are considered as Unfair Contract Terms provisions are whose object or effect is to:

1) the exclusion or limitation of liability of the seller for death or personal injury to consumers due to an act or omission of the Merchant;

2) limiting the trader to execute and take on the obligations that on his behalf or for his account has taken counsel or the agent or dealer or connection of the obligation to make or take obligations on his behalf or for his account, that counsel took or the agent with the condition whose fulfilment depends exclusively on the trader;

3) excluding or limiting the rights of consumers to initiate a specific procedure or to use a specific remedy for the protection of their rights, in particular the imposition of obligations to consumers that resolves disputes by arbitration in a manner that is inconsistent with the provisions of this Act;

4) prevent or limit the possibility for consumer to make familiar with the evidence or the transfer of the burden of proof on the consumer in cases where the burden of proof, in accordance with the law, is on the merchant.

Unfair Contract Terms shall be deemed a contractual provision under which the merchant has:

1) the right to determine whether the goods were delivered or services were rendered in accordance with the contract;

2) The exclusive right of interpretation of contractual provisions.

Contract terms which are presumed to be unfair contractual terms unless it is proved otherwise are prescribed by Article 48 of ZP. Contract terms which are presumed to be unfair contractual terms unless it is proved otherwise are provisions whose object or effect is to:

1) the rights of the consumer to the retailer or a third party in the event of a total or partial failure to fulfil any contractual obligations dealer, including the rights of the consumer to a claim that has leveraged the claim with the trader a claim that a trader has towards the consumer;

2) enabling the trader to keep everything he received from the consumer in the event that the consumer is in the violation of a contractual obligation, or refuse to conclude the contract, if the same right is not granted to the consumer;

3) obliging the consumer who has violated a contractual obligation to pay the seller a fee in an amount that significantly exceed the harm suffered;

4) allowing the trader to terminate the contract at any time if the same right is not granted to the consumer;

5) allowing the trader to terminate the contract concluded for an indefinite period without reasonable notice, unless the consumer fails to perform its contractual obligations;

6) tacit renewal of a contract concluded for a fixed period, if necessary, to the consumer that he (or she) does not agree to a contract extension which is inappropriately long compared to the time for which the contract is concluded;

7) the trader to in any way increases the agreed price, unless the consumer agreed that in this case, terminate the contract;

8) obliging the consumer to fulfil all his obligations in the event that the trader does not fulfil its contractual obligations in full;

9) enabling the trader to transfer their contractual obligations to a third party without the consent of the consumer;

10) restrict the right of consumers to resell the goods by limiting the transferability guarantees given by the trader;

11) enabling the trader to unilaterally alter the terms of the contract, including the characteristics of the goods or services;

1) unilateral modification of terms that are communicated to the consumer in a durable record carrier (continuous medium), communication of the new provisions with which the consumer is not agreed by means of distance communication.

Article 54 of ZP provides for the legal consequences in case of lack of conformity. If the delivered goods is not in conformity with the contract, the consumer has the right to require the seller to remedy the lack of conformity, without charge, trough repair or replacement, or to request an appropriate reduction in price or to cancel the contract in respect of these goods. The consumer, in the first place, can choose between the demands that the lack of conformity is removed by a repair or replacement. If removal of the lack of conformity is not possible or it constitutes a disproportionate burden on the dealer, the consumer may require reduction in price or terminate (withdraw from) the contract. Disproportionate burden on the dealer occurs when compared with reductions of rescission and creates excessive costs, taking into account:

1) The value of goods that would have the conformity with the contract;

2) the importance of conformity in the case;

3) whether the conformity can be eliminated without significant inconvenience to the consumer.

Any repair or replacement must be made at reasonable time and without significant inconvenience to the consumer, taking into account the nature of the goods and the purpose for which it was acquired by the consumer. All costs that are necessary to make the goods as prescribed by the contract, especially labor costs, materials, and delivery shall be borne by the trader. The consumer has the right to terminate the contract, if it cannot qualify for repair or replacement, or if the dealer did not perform repair or replacement at reasonable timeframe or if the dealer did not perform repair or replacement without significant inconvenience to the consumer. For dealer obligations arising due to lack of conformity of the goods, the manufacturer to the consumer is in a position guarantor. ZP provides that a consumer can't terminate the contract if the lack of conformity of the goods is small. This law does not affect the consumer's right to require from the dealer damages derived from the lack of conformity in accordance with the general rules on liability for damages.

Time limits and burden of proof are laid down in Article 55 of ZP. So the merchant is responsible for the lack of conformity of goods in contract that appears within two years from the date of passing of risk to the consumer. If the lack of conformity occurs within six months from the date of passing of risk to the consumer, it is assumed that the lack of conformity existed at the time of transfer of risk, unless this is incompatible with the nature of the goods and the nature of a certain lack of conformity. When selling second-hand goods it can be arranged a shorter period in which the retailer would be responsible for the lack of conformity this, however, may not be less than one year.

Law on consumers protection prescribes the procedure for the guarantee. The provider of the guarantee and warranty card are defined in Article 56. By it a guarantee is: any statement with which the provider gives promise relating to the goods, and is legally binding under conditions specified in the declaration, as well as advertising in connection with such goods. Warranty card is a document in written or electronic form, or on another durable medium, which contains all the data from the warranty, stated in a clear and legible manner, easily understandable language, and in particular consist of the following information:

1) consumer rights under Art. 54 of this Law, with notification that the contracting guarantee does not affect those rights;

2) the name and address of a guarantor, content of contractual guarantees and conditions for exercising the right of contractual guarantees, and in particular its duration and spatial validity;

3) non-transferrable in the event that the rights of warranty which is non-transferable, and which does not affect the presumption under Article 48, item 10) of ZP.

The provider of guarantees shall, at the request of consumers to issue the guarantee card. On the validity of the guarantee does not affect any of the previously described violations of the obligations of a guarantor, and the consumer may request that the guarantee might be fulfilled in accordance with the given statement. The warranty does not exclude or affect the rights of consumers in relation to goods conformity according to the contract.

There are also provided by the ZP rules of abusement of expression guarantees (Article 57). At the conclusion of the sales contract and advertising on the occasion of sale, the dealer is obligated to refrain from the use of the term "guarantee" and the term with this meaning, if on the basis of the contract of sale the consumer does not acquire more rights than they have under this law.

The complaint is also treated by ZP in Article 58. Consumer may file Complaint to the seller, to exercise their rights under Article 54 or Article 56 of the ZP. The trader shall, without delay, and no later than 15 days from receipt of the complaint, to answer to the consumer, with Observations on the proposal and submit the proposal to its solution.

Liability for lack of Product ZP governs in the Title VII. Lack is defined in art. 59 and it exists if the product does not provide the safety that is rightly expected considering all the circumstances, including advertising, use of the product that was reasonably expected, and the time when the product was put into circulation. It is not considered that the product has the disadvantage just because it was later placed on the market a higher quality product.

The right to compensation (Article 60) is defined in the case if it could be proven that the damage was inflicted, that the product had a defect and there is the causal relationship between that failure and the damage suffered. The injured party is entitled to compensation for non-pecuniary damages under the general rules on liability. Producer responsibility is defined by Article 61. Manufacturers are responsible for damages caused by defective products regardless of whether they knew about the flaw. The manufacturer shall not be liable for damage caused by defective products if it proves that:

1) did not trafficked the product;

2) the lack existed at the time when the product was trafficked or that appeared later;

3) did not produce a product intended for sale or any other kind of marketing & product that is not produced within the framework of its regular activities;

4) the defect is due to compliance of the product with the properties of binding regulations issued by the competent authority.

Manufacturer of the integral part of the product will not be responsible for damage caused by defective products if it proves that the disadvantage can be attributed to the product design or the consequence of instructions given by the manufacturer of the whole product. Also, the manufacturer may be partially or fully exempted from liability for damage caused by defective products if it is the damaged or a person for whom he (or she) is responsible through his own fault contributed to the damage. If to the damage of the product partially has contributed a third party, the sole responsibility is on the manufacturer.

The responsibility of more than one person for the same damage is defined by Article 63. If more than one person is liable for damage caused by defective products, their liability is joint and several. Obsolescence of the claims is prescribed by Article 64 and there is the obsolesce in subjective and objective sense. Claim for damages from defective products become obsolete within three years from the date when the injured party learned of the damage, and the lack of purchased goods and the identity of the manufacturer. In any case, the claim becomes obsolete in ten years from the date when the producer has put in market the product with the defect.

Liability for damage caused by defective products cannot be limited by contract or waived (Article 65 of ZP). Consumer protection in the exercise of rights under the contract for providing services is prescribed in the chapter VIII of ZP. First that is elaborated is the quality of the materials provided (Article 66). If it is agreed that a trader is making a thing of their own material whose quality is not agreed upon, it shall be required to use the material for the production of medium quality. On the responsibility of the merchant to the quality of the material used must be in accordance with the applicable provisions of Art 49-58 of ZP. Also are defined things in relation to material that gave the consumer (Article 67). The dealer is responsible for damage caused by defects of material that has noticed or should have to notice if they fail to warn consumers to defects in materials obtained from it. If the consumer requires making things of a material of whose defects he was warned by trader, the trader is obliged to comply with the request of the consumer, unless it is obvious that the material is not suitable for commissioned work or making things of such materials may harm the reputation of the dealer, in which case the retailer may terminate the contract. The trader is obliged to inform the consumer of the deficiencies in his order, and in other circumstances which he knew or should have known that may be of importance for commissioned work or to carry it out on time, otherwise they will be liable for damages.

Performed services (Article 68). The service should be deemed as completed when the contracted work was completed. If the thing that is subject to a contractual obligation is at possession of the merchants, service is deemed completed when the

contracted work was completed and the matter returned to the consumer. If the period of service is not agreed, the dealer is required to perform the service at reasonable time required for execution of similar services. The dealer is not responsible for late payment arising from consumer's fault. Provision of services (Article 69) is also defined by ZP. The trader is obliged to obtain supplies and spare parts that are needed to deliver the service, unless otherwise agreed. The dealer is required to perform the service in the agreed manner, according to the rules of the profession and the professional care.

Chapter XII has provided the amicable settlement of consumer disputes. Consumer dispute is defined in Article 132 of ZP. According to it, a consumer dispute is any dispute arising from the contractual relationship, between the consumer and the merchant. Consumer disputes, in terms of the ZP, is not considered litigation arising due to:

1) death, bodily injury or impaired health;

2) providing medical or legal services;

3) transfer of immovable property.

For Consumer disputes, in terms of ZP, it is not considered a dispute worth over one million dinars. Consumer dispute can be resolved by extrajudicial resolution of consumer disputes through amicable settlement. Extra judicial settlement of consumer disputes is confidential and urgent. The party of non-judicial settlement of consumer disputes that violate previously described obligation, has the liability for damages that may be incurred as a result of such a procedure for the other party. The parties of extra-court amicable settlement of consumer disputes are equal. ZP prescribes the method of initiating procedures of extra judicial settlement of consumer disputes (Article 133). Extra judicial settlement of consumer disputes starts by accepting proposals for an amicable settlement of consumer disputes the other party, depending on the type of extra-judicial proceedings in which solves a consumer dispute, on a proposal from the consumer, or the association or federation, or the merchants. Mediators and arbitrators of consumer dispute are defined in art.134. According to it, parties in the consumer dispute may agree to entrust resolving consumer disputes to one or more of a mediators in resolving disputes (mediators), chosen from a list of mediators, in accordance with the law governing mediation. Parties to a consumer dispute may agree to entrust solving consumer disputes to an arbitrator, chosen in accordance with the law governing the arbitration. Admissible non judicial settlement of consumer disputes does not preclude or affect the exercise of the right to judicial protection, in accordance with the law. In the process of keeping and completion of non-judicial settlement of consumer disputes, in accordance with the applicable provisions of the law governing the arbitration, or mediation, as well as other regulations governing the resolution of consumer disputes.

Chapter XIII of ZP has prescribed procedure of prohibiting unfair contract terms and unfair business practices. A consumer whose rights or interests were injured can file a request to institute proceedings (article 137):

1) The prohibition of unfair contract terms in consumer contracts;

2) prohibiting unfair business practices;

3) the unlawful confiscation of proceeds.

This request may be filed by the Association and Association of Article 129 of the ZP, due to the violation of the collective interests of consumers. Pending a decision on the request referred to in Article 137 it may not be filled the identical request to run another procedure.

The process on the request referred to in Article 137 of this Law shall be initiated and conducted before a competent court in accordance with the law governing the jurisdiction of the courts. On the process according to the request are also applied provisions of the law governing civil proceedings, unless this law provides otherwise. Ministry publishes the available jurisprudence regarding the submitted requests and decisions reached in the proceedings under these requirements, based on data received from the ministry responsible for justice. The Ministry is obliged to make this information publicly available on its website.

In the proceedings at the request the value of the dispute is determined by the amount of the total value of goods or services in cases that are contained in the request, and the maximum in the amount of 500,000 dinars. ZP prescribes measures to prohibit unfair contract terms in consumer contracts and unfair business practices in Article 143. In the procedure at the request prescribed in Article 137 ZP, the competent court may:

1) annul and make void any unfair contractual term in a consumer contract and determine that a particular business is unfairly, in accordance with this Law;

2) order the trader to immediately suspend the contracting with unfair contract terms in dealings with consumers and suspend unfair business with consumers;

3) establish the obligation of the seller to, on its own expense, correct part of ads which under the provisions of this law are considered unfair business practices;

4) order the seller to announce its decision of a competent court, to the media, which pronounced the measure of prohibition of unfair contract terms in consumer contracts or measures of unfair business practices, at its own expense.

The applicant referred to in Article 137 of this Law shall be required before such application to invite the other side to resolve dispute in extrajudicial manner. On extra-court dispute settlement procedure are applied provisions of this law on court settlement of consumer disputes.

Law on consumers protection also provides for the temporary measure (Art. 145). The Court may, on the proposal of the applicant under Article 137 of this law to pass an interim measure ordering the suspension of dealer implementation of unfair contract terms in consumer contracts or suspension of unfair business relationships with customers. Provisional or temporary measures may last until the decision of court on a request from Article 137 of this law has been brought.

Lawful confiscation of proceeds is prescribed by article 146 of ZP. If a trader against who has been brought the final court decision on the request referred to in Article 137 of this Law does not comply with this decision within the deadline, any person who has a legitimate interest in it, may submit a request to the court for decision on lawful (seizure) confiscation of proceeds.

PART IV

PRIVACY PROTECTION

PRIVACY PROTECTION

Regulation of Personal Data Processing

Internet works, simplistically speaking, like a large (global) computer network. Hence to the rules of behavior on the internet can be applied general data protection rules that govern in every other computer network, but always bearing in mind the specific actions that the internet has. Data protection may be facing issues of functional nature, such as: a) limiting the use of certain types of data, b) the obligation to provide information, provided the relevant state bodies and organizations and c) informing the citizens about the data on it is collected and for what purpose.[1] Data protection therefore involves situations in which the information belonging to citizens and/or state and non-state institutions, agencies and bodies, are shared in a certain way, or simply made available to some or all users of the Internet. In a broader sense, the study of data protection on the Internet can include legal provisions concerning the existence of certain bodies that take care of the implementation of regulations on data protection. The data on which this is all about can be as personal data, and data relating to the functioning of legal entity's or public authorities and institutions, and welfare implies a double action: on one hand, there shouldn't be made public information that are not defined as such by regulations; On the other hand, the problem of ensuring the integrity of computers and computer systems containing data that are placed on the internet in a restricted form (in strictly certain number of users who have an interest in them and have access to them and manage with those after). It is specific, and understandable that the legal doctrine is primarily engaged in legal regulation of privacy and data, while the area of security systems gains less consideration. However, achieving security system entails, inter alia, regulation and prescription of mandatory standards and norms that should be applied by technical executives (in example: Institutes for informatics and computer centres), independent of the manufacturer of computer systems and software. Measures aimed at systems security are applied to achieve various objectives of safety and security of computerized information systems and those can be various, inter alia: a) measures to ensure the security integrity of computer system's technical components (i.e. hardware), programs, equipment, terminal, console, etc., b) measures to ensure the security and integrity of software components of the system (i.e.,. process) i.e. programs, files, data banks etc.., v) measures the physical security of premises, buildings, vehicles and the like, of accidental or intentional damage, g) measures that contribute to maintaining and raising standards in the professional training of the staff, d) measures of maintaining and improving the standards "regular operating procedure "and so on." Security of computer systems is an umbrella that protects the hardware and software elements of the organization, as well as data and information to be processed by computer misuse, fraud, embezzlement, sabotage, intentional or accidental damage, as well as from natural disasters."[2]

[1] Prlja Dragan, Reljanović Mario, Pravna informatika, op.cit, p. 87.

[2] Van Duyn J. A., The Human Factor in Computer Crime, Los Angeles, 1985, p. 4.

Legal status of Data Protection

Special regulations dealing with the problem of data protection on the Internet and electronic communications in general, emerged as a response to the inadequacy of existing legal protection in the country. The extraordinary development of computers and the widespread use of computer systems has led to digitization of data in almost all areas controlled by the government – in many countries it is possible and entirely common to request through the Internet, using the existing database of citizens, various certificates, and other documents, and even some types of documents, such as traffic and driving permit. "The first concrete forms of legal regulation of data protection in computerized information systems appeared thirty years ago – the first special law that directly regulated the issue of data protection has been brought in 1970 in Germany, a federal state Hesse. In the world today there are in effect a large number of different laws which regulate data protection and privacy rights. As a rule, this area is regulated by a special law or if the state is a federal type then with a special unit of federal laws (e.g., Germany, USA, Canada, etc..).

The Council of Europe adopted in January 1981, in Strasbourg Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data. The intention of the Convention was that signatory countries to harmonize their national legislation with the fundamental principles and recommendations laid in this document. With the respect for the rule of law, human rights and fundamental freedoms, the Convention was intended to bring together its members in extending the protection of fundamental rights and freedoms of individuals, notably the right to privacy, with regard to automatic processing of personal data. States are left to take initiative in the process of regulating this matter in terms of content choice, scope and inclusion of the protection of personal data, with the possibility of expressing certain specifics. In addition, each state must adhere to established principles. One of the basic principles of personal data protection is the principle of legality and impartiality. It means that personal data are collected, processed and used in the manner prescribed by law, which on the other side means that the protection of personal data should include measures and procedures that prevent the illegal gathering, processing, storage, use, exchange and disclosure of personal data from the country. It also means that personal data are collected, processed and used fairly and in a way that does not offend personal dignity of man. Regulations governing the protection of personal data should include provisions based on the principle of data accuracy. This principle determines the quality of personal data and the obligation of responsible persons for the collection and processing of personal data, to perform verification of accuracy, timeliness and completeness of data, as well as their being based on credible sources. The principle implies the responsibility of the person responsible for maintaining records, catalogues, collections of personal data for incorrect, untimely and incomplete data collection, processing and use of personal data. The right of persons to be informed with the collection and processing of data, and in which collections are contained data relating to them, what information are collected and processed, who processes them, for what

purpose and on what basis, and who are the users of these data, is contained, in principle of purposes determination. This principle implies that the obligation of the processing and storage of personal data shall terminate upon termination of the purposes for which the data were collected and processed, or after, by law or by written consent of the person, a certain lifespan of personal data collection. The principle of data availability, in which is included the person whose data are the right to be informed of the existence of the database or other records containing personal information, the right to be able to have access to own personal information, the right of requesting of inaccurate data correction on him or her, and deletion of data if their processing is not in accordance with law or contract, right to prohibit the use of incorrect, outdated or incomplete data relating to him or her, or ban the use of such data if it is not used in accordance with the law or contract. Rights of determined by principle of determining the purpose and principle of the availability of data to the person on which they are can be restricted and can be used to the extent necessary to protect national security, public safety, the monetary interests of the State or the suppression of criminal offenses, as well as the rights and freedoms of others. These are cases in which the exception exists, in accordance with Article 9 of the Convention, and also in accordance with the principles set out in the guidelines for the regulation of computerized files with personal information, the law may restrict the rights of persons whose data were collected and processed and determine the appropriate forms of protection. Because of the need for certain personal information to be collected, processed and used in a special mode for those data sets, as a special category of data, in accordance with the principle of non-discrimination there are prescribed special rules. This special category of data consists of personal data on racial origin, nationality, religious or other beliefs, political or trade union affiliations, sexual life. This type of data can be collected, processed and made available for use only with the written consent of the person to which they relate, and under the conditions prescribed by law. Also personal data on the health status and conviction of persons can be collected, stored and made available for use only in accordance with the law. Exceptions to this principle may be regulated by law, and within the limits established by the International Charter of Human Rights and other relevant documents in the field of human rights and prevention of discrimination. The above exceptions from the proclaimed principles, in accordance with the principle of approval for the exemption, provided that such derogations are expressly provided by law or other regulation adopted in accordance with the internal legal system that clearly specifies its limitations and determines the appropriate forms of protection. In accordance with the principle of security, the law should regulate the measures and procedures that the person responsible for the registration and collection of personal data should have taken to protect these collections, both from natural hazards from accidental loss or destruction, and of the risks that can arise from human action factors, such as unauthorized access, misuse of data or computer virus infection. According to the principle of free flow of exchange and disclosure of personal data from countries in which they were automatically processed or collected for such processing and principles of cross-border exchange of information, national law should provide conditions for cross-border information sharing and privacy protection measures. Unjustified ban on the flow of information cannot be predicted, unless it does not require the

protection of privacy or respect for the principle of reciprocity. Given the importance of the issue of protection of personal data in the laws governing the protection of personal data should be given a separate chapter exercising oversight, or should, according to the national legal system, establish a body to be responsible for the implementation of the provisions of law and respect for the principles on which as they are concerned. The principle of control, in addition to the above, includes a detailed elaboration of the rights of the competent authority and measures to be taken in the exercise of supervision and control of data manipulation. In the domain of power of the competent authorities there is the right to be able to review the collection of personal data and documents related to the collection, processing, storage, transmission and use of personal data, and also to be able to control measures and procedures that responsible person undertakes to protect personal data and to exercise control over the premises and equipment, in terms of achieving the protection of personal data. The competent authority should have the power to prohibit the collection, processing, use and transfer of personal data, if it considers or establishes that it did not meet the prescribed requirements. In the domain of measures that the competent authority may take, which should be regulated by law, are included the right to be able to order the elimination of perceived flaws in the preservation, deletion of data that are not correct or not used according to the law, as well as modify or ban of the use of personal data when it is determined that the personal rights were violated. In line with the need to emphasize the responsibility of all stakeholders involved in the collection, processing, use and protection of personal data, and in case of violation of the provisions relating to the implementation of the basic principles underlying the protection of personal data, national law should predict criminal, civil or other accountability and penalties, depending on the legal system of the state. In Serbian legislation with regard to information of public interest, a special role is given to the Law on Free Access to Information of Public Importance (2004).[3] This law regulates the right of access to public information held by public authorities, in order to achieve and protect the interests of the public to know and the free democratic order and open society. In order to exercise the right of access to public information held by public authorities, the law establishes the Commissioner for Information of Public Importance, as an autonomous state body, independent in the exercise of its jurisdiction. Information of public importance, in terms of this Act, is information held by a public authority, created during or in connection with the work of public authorities, contained in a document, which refers to all that the public has a legitimate interest to know. In order for some information to be considered information of public importance it doesn't matter whether the source of the information was the public authority or any other person, nor what was the information medium (paper, tape, film, electronic media, etc.) whether it is a document containing information, date of creation of information, method of obtaining information, neither are another feature information. Public authority within the meaning of this law is: 1) state authority, territorial autonomy organ, the authority of local governments, and organizations entrusted with public authority (hereinafter referred to as the state authority); 2) a legal entity established or funded wholly or predominantly state agency. Everyone has the right to be informed whether the public authority holds specific information of public importance,

[3] Official gazette of RS, nr. 120/2004.

namely, whether it is otherwise available. Everyone has the right to have available information of public importance so that he or she is allowed to examine the document containing information of public interest, the right to a copy of the document, as well as the right to receive, upon request, a copy of the document by mail, fax, electronic mail or other means. When the public authority does not hold the document containing the requested information, it will forward the request to the Commissioner and the Commissioner shall notify the applicant of its possession, and location to its knowledge. Upon receiving the request, the Commissioner shall check whether the document containing the information sought in the request is in the possession of the authorities who had referred the request. If it determines that the document is not in the possession of the authorities who had referred the request, the Commissioner shall refer the request to the public authority that holds the document, unless specified differently, and shall notify the applicant or refer the applicant to the authority in whose possession of the requested information. The procedure will be determined by the Commissioner, depending on efficiency of realization of the right of access to information of public importance. If the Commissioner submits a request to the authority, the time limit begins to run from the date of delivery. To this procedure are implemented provisions of the law governing general administrative procedure relating to the decision of the first instance, unless the law provides otherwise.

Within three months from the end of the fiscal year, the Commissioner shall submit to the National Assembly an annual report on the activities undertaken by the authorities in the implementation of this law, as well as their activities and expenses. In addition to this report, the Commissioner shall submit to the National Assembly other reports as it deems it necessary.

National instruments of protection – Law on protection of personal data

The new Constitution of the Republic of Serbia guarantees the right to protection of personal data. In addition, Serbia has signed the Additional Protocol to the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows of the Council of Europe. Also, due to the transfer of responsibilities from former federal agencies to state bodies of the Republic of Serbia, the relevant legislation was not determined by the state authority to take over the responsibility for the exercise of rights under the law, which actually means that the protection under the law could not be realized in practice.[4]

For these reasons, a new Law on Personal Data Protection Act,[2] which came into force on 1 January 2009. This law thoroughly regulated protection of personal data, processing and use of this information, citizens 'rights of access to information, as well as the body responsible for overseeing the implementation of this law and the protection of citizens' rights, in accordance with the law.

[4] Drakulic M., Jovanovic S., Drakulic R., 2010, *Establishment CSIRT-a in Serbia, Incorporation of Broadcaster according to Serbian Broadcasting La,w* article presented at the conference 12h International symposium FOS, SymOrg 2010, Zlatibor, 2010.

Subject to the law as defined in Article 1: This law regulates the conditions for the collection and processing of personal data, the rights of persons and the protection of rights of persons whose data are collected and processed, restrictions on personal data protection, the procedure before the competent authority for the protection of personal data, providing information, records, data export from the Republic of Serbia and supervision of the execution of this law. Protection of personal data is provided to every individual, regardless of nationality and place of residence, race, sex, language, religion, political or other opinion, nationality, social origin, property, birth, education, social status or other personal characteristics. The tasks of protection of personal data are within the powers of the Commissioner for Information of Public Importance and Personal Data Protection (hereinafter the Commissioner), as an autonomous state body, independent in the exercise of its jurisdiction.

The aim of the law is that, with regard to the processing of personal data, for every natural person to exercise and be protected of the right to privacy and other rights and freedoms.

The Act contains 11 sections: General provisions, terms and conditions for the processing, rights of persons and the protection of the right people, process the appeal, the Commissioner, data security, Database, Presentation of data from the Republic of Serbia, Supervision, Penal provisions and transitional and final provisions.

Article 5 gives us the specific personal data on which are not applicable points of the law, and that are the data which are available to anyone and published in newspapers and other publications, the data which are processed for family purposes and are not available to third parties, information about members political parties and other associations, when processed by these organizations, and information published by a person about himself or herself.

In the second part of the conditions for processing (Article. 8-18), article 8 of the Act governs the Unlawful processing of personal data. Processing is not permitted without the consent of an authorized person and without lawful authority, if it is done for a purpose different from that for which it is determined or if the purpose of the processing is not clearly defined or changed, or if the method of processing is illegal for other reasons prescribed by law.

Articles 10-12 of the Law are regulated by the processing with the consent, or without consent. Article 12 of the Law stipulates that the processing is permitted without consent for the purpose of exercising or protecting vitally important interests of the person, for the purpose of enforcement of obligations under the law and in other cases prescribed by law exclusively.

Article 13 of the Law stipulates that the state agency can process data without the consent of the person if necessary to achieve the interests of safety, criminal proceedings, to protect the economic interests of the state, protection of health, rights and freedoms and other public interests.

Article 14 of the Act governs data collection. Data can be collected from the person to whom they relate, and from other persons on the basis of the contract, if required by law or regulation, if it is necessary, given the nature of the work, and if the data is collected to achieve the vital interests of the person which to they relate and if

data collection from the very people they refer, doesn't require excessive amounts of time and resources.

Article 15 of the Law stipulates that the data controller shall, prior to the collection and processing of that person make person (on which the data relate) familiar with it. Also, this article has an exception from this obligation, but provides that the operator shall subsequently inform the person to whom the data relate about the processing and data collection.

Articles 16-18 of the Law prescribe the treatment of particularly sensitive data. Article 16 of the Law stipulates that particularly sensitive data are data relating to nationality, race, sex, language, religion, political or other opinions, trade union membership, health, sexual life, social assistance, a victim of violence and conviction for a criminal offense. It also stipulates that the processing of these data must be specifically defined and protected by security measures.

In the third part under title of the rights of persons and the protection of the rights of persons (article 19-37) in articles 19-22 Law regulates the rights of persons regarding the protection of personal data, namely: the right to be informed about processing, the right to access, the right to copy and right after the insight. It should be particularly emphasized the right of persons after the insight, which is accomplished by the entitlement of the person to require amendment, update, deletion of data, as well as stopping and temporary suspension of the processing of personal data from of the operator of the personal information.

Section 23 of the Act prescribes the limits of the above rights. These rights may be restricted if a person is abusing their right to be informed, to have insight, and to a copy, if the controller is enabled from performing their duties, if giving notice would seriously jeopardize the security of the country, an important economic or financial interest of the state and the criminal proceedings, if the notice to make available data that is marked as confidential, if the information would seriously jeopardize the privacy or vital interest of a person and if the information about the person solely for use in scientific research and statistical purposes.

Articles 27 and 28 of the Act are governing the enforcement of the right to insight and copy. It was introduced the obligation for the operator to make all data available to the applicant in the state in which they are, as well as to provide the necessary expertise to understand the content of the data. It also stipulates that the right to insight shall not be subject to the payment of fees, and that the applicant bears only the necessary costs of making and transferring data.

Articles 35-37 of the Law stipulates obligation of storage and use of data in the case of death of person whose data are, also stipulates the obligation of the data operator to delete data in the event of termination of the contract or withdrawal of consent, and adequate application of the law governing general administrative procedure.

In the fourth part under the title the procedure on appeal (article 38-43) under article 38 of the Act provides that the applicant for the enforcement of rights in connection with the processing of data can appeal to the Commissioner. It is stipulated that an appeal may be filled to a decision which was denying or rejecting the request, in case the operator does not decide on the application within the prescribed period, if

the operator does not decide upon request to information, or issue a copy in the time and in the manner prescribed by law, if the operator conditions the issuing by payment of a fee which was not prescribed, and if the operator makes difficult the enforcement of rights.

In the fifth section, which deals with the Commissioner (Art. 44 and 45), Article 44 of the Law stipulates the powers of the Commissioner under this Act. The Commissioner is required to submit a report to the National Assembly, which shall also be submitted to the Government and the President of the Republic and appropriately available to the public. The Commissioner may also have a deputy for the protection of personal data. In Article 45 of the Law it is stipulated the right to access and inspect the Commissioner in relation to the protection of personal data, as well as the limitation of this right.

In the sixth part related to data security (articles 46 and 47), Article 46 of the Law stipulates the obligation for the Commissioner to maintain confidentiality, his deputies and employees in professional services in connection with the information learned in the performance of their duties. The obligation to maintain confidentiality continues even after the termination of office or employment. Article 47 of the Law stipulates the organizational and technical measures to protect personal data against misuse, destruction, loss, alteration or unauthorized access.

In the seventh part of the record (Articles. 48-52), in Article 48 of the Law stipulates that the operator is obliged to create and keep a record of the data and the collection of data which processes, as well as the content of such records.

Part Eight - The transfer of data from the Republic of Serbia (Article 53) it is provided that the data from the Republic of Serbia may be transferred in a Member State of the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe, and in other countries that are not party to the Convention if it is provided level of data protection in accordance with the Convention, on the basis of permission of the Commissioner.

In the ninth part under the title Supervision (Art. 54-56) stipulates that supervision over the implementation of this law conducts the Commissioner through authorized persons. Based on the findings of the authorized person in the enforcement of supervision, the Commissioner may order that the irregularities are corrected within a specified time, temporarily prohibiting the processing that is done contrary to the provisions of this law, and order the deletion of data collected without legal ground. Against the act of Commissioner in the enforcement of supervision the plea is not allowed, but an administrative dispute is.

Tenth part under the title of the penal provisions (Article 57) contains provisions for the misdemeanor violation of the law. This law is prescribing a fine of 50,000 to 1,000,000 dinars for a violation of this Act by the operators, processors or users that have legal status of legal entity.

The eleventh part refers to the transitional and final provisions (Articles. 58-63).

Article 59 of the Act provides that the Commissioner for Information of Public Importance, established by the Law on Free Access to Information of Public Importance, continues to work as the Commissioner for Information of Public Importance and Personal Data Protection.

The rights of a natural person are defined by the Law on the Protection of Personal Data are:

Right to giving/not giving consent for processing - any natural person has the right to refuse/or to consent to the processing of data about themselves, if the operator does not perform processing on the basis of legal authority. Natural person may give a valid consent through middleman / representative, and may revoke given consent in such manner. To the person consented to, the operator is obliged to previously inform about its identity and any other matters referred to in Article 15 of the Act.

Right to be noticed of the processing - person has the right to require from the operator to be fully and accurately informed about whether it processes information about him, which data and for what purpose and on what legal basis and from whom they were collected; which collection of data contains information about him, who are the users and what data and for what purpose and on what legal basis; where and which data is transferred, for what purpose and on what legal basis, as well as all other matters referred to in Article 19 of the Act.

The right to have insight - has the right to demand that operator makes available data relating to him. The right to access includes the right to see, read and hear the data and make notes.

The right to copy - a person has a right to request from the controller back up (or copy) of the data relating to him (or her) and is obliged to bear only the necessary costs of making and submitting of those copies.

Rights after the insight - a person has a right to request from the controller amendment, update or deletion of data, as well as stopping and temporary suspension of the processing, if the conditions laid down in Article 22 of the Act are met.

The operator of personal data, which may be a natural person, legal entity or authority, collects information from the person to whom they relate, or from any other person. The operator is obliged to perform data processing on the basis of the consent of the person or by law prescribed power. If an individual withdraws consent, the operator must then stop performing of data processing.

The operator is required to process the data in all respect to the provisions of the permissibility of processing (Article 8 of the Law).

The operator shall, prior to collection, usually in writing, inform the person to whom the information relates, or another person on their identity and all matters relating to the processing of data, in accordance with Article 15 of the Act. The operator shall notify the person about the amendment (change) or deletion of data.

The operator is obliged to truthfully and fully inform the applicant on all matters relating to the processing of data under Article 19 of the Law, and without delay, no later than 15 days from the date of the request for information about the processing was filled.

The operator is obliged to allow the person to inspect the data relating to him (her) or to hand over a copy, without delay and at the latest within 30 days of receipt. In case of justified reasons, these deadlines of 15 or 30 days can be extended for 30 days more. The operator is obliged to make available to the applicant information that relates to it, and in a comprehensible form, or to make data available in the state they are located, and at the request of providing professional help to understand the contents of the data do

so. The enforcement of the right of access is free, but the applicant has to pay only the necessary costs of making and transferring of backup (copied) data.

Also, the operator shall, without delay, and no later than 15 days from the date of the request, decide on the request for eligibility after the insight (correction, addition, updating, deletion, interruption and suspension of processing), as well as the notice to the applicant.

If the controller does not process the information, it will forward the request to the Commissioner, unless the applicant opposes to that. The operator is required to implement the decision (order) of the Commissioner and to the authorized people of the Commissioner provide uninterrupted supervision and give them access into the necessary documentation.

If data collection is established by contract, or with the consent in writing, in the event of termination of contract or withdrawal of consent, the operator is required to delete submitted data within 15 days from the date of termination or withdrawal of consent, unless otherwise required or agreed.

The operator is obliged to take all necessary technical, personnel and organizational data protection measures, in accordance with established standards and procedures, which are necessary in order to protect data from loss, destruction, unauthorized access, unauthorized alteration, publishing and every abuse, and to determine the obligation of persons employed in the process, to keep the secrecy of the data.

The operator is obliged to form, maintain and update records of processing data that contains the elements referred to in Article 48 of the Law, all in accordance with the Regulation on the form for keeping records on the processing of personal data.[5]

The operator shall, prior to commencement of processing, or the establishment of databases, submit to the Commissioner a notice of intention to establish a data collection of the necessary data (Article 49 of the Law), as well as of any subsequent intended processing, before undertaking procession and no later than 15 days before the establishment of the data base, or processing. The operator shall submit to the Commissioner also records relating to the collection of data or changes in data records, not later than 15 days from the date of establishment or changing. The above information and records are mandatory entered in the Central Registry.

In accordance with the Act, the Regulation on the form for recording and keeping records on the processing of personal data has been brought and also the Ordinance on the manner of prior inspection of processing operations of personal data and the Ordinance on the form of identification of the authorized person to supervise the Law on the protection of personal data which all precisely regulate this area.

Current law does not cover the collection and processing of data over the Internet. Consent of the person for processing personal data is requested in writing and in the case of online registration is virtually impossible. The law does not recognize the terms of the many portals where users daily leave various personal data. Using social networks and specific methods of creation and use of databases definitely requires modification of the existing law and the introduction of specific provisions that precisely regulate this area.

[5] Official Gazette RS, nr. 50/09.

PROTECTION OF TELECOMMUNICATIONS PRIVACY

The right to privacy on the internet and protection of personal data

Despite numerous attempts to establish a single definition that refers to the right to privacy, the term has remained relatively vague. One of the earlier definitions of the rights formulated by the American jurisprudence at the end of the nineteenth century was that it means "right to be left alone". It has often been pointed out that, along with the first devices of information technology (telephone, telegraph, etc...), the modern concept of the "right to privacy" was created. The concept of privacy was finally set out at the end of the last century, in the famous work "right to privacy" of authors American Judge Samuel Warren (Samual Warren) and Louis Brandeis (Louis Brandais).[6] Contemporary legal theory of the right to privacy observes it from the so-called active standpoint. The advantage of definitions of privacy, which start from the control of information, is that it makes it possible to clearly identify the actual interest (e.g. while performing electronic surveillance and monitoring). Interest that occurs when the right to privacy is the interest of self-determination of communication (of the individual) with others and reflects the desire of individuals and groups to communicate information about themselves as they see fit and where they see fit.[7] Contemporary concept of the right to privacy of personal and family life involves complex human right, which can be observed from several aspects: the privacy of home, correspondence, communication, intimacy and family life. there are various consequences of the existence and practice of law: the private life of each individual, especially the part that takes place in his home, is protected from any (unauthorized) public scrutiny; Even when it comes to public figures who are always under the watchful eye of the public and the media, the boundaries are clearly drawn and cannot be crossed. Home, as such, is protected from unauthorized intrusion of others, as well as representatives of state government and law, except in cases in detail and clearly regulated by law. The same is the case with the correspondence, or more recently the current communication via telephone and electronic devices. It is forbidden to eavesdrop, intercept and interfere with the communication of individuals or groups with other individuals or groups – it is a constitutional principle that must be respected and which suffers a small number of statutory exceptions, related to the investigations of crime. On the other hand, there is the protection of individuals and groups from the insights of other individuals in their private and family life. The state, therefore, is in a specific position – it refrains from violating the right to privacy, but at the same time protects citizens from such violation of rights by non-state actors, individuals and organizations.[8] Development

[6] WarrenSamuel, BrandaisLouis, The Right to be Left Alone, Harvard Law Review, 1890. (G.L. Simons, Privacy on the Computer Age, p. 14).

[7] Schafer Arthur, Privacy - A Philosophical Overview, Aspects of Privacy Law, Edited by Dale Gibson, Toronto,1980, p. 9.

[8] Schafer Arthur, Privacy - A Philosophical Overview, Aspects of Privacy Law, Edited by Dale Gibson, Toronto,1980, p. 9.

of electronic communications as such has brought a range of options to compromise or violate the right to privacy. Many of the actions that individuals or organizations are doing and that could be categorized as a violation of privacy rights, does not fall within the high technology crime; In fact, it still does not fall within any of punitive or prohibited types of behavior. The right to privacy, however, may be violated by the use of electronic communication devices in two main ways. The first is a violation of law by individuals, groups or organizations, as well as other government and non-government bodies; another is a violation of the police and other relevant authorities in investigating crimes cybercrime.

The most drastic form of invasion of privacy by using the Broadcast Communications is stealing a person's identity in order to obtain financial or other benefit (Phishing). This will happen when someone carelessly leaves or uses their personal information such as identification number, credit card number, different passwords and pin codes in a way that allow access to private data of that person. Once his personal data are compromised or have become available to another person who otherwise has no authorization to access them, they can be used for various illegal purposes. A person who has obtained the private data is impersonating as a person whose information illegally were obtained and as such, for instance concludes electronic contracts, purchases in online stores, transfers money from a credit card, and so on. It is possible to imagine other forms of invasion of privacy of persons, which in most cases are defined as punishable, such as the use of others' data or character without intending to take over the identity of the person; use of data that people leave on the internet for marketing purposes. All of these actions represent violation of the rights of individuals to privacy and other personal rights. It should be noted that there are still significant differences in the manner of execution and the proceedings o crime and social hazards that traditional crimes carry out. How for example can we characterize falsely posing like someone else's character? This is a question that has not been resolved in the legislation, both in Serbia and in other countries. It is obvious that stealing someone else's character (digital identity) by itself does not entail consequences that would be socially dangerous – unless the person impersonates other person while committing criminal act (e.g. Paedophiles on the Internet often pose as children to gain their trust their potential victims). However, taking other people's photos and creating fictitious profiles in order to achieve the popularity of a particular social network, is certainly a violation of the privacy of persons whose images were used. Electronic payment, online shopping or just visiting some specialized sites can also be misused, and for marketing purposes. Based on the information that a person leaves, in this way can be reconstructed his or her entire private life, habits, marital status, whether he or she has have a pet, and the like. Famous examples are people who have bought certain products on the Internet, and all of the sudden they have begun to receive unwanted e-mail – advertisements for the same products. If you post a picture today from a trip to a social network and specify the location where they were taken (geotaging) there is a great possibility that you will be in some of future visits of that site, "ambushed" with series of ads – advertising just to travel to the location you visited, or sites that are culturally, historically or otherwise related. The question is whether this is legal?

Unfortunately, the conditions of use of various social networking and other services that are on the Internet and that people typically "in good faith" are to accept without reading, always include a clause on the use of personal information that users leave on those sites for various purposes, most commonly for modelling of the ads that appear on the sides of the examination in accordance with his habits, experiences, education, interests, etc..[9] Although this is, formally speaking, however, a step in the right direction in relation to the situation which existed before and which is still often experience (especially in countries like Serbia where there is no developed awareness and culture of personal data storage and the sanctions under Rule are absent) when the companies that come to the personal data of the user remains the same sold for advertising, or exercise more drastic criminal activity.[10]

The basic question in the conducting of investigations of pre-trial proceedings and during the presentation of evidence during the criminal proceedings, it is how it can interfere with the privacy of citizens, in order to establish an appropriate balance between finding and prosecuting the offender, and that in this manner it is done without compromising any of his rights or the rights of third parties. This question has received a new dimension when it comes to high technology crime. How the classical methods and investigative techniques, classic standards invasion of individual privacy can be used, when it comes to the virtual world? Very quickly it became apparent that the acts committed with a computer and computer networks were not easy even to perceive, and that traces of their existence easily and efficiently were removed by the perpetrators, but also as a result of the action by a variety of other factors. Therefore, it had to be developed specific powers of investigation agencies, primarily the police in conducting investigation activities. In the modern theory prevails point of view that the scope of these powers is still vague and that only practice will show how it could be developed further.[11] European Convention on Cybercrime specifies the procession (investigation) actions that can be executed when investigating high technology crime. In these actions, among others, are included: Expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, issuing orders (Production order) to give – produce, as well as search and seizure of stored computer data, Real-time collection of traffic data, Interception of content data. This Convention in Article 15 states "Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments,

[9] Compare with: Reljanović Mario, Odnos prava na privatnost i pojedinih aspekata visokotehnološkog kriminala, in: Komlen-Nikolić Lidija et alia, Suzbijanje visokotehnološkog kriminala, Beograd, 2010, pp. 201-213.

[10] For example it is famous case of selling of house addresses of families who were paying tourist arangements online. In this case their homes were exposed to burglaries and perpetrators were informed of their (house tennants) absence from homes – because of vacation. Ibidem.

[11] Drozdova Ekatarina A, Civil Liberties and Security in Cyberspace, u: Abraham D.Sofaer, Seymour E. Goodman (ed.), The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press, 2001, p. 204.

and which shall incorporate the principle of proportionality." This sends a clear message that there must be set the clear line between the new investigative powers and guaranteed human rights and freedoms, as well as in the event of a conflict between these two types of norms, the preservation of human rights and freedoms of citizens is a priority. Guidelines for the cooperation between law enforcement authorities and Internet service providers in the fight against cybercrime, which was published by the Council of Europe in 2008,[12] believe that Internet Service Providers (ISP) and police and prosecutorial authorities are the basis of investigating on which the system for detecting and investigating these types of crimes is funded. Hence, it is important for each country to regulate their relationship in a way that would allow monitoring of traffic on the Internet, but at the same time guaranteeing the protection of the rights of computer users, and worldwide network. Even the privacy of data traffic specifically mentioned as one of the goals that effective cooperation must aim.[13] Of other ways to prevent abuse of such procedures, guidelines specifically recommend that every order that comes from the prosecution or the police may be submitted only in documented form (in writing), and in extreme emergencies when it is possible only a verbal agreement, the documents shall be subsequently delivered without delay. Requests must be clear and unambiguous and precise and focused only on the data that are necessary to implement the necessary investigations. Also, all the data that ISPs provide to investigating authorities must be confidential and used only for the purposes for which they were collected. Comparative solutions are based on these principles.[14] It was established the principle of proportionality, the measures to be taken and the severity of the offense in question, so that invasive measures do not apply to petty forms of crime, or in cases where they don't have a rational purpose. In those cases with realistic expectations that implementation will lead to the discovery of a crime or facilitate its processing, are applied different restrictions. Thus, for example in Belgium and Hungary, the data owner or administrator of the system must be informed about which data are copied during the investigation; information stored on computer networks will be copied only if there is a real danger that they will otherwise be permanently deleted; In any case, it will copy only the data that are necessary for the implementation of criminal procedure - the standard "minimum occupation of privacy" can also be found in other countries, e.g. Estonia, Spain, and in the Austrian Code of Criminal Procedure. Also in Belgium, Austria and Finland, there is a standard of confidentiality of data downloaded and its use could be only for purposes of investigation and criminal proceedings. There are other specific limitations – e.g. German Code of Criminal Procedure provides that this data can be viewed only prosecutors, but not the police authorities. Further, the evidence found on the computer can be accepted in the proceedings against a person if the claimant can show that the computer was working normally at the time of its seizure, or that that person is actually used in a database from a computer (audio, video,

[12] Guidelines for the cooperation between law inforcement and Internet service providers against cybercrime; Internet addres http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_provdguidelines_provisional2_3April2008_en.pdf i http://www.ifap.ru/library/book294.pdf, 01.07.2012.

[13] Guidelines for the cooperation between law inforcement and Internet service providers against cybercrime, articles 14. i 15.

[14] Compare: Lorenzo Valeri, et alia, Handbook of Legal Procedures of Computer and Network Misuse in EU Countries (2006), and national reports available at Internet address: http://www.coe.int/cybercrime , 01.08.2014.

documents, malware and the like.), as well as to the content of hard disks and other carriers of information on computer was not changed from the time of its seizure and the presenting of evidence. Otherwise, the performance of the alternation of the computer is considered evidence of contamination. This solution exists for example in The Cyprus legislation (Law of Evidence and Criminal Procedure), as well as in the UK (the Law on Police and Criminal Evidence and Procedure police Guide good practice in collecting computer evidence). Search and seizure performed at premises (apartments, office space) is mostly for the same conditions as for any other crime – the police can access the search (the search) with the court order, and without it, only in cases prescribed by Code. When it comes to wiretapping and interception of communications data, are also parallel can be drawn with the "classic" investigative methods – mandatory court approval (in Finland, for example. Comes to superior court), and these actions can last a limited time. In Estonia, for example it is expressly stated that the so-called "Internet monitoring" is not an everyday police activity, and can be done only in cases where there are grounds to suspect that certain communications are used for the commission of acts of cybercrime. French Code of Criminal Procedure (Article 100) makes additional requirements for the interception of data - information that will be collected in this way, must be particularly important for the study of the crime. The German Constitution (Basic Law) protects citizens' rights to privacy in communications – hence the interception can only be done for certain offenses of particular interest (threat to national security, terrorism, etc...) while for all other work must obtain a court order, or prosecutor in an emergency. In Poland, data interception and surveillance of electronic communication is possible only for acts which are expressly stated in the Police Act and the Criminal Procedure Code, a part of cybercrime can be subject to such measures only if it is proved that it was one of the execution phases of a complex, more serious criminal offenses. In many countries there are no specific provisions for the investigation acts of the cybercrime: Italy (with a few exceptions), Belgium, Portugal, Estonia, the Netherlands, Latvia, Lithuania, Slovenia, Luxembourg, Poland, etc... In these states the offenses associated with computer investigate and prosecute on the basis of an extensive interpretation of the existing provisions on investigative and other activities. In each case, the prosecutors and the judge who determines what can be implemented as an investigative action and what evidence can be admitted in the proceedings. However, the main conclusion to be reached is that the courts have accepted all the specifics in the process of proving acts of cybercrime as absolutely necessary, and that the emergence of electronic evidence normally takes place in these proceedings. It also means that they must be collected with care and that to them and their acquisition are applied the same standards of respect for human rights, especially the right to privacy, as well as other substantive and procedural limitations written into national laws. The Law on Personal Data Protection provides answers to some of the questions that may be important when it comes to problems with the collection and retrieval of data in the process of carrying out an inquiry or investigation by regulatory authorities. Personal data is any information relating to an individual, regardless of the form in which it is expressed and the information (paper, tape, film, electronic media, etc..), on whose orders, in whose name and for whose account information is stored, the date of creation of information, a place to store information,

the method of obtaining information (directly, through listening, watching, etc., or indirectly through access to a document containing the information, etc.); written form shall mean any method of electronic printing, and storing data. Data processing is any action taken in connection with data such as collection, recording, copying, reproduction, copying, transferring, searching, sorting, storage, separation, intersection, merging, adapting, modified, providing, use, disclosure of, disclosure, publication, dissemination, recording, organization, storage, adaptation, use, disclosure by transmission, or otherwise making available, hiding, moving and otherwise making available, as well as implementation of other actions in connection with the above data, regardless of whether the performed automatically, semi-automatically, or in another way. Data processing is not allowed in the following cases: if the person has not given consent for processing, or if the processing is done without lawful authority; if it is done for a purpose other than that for which it is determined, whether it is done on the basis of the consent of the person or legal authorization for treatment without consent; if the purpose of the treatment is not clearly defined, if it is altered, unauthorized or already accomplished; if the person to whom the data relate to could be a fixed or determinable, and after reaching the purpose of processing; If the mode of processing is not permitted; if the data being processed is unnecessary or unsuitable for achieving the purposes of the processing; If the number or types of data to be processed to the purpose of processing; if the information is false or incomplete, that is not based on a credible source or is outdated. When this provision is considered from the point of view of electronic data processing, this may mean that personal data can be collected (the same applies to their processing, analysis, storage, modification, destruction, etc..) only if: it was done while respecting legal procedures (as with respect to the jurisdiction of which they collect, and in terms of the steps that the law defines); there is a real basis for their collection (otherwise there is abuse of authority by the authority collects them); the collection is done to the extent that is absolutely necessary for the execution of investigation and at the same time using the least invasive means. This basically means that the person who collects the data as provided by law, to refrain from any access to the data, their copying, other ways of distributing or other types of analysis, in a situation where it is clear that the data in question cannot relate to the subject his conduct. These rules have a practical significance, especially in situations of carrying out an investigation, or some other kind of test procedure. In practice this for example would mean that, if it is known that a person with his private e-mail accounts communicates with another person in a manner that constitutes a violation of a regulation (e.g. betraying trade secrets), a person who is reviewing the data can easily view e-mails to the address of the recipient message and isolate only those messages for further processing. The moment he or she finds the email that was requested, that person will not go into further search, for example other recipient address or other e-mail accounts that are on that computer. The exception to this may occur when there is a reasonable suspicion that there is a similar communication with others, or that were used some other e-mail accounts for unauthorized communication. It is very difficult at that time to assess whether the conditions for further examination of electronic data on computer or other medium, when a person performs search finds the data for which have been searching, or data that was known of in advance or suspected of their existence. How-

ever, if during the search of the computer or other device comes to personal data which obviously cannot have anything to do with the subject of the investigation, the person who is searching is obliged to refrain from their review and analysis. For example, if the above-mentioned search of e-mail comes to medical data or data on the sexual orientation of people, they can't be further reviewed and analyzed, or used in any other way, because they aren't relevant factors in the proceedings pending against the person. The exception to the various limitations of this kind exists if a person, after being informed of the processing of the data, consents to the disclosure of all data with no exceptions. However, even then there are exceptions related to special categories of data: those who reveal their nationality, race, sex, language, religion, political party affiliation, union membership, health, social assistance, victim of violence, a conviction for a criminal offense and sex life. They can be processed only with the prior consent of the person, in accordance with the relevant legal regulations which allow for such processing. The person whose data is used in each case have the right to be informed that information about him (her) being used, for what purpose and in what manner, and in case it finds that any of his rights have been violated during the inspection, collection and processing of personal data, person may appeal to the Commissioner for Information of public Importance and Personal Data Protection. Violation of regulations on the protection of personal data is the basis for tort liability.

The Criminal Code of the Republic of Serbia

The Criminal Code of the Republic of Serbia in the Chapter Offences against the rights and freedoms of man and citizen prescribes seven offenses in violation of the right to privacy and protection of personal data.[15] Violation of a confidential relationship doctor-patient or lawyer and client in which is circumvented even particularly sensitive personal data is criminalized by Article 141. Unauthorized circumventing of secrets can be done only in the public interest or in the interest of another person that outweighs the interest of keeping it a secret. This ensures that information systems are increasingly present in the public sector (health, justice, education, etc...) and they must be carefully implemented with precisely defined authorities who have the right of access to that information in accordance with existing regulations. Article 146 stipulates that unauthorized collection of personal information and one shall be liable to any unauthorized collection, processing, use and disclosure of other personal data. What is often controversial in the collection and processing is a choice of a range of data required for the purpose of procession is not clear. It is necessary to review the existing requirements, forms, both paper and electronic, those are filled without a doubt of the legitimacy and relevance by individuals who are often not asked nor informed of how these data continue to be used. Separate paragraph prescribes the punishment for an official who commits the act in an official capacity for what may be sentenced to imprisonment violation of the secrecy of letters and other items (Article 142) which protects the privacy of written communication. This article explicitly points out that the criminal act may involve a violation of the privacy of electronic mail or other means of

[15] Criminal code, "Official gazzete of RS", nr. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012 and 104/2013.

telecommunication by which electronic communication is equated with the traditional writing letters, telegraphs, etc... In case this is done by some other person may be punished by a fine or imprisonment of up to two years. Infringement of privacy in the case of oral communication is defined in Article 143 of the unauthorized interception and recording that is becoming more actual with the development of technologies which easily be exploited for this purpose. With audio often performs video recording which is specifically provided for in Article 144 Unauthorized photographing. Intervention of the Commissioner that the traffic monitoring cameras are removed because they are not properly installed, as well as some cases of the use of public cameras intended to enjoy the panoramic view of the city for the purpose of recording and invasion of intimate lives of citizens are just some of the examples of violations of privacy. Incriminating allegations of former Officer of National Security Agency – Edward Snowden that,[16] under the auspices of national security are violated basic human rights and that are performed unauthorized recording of electronic communications not only by politicians and other public figures, but a large group of people without a clear basis, suggest that such situations are possible in Serbia. Official person for unauthorized photographing can get up to three years for wiretapping and recording of up to five years prison sentence. Law on Electronic Communication prescribes ways of performing covert surveillance without a regulated video surveillance and information security in general, and there can't be precisely determined frameworks of individual privacy without jeopardizing the security of the state and vice versa. In the era of social networks is important to mention Article 145 Unauthorized publication and presentation of someone else's writings, portraits and recordings without the consent of the person whose determination, at least when it comes to the most popular networks – Facebook, which is one of the main activities of sharing photos, texts and comment require additional review.

The key problem is that for all the offenses which criminalize violations of privacy and some form of misuse of personal data all proceedings can be initiated only by private action of citizens, except when officers on duty have done the criminal act – when the prosecution is ex officio starting procedure. This means that state has left the realization of this right to individual. This raises the question whether the severity of the offense is adequately regulated because for other freedoms and human rights (equality, the right use of language and script, expressing national or ethnic origin, freedom of movement, confession of faith, and the like.) it is provided that the state must intervene. By amending of the Criminal Code provisions message will be sent to all who are willing to ignore the right to "be left alone" would be clearer. Identity theft and various forms of downloading personal data from the Internet (e.g. Phishing) are not specifically criminalized in the Criminal Code of the Republic of Serbia but are treated as fraud (Article 208).

[16] The National Security Agency/Central Security Service, USA, http://www.nsa.gov/index.shtml, last accessed on 13.03.2014

PART V

COMPUTER RELATED CRIME

COMPUTER RELATED CRIME

General Legal Development

The significance of information and communication technologies has created the need to establish worldwide measures and mechanisms for the protection of society and the individual against abuses in this area, through adopting appropriate legislative solutions and improving international cooperation. The result of these efforts, among other things, the adoption of Council of Europe Convention on Cybercrime,[1] which has established minimum standards that are necessary, in the opinion of the international community to meet the national legislation in order to effectively combat the abuse of high technology. Criminal-law solutions in this field in Serbia can be classified into two groups. The first group makes a substantive provision which stipulates those actions are socially unacceptable behavior that violate or infringe certain protective structures. It's Criminal Code.[2] The provisions of this legal text were analyzed primarily in the part relating to offenses against the security of computer data, as well as to crimes that are under the provisions of the Convention on Cybercrime grouped with computer offenses and which, by their nature they are, although they in the Criminal Code are grouped into chapters that protect business operations, sexual freedom, copyright, intellectual property and others. The second group consists of the Criminal Procedure Code[3] and the Law on Electronic Communications[4] (as well as certain by-laws) that establish a procedural framework, but the framework provided by the Convention and without procedural nature, which have provided mechanisms and powers of state agencies in the detection procedures, evidence collection, criminal prosecution and trial of offenders cybercrime.

Significant concerns in this segment was created on the issue of the organization of the judicial system of the state towards creating conditions for successful combat and combat new forms of criminal activity. Specifically, whether to opt for a comprehensive systemic change, or change a number of regulations in order to create an adequate legal framework, or be oriented towards a partial amendment of certain legal provisions in order to create conditions for the timely and adequate response to new forms of criminal behavior, that is the question each state has solved or is dealing in accordance with their capacities. The first method is without a doubt very effective, but also very demanding, since it requires a high degree of political and social consciousness of the necessity of changes that should be followed, while the second method is more economical and less demanding method, as it does not impinge on the basis of the system, but who can leave behind a series of unresolved issues such as the question of jurisdiction for certain crimes, the collision of new and existing legislation, and so on. In accordance with the

[1] Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5, 2010)

[2] Official gazette of RS, nr. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013.

[3] Official gazette of RS, nr. 85/2005, 88/2005 - change, 107/2005 - change, 72/2009, 111/2009 i 121/2012

resources available, Serbia, with the aim of criminal law protection of new forms of computer crime, opted for a different way of organizing its judicial system, oriented for partial changes of certain legal provisions and the adoption of new laws, establishing new state authorities for procedure in criminal cases in this area.

In order to complete the analysis of criminal-law provisions in Serbia at the beginning will be presented to Council of Europe Convention on Cybercrime and its Additional Protocol, and then the substantive and procedural provisions of legal solutions in the field of ICT abuse.

Council of Europe Convention on Cybercrime was signed in Budapest on 23 November 2001, and the Additional Protocol referring to the criminalization of acts of a racist and xenophobic nature committed through computer systems was signed in Strasbourg on 28 January 2003. The Republic of Serbia signed both documents in 2005 in Helsinki, and in 2009 the National Assembly of the Republic of Serbia has ratified them. By ratifying the Convention and the Additional Protocol should be essentially innovated all laws that directly or indirectly regulated the area of information and communication technologies, and particularly the laws governing criminal-legal protection of these areas. In this way, the institutional framework was created for a more effective fight against cybercrime.

Decision of the Council of Europe

Convention on Cybercrime

So far, the Convention has been signed by 47 countries, of which those that are not members of the Council of Europe (4 of them including the US), of which it has been ratified by only 26 countries.[4] Serbia is among the countries that have signed the Convention (2005) and ratified it (2009). States that are not members of the Council of Europe signed the Canada, Japan, South Africa, Australia (which has ratified it) and the United States).

The Convention defines a total of nine offenses that are classified into four groups.

The Convention consists of four sections:[5]

(I) The use of the term;

(II) Measures to be taken at national level – substantive criminal law, procedural law and the jurisdiction of the Contracting Parties for the criminal acts prescribed in accordance with the Convention;

(III) International cooperation – general principles, specific provisions;

(IV) Final Provisions.

The first chapter gives a brief overview of the Convention and definitions of key terms that are used in the text of the Convention.

[4] Convention was not signed by Council of Europe parties: San Marino, Russia (which decisevly has rejected signing of this Convention). On the other side it is interesting that within EU Ireland, Liechtenstein, Poland, Sweden, Greece and Andora haven't ratify the Convention.

[5] Official gazette of RS", nr. 19/2009.

The second chapter of the Convention which includes Articles 2 - 22, is divided into several sections and includes substantive and procedural provisions. Within the substantive provisions, there are stipulated nine offenses, grouped into four categories.

The first group of alleged acts constitutes crimes against computers and computer systems in the strict sense. Convention has named this group as: Criminal offenses against the confidentiality, integrity and availability of computer data and systems.[6]

The second group of criminal acts constitute crimes classic whose execution is linked to computers as computer related acts.

The third part of the second chapter deals with the criminal acts that are related to the content of the communication on a computer network and is dedicated to the related crime so called "Child pornography", or exploitation of children (or minors) in pornography in Article 9 (Offences related to child pornography, Article 9). The States Parties shall incriminate under national legislation the following activities: production of child pornography for the purpose of distributing through its computer system; offering or making available child pornography through a computer system; distribution or sending child pornography through a computer system; procuring child pornography for oneself or for another through a computer system; possession of child pornography in a computer system or on a medium for the transmission of computer data. So, there should be criminalized any behavior related to child pornography.

The fourth segment of the second chapter is devoted to criminal offenses related to copyright and related rights in the art. 10 (Offences related to infringements of copyright and related rights, Article 10). The Convention does not devote much space to this problem, primarily because in the field of copyright and related rights there are relevant international instruments, whose scope is now extended to the execution of the alleged acts using computers and computer networks. Therefore, it criminalizes copyright infringement by the definition contained in existing international treaties.

The fifth segment of the second chapter covers the criminalization of attempt to commit, aiding and abetting of the offenses (Art. 11), the liability of legal persons (Art. 12) and prescribing penalties for offenses committed under the Convention (art. 13).

To the criminal procedure law is devoted to the second part of the second chapter of the Convention. These provisions deal with the procedural powers of government bodies in investigations of criminal offenses related to new technologies. The Convention introduces some classic instruments of investigation of criminal offenses in the new virtual environment, thus respecting the specific nature of cyberspace.[7]

In addition to the general provisions that require from the states to include in their criminal law the crimes in question, as well as other acts which are not found in the text of the Convention which may be subsumed under this group, great attention is paid to the method of collecting the data stored on computers or portable devices, and the protection of basic individual rights guaranteed by the European Convention on Human Rights and the Covenant on Human rights of the UN.[8]

[6] Offences against the confidentiality, integrity and availability of computer data and systems, Title 1, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013)

[7] Procedural part of Convention: Articles. 14-22., Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013).

[8] Article 15. Of Convention.

Procedural rules should be complied with in respect of offenses provided previously described members of the Convention, as well as other criminal acts committed by computers, computer systems and networks, as well as in finding, developing, providing and collecting clues in electronic form related to such offenses.[9]

Under the Convention, the competent national authorities shall have the authority to search and seize any computer or data storage medium on which they are or where there is suspicion that in them may be contained incriminating materials, as well as that of the provider of electronic communications they can collect data relating primarily to the use of the Internet and credit cards through which one can get information about a potential perpetrator of the offense of cybercrime (Art. 19 and 20). Also the authorities responsible for prosecuting criminal acts and perpetrators have the powers: to order or similarly obtain or achieve expeditious preservation of specified computer data, including traffic data that have been stored by means of a computer system in those cases where there is reasonable suspicion that the data subject changes or can be lost;[10] to order the surrender of certain computer data to certain persons in whose possession are included in a particular computer system or a particular medium for storing data; as well as Internet providers to hand over information about users of services related to such services, which are owned by Internet Service Provider or its *de facto* authorities; require partial disclosure of traffic data; to review (search) and seizure every computer or part of computer and data stored on them, as well as a medium for storing of computer data if there is reasonable suspicion that they could be considered as incriminating materials; as well as that from of the provider of electronic communications to collect data relating primarily to the use of the Internet and credit cards, and on the basis of which may be the name or IP address of a potential perpetrator of a crime.

Third part of Convention is dealing with international cooperation of states in combatting computer crime, and above all the manner for overwhelming practical obstacles in enforcement of national legislative solutions embodied in criminal acts which normally cross borders of national boundaries, and also include involment of individuals from different countries all over the world. Convention prescribes general principles of international cooperation in art. 23 in art. 24 general principles of extradition, art. 25 general principles on mutual legal assistance even in cases of missing of applicable international treaties (art. 27). Art. 29 and 30 deal with expedited preservance of recorded computer data on international level and expedited preservance of recorded communication traffic again on international level. Especially article 31 is dealing with accessing to recorded computer data within framework of mutual legal assistance and art. 33 and 34 cover gathering information about traffic in real time and interception of content data on international level. Article 35

[9] ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.19. 14.03.2010.

[10] Article 16 of Convention. Those data are those which were not deleted until issuing of order. This kind of measure for obtaining data can last by the Convention up until 90 days. Also there is no obligation of ISP to deliver this data to law enforcement agencies; they should obtain it by themselves. It is of importance to stress that this power is different than power of data retention. Nature of communications and contemporary forms of communicating through that channels forces creators of measures to divide forms of activities with data, because of service providers and service users, but as well law enforcement personnel. But convention just gives framework for this and it is on the parties to prescribe their own measures and measures for protecting all communication parties in communication traffic

brings, in course of expedited acting especially in cases of preserving of communication data in other states, network of 24/7 points of contact.[11] It is conceived to support the police and other authorities, as well as the contact for all information and the starting point for all requirements concerning the prosecution and investigation of cybercrimes. States are left to correct in practice existing differences through additional bilateral agreements, and to further specify the kind of cooperation for which there is a special interest. According to article 31 each State Party may request the other to carry out a specific investigation on its territory if it is necessary for the purposes of an investigation in connection with any of the offenses provided for in the Convention.

When the Extradition is about, there are situations where a State shall not be obliged to extradite a person. This is primarily the case when it comes to the lack of dual criminality, but the Convention provides an additional condition – the criminal act must be labelled as seriously in the law itself, or for its enforcement shall be punishable by a minimum sentence of one year imprisonment, except as otherwise provided in some other international agreement between states in terms that can be applied to a given situation (Art. 24). Also, among the countries that have reciprocal bilateral or multilateral extradition treaties, the Convention shall serve as the basis for extradition.

The provision concerning the establishment of 24/7 network with points in each country, which will serve as support for the police and other authorities, as well as the contact for all information and the starting point for all requirements concerning the prosecution and investigation of computer crime offenses (Article . 35).

The Convention is specific by it's, again, negative aspect, which we could be sought earlier in the text – the specificity of the slow ratification by the developed countries. Of the countries that can be called highly developed when it comes to modern technology, have ratified the only United States (2006), France, Denmark and Norway. The same hasn't been signed by Monaco, Russia (which, clearly, in August 2009, refused to join the signatories) and San Marino. On the other hand, it is interesting that within the EU, for example, Monaco, San Marino, Poland, Ireland, Liechtenstein and Sweden, although it was signed by them, they didn't ratify it. Why is this happening? Some authors[12] cite as the main reason already mentioned procedural powers of state agencies, which the Convention provides almost with no limits. Many critics point out the negative traits of the Convention, for diverse reasons.[13]

The fourth chapter contains the final provisions of the Convention. It is of special interest to countries that are not members of the Council of Europe, because it allows agreement on the implementation of the Convention approaches and states that are not in Council of Europe.

[11] This cooperation incorporates: providing of technical advices, securing and expedited preserving of traffic data and data of communication content, finding and gathering of data and traces of committed criminal act.

[12] Komlen-Nikolic, L. et all. Op. cit. p. 51.

[13] EFF (*Electronic Frontier Foundation* http://www.eff.org, 01.10.2014.) calls it the wort internet law in the whole world. More of other reasons at: Nate Anderson, *World's Worst Internet Law*, http://arstechnica.com/news.ars/post/20060804-7421.html, 01.10.2014

Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems

In 2003 there was signed the Additional Protocol to the Convention of cybercrime under title CETS nr. 189. It refers to the criminalization of acts of a racist and xenophobic nature committed through computer systems and it was entered into force on 1 March 2006. Of the countries in the region which have ratified it we could state: Albania, Bosnia and Herzegovina, Croatia, Macedonia, Romania and Montenegro while Hungary and Bulgaria are neither signed nor ratified, and, for example, Spain, Sweden and Switzerland are the only signed but not ratified.[14]

The main purpose of the adoption of the Additional Protocol relating to the criminalization of acts of a racist and xenophobic nature committed through computer systems is the incrimination of behavior not covered by the Convention, and that the spread of hatred, intolerance and bigotry toward racial, national, religious and other groups and communities, using computers as a means of communication and dissemination of propaganda. The activities in question carry a great social danger because of inability to control the availability and distribution of highly flammable contents. We are not talking about the right to publicly express their opinions, but this is a very complex phenomenon, which carries abuse on this or other rights on the Internet or another network by using a computer, where the ability to react adequate authority significantly reduced. The protocol is primarily focused on the criminalization and punishment of such incidents, regardless of whether they are spreading hatred, intolerance or historical facts represent the false way, or by any other means discriminate against or denigrate certain ethnic, racial, religious group or organization that they represent.

Authors of protocols in the preamble invoke the European Convention on Human Rights and Fundamental Freedoms, Protocol 12 to the European Convention, which prohibits any form of discrimination against individuals or groups on the basis of a protected personal characteristics, and the Convention on the Elimination of All Forms of Racial Discrimination, which was adopted in 1965 within the United Nations.

The protocol consists of four chapters:

- General provisions (art. 1-2)
- Measures to be taken at national level (Art. 3-7)
- Relations between the Convention on Cybercrime and its Additional Protocol (art. 8)
- Final provisions (Art. 9-16).

In a relatively short text, the Protocol establishes the obligation of States Parties to the national legislation criminalize the following conduct:[15]

[14] State Union of Serbia and Montenegro signed it on 07.04.2005. The list of ratifications can be found at: http://conventions.coe.int/treaty/Commun/ChercheSig.asp?NT=189&CM=&DF=&CL=ENG, 11.02.2014.

[15] Art. 3-6. Of Protocol, Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems CETS No.: 189, Convention Explanatory Report, Strasbourg, 28.I.2003 http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm> (December 20, 2013.

1) Dissemination of racist and xenophobic material through computer systems - means any act by which the material is made available to the public, using a computer or computer system. The material can be made available in a variety of ways, such as sending it to a large number of e-mail addresses or the presentation on the Internet; States are allowed the freedom to say whether this process will be introduced in criminal law (criminalized), and given the possibility of making a reservation on those behaviors that under domestic law can be considered to represent a form of expression freedom of speech.

2) The threat motivated by racism or xenophobia – represents making it inevitable to an individual or group that on them would be committed a serious crime, as defined in the domestic law of the states, by using a computer or computer system. An individual or group should be individualized according to their race, color, descent, national, ethnic or religious affiliation, to have this criminal act that it has a specific form provided by the Protocol;

3.) insult motivated by racism or xenophobia - has the same elements as the previous act, only it is not a threat, but rather insulting an individual or group based on race, colour, descent, national, ethnic or religious affiliation; State can make a reservation to this article fully, or may limit criminalization to those offenses which spreads hatred, or through which an individual, or group, is humiliated or shamed to ridicule. Probably the specificity and diversity of Internet communications with a combination of the right of exercising free expression of opinion in public has allowed to the Protocols creators to define in this way this offense.

4) Denial, reduction, approval or justification of genocide or crimes against humanity - introduces an interesting concept of punishment for the alleged acts committed via a computer or computer system if the subject cases were decisions by international tribunals. Also, this content must and alike has to be somehow made available to a larger number of people who use computers and the Internet or other computer networks.

Each Party shall adopt such legislative provisions that would previously elaborated actions qualify as a criminal offense if they are made of premeditation, aiding or incitement to commit any of these offenses.

In this section, subject to execution are the cases that were subject to decisions by international criminal courts, starting with the International Military Tribunal in 1945. in Nuremberg, through processes of Tokyo in 1946. onwards, which implies the offenses as subject to decisions of the Tribunal for war crimes in the former Yugoslavia as well as Rwanda, the International Criminal Court in Rome.

Decision on the implementation, the practices and international cooperation enshrined in the Convention shall also apply to the acts that are established by the Protocol.

Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108)

The Convention was concluded on 28 January 1981 and entered into force on 1 October 1985.[16] The main objective of the Convention was to strengthen the legal framework in the field of personal data protection, given the increase in the use of computer technology for administrative purposes (especially the introduction of e governance), and the possibilities of abuse that it brings. The issue is based on the assumption that, in modern societies, passing many decisions concerning the exercise of the rights of individuals, based on the information and data stored in computers and computer systems (data necessary for the calculation and payment of salaries, the data related to the creditworthiness of persons, social and medical care, data on the health status of individuals, etc.). It is necessary to prescribe the conditions for use of such information and that they are available to persons who meet appropriate conditions and pass required procedures and thus reduce the possibility of abuse. It is particularly interesting to look at the proposals for modernization of the Convention since the majority of EU member states have harmonized legislation according to EU directives and that in one and in another legal system has certain shortcomings. The Explaining report[17] states that the national legislation of the Member States do not provide the necessary level of protection of citizens in this area, particularly with regard to the mechanisms of effective control over citizens' personal information about them is collected and used by state agencies and other entities. This is explained by the existence of certain social responsibilities of that agencies or persons who process the data, given the power that this information carry with them and processing them separately.

The central and essential part of the convention is the second chapter in which the substantive provisions contained in the form of basic principles (such as minimum protection that must be given to the processing of personal data) concerning: 1) the quality of data collected (the pattern in the data collection, data for purposes that are permitted by law, the accuracy and timeliness of data as well as keeping in shape and form which permits identification, Article 5 of the Convention), 2) special categories of data (data on racial and political affiliation, religious beliefs, as well as data concerning health status, sexual orientation and prior convictions cannot automatically be collected and made publicly available unless the law does not provide special measures of protection in respect of the above data, Article 6 of the Convention), 3) the security of the data collected (obligation to apply appropriate security measures to thwart accidental or unauthorized destruction of data collected as well as loss, unauthorized access, modification or distribution of the automatically collected data, Article 7 of the Convention), 4) additional measures of safety for persons on whom information is collected automatically (concerning the right of access to any analysis of the collected

[16] "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", (ETS No.108, the 28 January 1981, Entry into force: 1.10.1985). Serbia signed convention and ratified on 06.09.2005 and it came in force on 01.01.2006. With this convention along came additional protocols: Additional Protocol to the Convention for the Protection of Individuals with regard to ETS no. 181. Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, из Strasbourg, 8.XI.2001. Serbia signed that protocol 02.07.2008. and ratified it 08.12.2008. it came into force on 01.04.2009.

[17] Stable internet address http://conventions.coe.int/Treaty/en/Reports/Html/108.

automatically information, the right to request deletion of illegally collected data and the right to a remedy if these requirements cannot be met, Article 8 of the Convention), 5) exceptions and limitations (rights prescribed in Articles 5, 6 and 8 of this convention may be limited only by certain law of the Member State in cases when it is necessary to in order to protect national security, public order, the monetary system of the country, the suppression of criminal offenses as and when necessary to protect persons about whom data is collected or to protect the rights and freedoms of other persons, a member of the 9th the Convention). States are obliged to provide for appropriate sanctions to effectively avert any injury or abuse the rights provided by the Convention.

The third chapter contains the provisions relating to cross-border traffic of automatically collected personal data. The essence of these provisions is to ensure the free flow of information between Member States and to ensure the absence of any special control mechanisms or the existence of the regime of permits or approvals. This solution is logical, bearing in mind that the Convention lays down the basic principles for the automatic collection of information that make up the so-called. "Common core" among member states so as there does not exist the need for additional regulation or individual restrictions in trade of personal data (except, of course, those restrictions that are established by the Convention in Article 12, paragraph 3). This common core also solved the problem and the possible application of the laws of certain states in the territories of other countries - conflict of law jurisdiction.

The fourth and fifth chapters of the Convention prescribes the mechanisms of cooperation of States Parties, in certain cases (Chapter IV – relating to cooperation between the competent bodies and assistance to persons who are resident in a Contracting State other than their own), but also in terms of issues relating the application of the Convention as such (chapter V - the consultative Council for the implementation of the provisions of the Convention.)

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (ETS201)

This is a significant international document which should lead to increased efficiency of criminal proceedings in which children are victims of sexual exploitation and abuse. Its aim is also to bring about the harmonization of national legislations with regard to substantive criminal legislation in the works in which computer technology and networks are used for the purpose of distribution, exchange and storage of illegal content.

The Convention prescribes and criminalizes certain behavior by providing guidelines to the States in the material criminal law and so Art. 18 entitled Sexual Abuse, defines the term sexual abuse and relations with coperpertrators of the criminal act regarding its sensitive nature. Article 19 criminalizes Criminal offenses related to child prostitution.

It is important to consider Article 20 of the Convention relating to crimes, "child pornography", due to fact that certain provisions directly related to (mis) use of computer technology. The said provision provides obligation to the parties to criminalize

the following illegal acts (that following types of intentional conduct, when committed unlawfully, are criminalized): production of "child pornography"; offering or making available in any other way, "child pornography"; distributing or (transfer) broadcasting "child pornography"; provision of "child pornography" for himself or for another person; possession of "child pornography"; knowingly obtaining access capabilities using information or communications technology. For the purposes of this Article, the term "child pornography" means any kind of material that visually depicts a child engaged in real or simulated sexually explicit conduct, and any display of sexual organs of a child for primarily sexual purposes. Each Party may reserve the right not to apply, in whole or in part, paragraph 1 a) and d) with regard to the production and possession of pornographic material that:

- Consists exclusively of simulated performance or non-existent realistic picture of the child;

- Include children who have reached the age determined in accordance with the application of Article 18, paragraph 2, when these were produced with the consent of and subject to the possession solely for their own private use.

Each Party may reserve the right not to apply, in whole or in part, paragraph 1 f).

It is particularly interesting to consider Article 21, which incriminates criminal offenses in connection with the participation of a child in pornographic performances:

1. Each Party shall take the necessary legislative or other measures to ensure that the following types of intentional behavior are going to be criminalized:

a) the engagement of the child to participate in pornographic performances or inducement of a child to participate in such performances;

b) forcing a child to participate in pornographic performances or income-earning or some other form of exploitation of a child for such purposes;

v) knowingly attending pornographic performances involving children.

2. Each Party may reserve the right to limit the application of paragraph 1 c) in those cases where children are involved or forced in accordance with paragraph 1 a) or b).

Based on this document, state parties are committed and will ensure that to the victims: 1) from the first contact with the competent authorities, are made available information on relevant court and administrative proceedings, consistent with their age and maturity of age and in a language they understand; 2) is accessible, free legal help, when they can have the status of parties to criminal proceedings; 3) as well as to predict the possibility for judicial officers appointed special representatives of the victims where holders of parental responsibility cannot represent a child because of a conflict of interest in relation to the child.

Article 23 provides coaxing (or abetting) of children for purposes of sexual exploitation and Article 24 provides for aiding or supporting and attempt and Article 26 stipulates the liability of legal persons. It is interesting to compare Art. 9. Convention on Cybercrime (CETS 185) and this Article. 20. CETS 201. The first main difference is in the fact that the first focuses on the criminalization of acts related to information and communication services (making materials "child pornography" for distribution through a computer system), and the Convention CETS 201. extends relations to a

given matter and covers even actions that are not related to computer networks. It includes "producing" of child pornography"" but art. 20 criminalize the act of obtaining material "child pornography" (Art. 20 (1) f. CETS 201). CETS 185 does not contain such a provision. Convention CETS 201, Art. 23. criminalize and guidance of children for purposes of sexual exploitation. Criminalization refers to the intentional offering, through information and communication channels, by adults, meeting to a person who has not turned the age of art. 18 section 2. for the purpose of committing any of the offenses envisaged in articles 18 section 1a or Art 20 section 1a against the child, in cases where such indication is accompanied by actions that lead to such a meeting. We can infer that this provision differs in relation to our offense in Criminal Code in the art. 185b titled exploiting computer network or other means of communication to commit offenses against sexual freedom of a minor, although it was changed in the year 2009 because in Serbia it is necessary that a person appears in place of the appointment for existing of this crime (grooming). In relation to the provisions of procedural nature, the Convention obliges Parties to take legislative and other measures which are necessary to give appropriately training to judges, prosecutors and other personnel involved in criminal proceedings, and to have them acquire additional skills that are necessary for dealing with the so-called "particularly vulnerable victims" or with minor victims who were subjected to sexual exploitation and abuse. It is very interesting provision on storing and preserving data on convicted perpetrators of acts "child pornography" in art. 37. These are the databases of above said perpetrators that would contain information about the identity of the person and their DNA profiles (not samples). This data storage is in accordance with the Convention ETS no. 108, of which we have already elaborated.

Convention on the Prevention of Terrorism (ETS 196)

The purpose of the Convention is to increase efforts to prevent terrorism and its negative effects on the freedoms and rights of citizens also to influence creation of the measures to be taken at national level and at international level, as well as through international cooperation. Achievement of these objectives, on the one hand, the Convention attempts to criminalize the behavior (including certain preparatory actions) that can lead to acts of terrorism (public provocation or public incitement to commit terrorist acts, recruitment and training of members of terrorist organizations). On the other hand, provides empowerment and collaboration, internally, at the level of creating a national policy for the prevention and, internationally, through a number of measures - through, when necessary, modification of existing agreements on extradition and legal assistance. Also Convention makes this through the exercise of the exchange of information, imposition of obligation to the authorities to prosecute and investigate such crimes, but the introduction of liability for legal persons (in addition to individuals) for crimes in this area: In addition to mentioned, with the imposition of obligation to proceed with the prosecution of the perpetrators of the territory of a country that has refused, in cases of refusal of extradition. It is necessary to point out that this Convention naturally leans to criminalization of an additional Protocol to the Convention on Cybercrime, CETS No. 189, specifically Art. 3 of the same.

In support of this view goes the opinion of the Committee of experts on terrorism (CODEXTER) from 10 November 2005 which was issued at the request of the Committee of Ministers concerning cyber-terrorism and the use of the Internet for the purpose of carrying out terrorist acts. In the opinion of the author highlights the issues regarding cyber-terrorism should be set in relation to the assessment of the effects of implementation of the Convention on Cybercrime. Since it was observed that most of the issues related to attacks on computer systems and networks adequately covered by the provisions of the Convention on Cybercrime, it is necessary to carry out continuous evaluation of the effects of the Convention and, if necessary, to complete the provisions with indispensable solutions that occur. As a conclusion it is stated that the focus needs to be accomplished to achieve effective and consistent application of the provisions of the Convention on the Prevention of Terrorism and Cybercrime and encouraging states to fully implement the Convention.

Before the analyzing the provisions of the Convention relating to the abuse of computer technology for the commission of terrorist acts we should point out the ways in which the Internet and computer technology in general can be used for such purposes. First of all, it is about attacks via the Internet, which can be directed in two directions, toward infrastructure and facilities on the one hand and human life on the other side. Furthermore, in addition to the attacks on the targets computer technology can be used for distribution of various facilities and the acquisition of funds that allow further terrorist activity.

For our consideration are important members 5-7 of the Convention relating to the preparation acts of such quality and character that have the potential to cause or facilitate acts of terrorism. These are public incitement to commit terrorist acts, recruitment for the commission of terrorist acts, and training of future terrorists.

The described act is possible to commit by misuse of computer technology and especially the Internet as a global network for communication and exchange of information. In such manner committed the given act can have much more powerful effects and also it carries a greater threat to society. Notable is mentioned connection with the Additional Protocol to the Convention on Cybercrime (acts of a racist and xenophobic nature), which is defined in Article 2 of racist and xenophobic material as "any written material, any image and any representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."[18]

Recruitment for the terrorism means the abetting of another person to commit a criminal act of terrorism or participate in the commission of such offense or to join an association or group, in order to contribute to the association or group commits one or more acts of terrorism. It is clear that the process of recruiting, in the way it is defined may be successfully carried out with the help of the Internet as a global network. In accordance with the provisions of the Convention, it is necessary that the recruitment carried out unlawfully and in particular Intent.[19]

[18] ETC 189.

[19] Many countries go much further in these aspirations. In Germany there are articles 89a and 91 of CC where there are criminalized acts of instruction for building explosive devices, weapons and nuclear and other radioactive materials,

Finally, the computer technology and the Internet (as well as email, discussion forums, chat or newsgroups etc.) can also be used to conduct a training for terrorism, which is defined as "the providing instructions for making or use of explosives, firearms or other weapons or harmful or hazardous substances, or for other specific methods or techniques, for the purpose of committing or contributing to the commission of a terrorist offense, knowing that the skills provided are intended to be used for this purpose."

The Convention on the Rights of the Child

By ratifying the Convention on the Rights of the Child,[20] Contracting States are, inter alia, pledged to provide to every child protection from exploitation and from performing any work that is likely to be hazardous to life or health of the child, or that constitute the violation and/or breach of its physical, emotional and sexual integrity. Ratification of the Convention on the Rights of the Child (hereinafter CRC) our country has assumed an obligation to take measures to prevent violence against children and to ensure the protection of all its forms (in the family, institutions and the broader social environment, etc.). Also, contracting parties are committed to provide measures to promote physical and psychological recovery of child victim - all forms of exploitation, and to ensure social reintegration, or provide a child's integration into a new social environment (Art. 39 CRC).

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (hereinafter referred to as the Protocol) obliges States Parties to, inter alia, adopt appropriate measures to protect the rights of the child victims of the acts prohibited by the Protocol at all stages of criminal proceedings (Art. 8), and in particular:

- through recognizing the vulnerability of child victims and adapting procedures to take account of their special needs, including their special needs as witnesses;
- by informing child victims of their rights, their role and the scope, timing and progress of the proceedings and the disposition of their cases;
- by allowing that the proceedings in which are threatened their personal interests are presented and considered the views, needs and concerns of child victims, in a manner consistent with the procedural rules of national law;
- by providing appropriate support services to child victims throughout the legal process;
- through protecting, as appropriate, the privacy and identity of child victims and taking measures in accordance with national law to avoid the inappropriate dissemination of information that could lead to the identification of child victims;

production, trafficking, storing, or facilitating to other to take possession of them, collecting, receiving in order to keep and providing access to those to other person (89a). Maintaining and establishing of the contact with terrorist organizations or their members with intention of receiving instructions for executing serious violent attacks and endangering national security (89b). Dissemination of written content through internet containing instructions and material for committing acts against state (91).

[20] *Law on ratifying of The Convention on the Rights of the Child,* "Official gazette of SFRY – International contracts", no. 15/90

- by providing, in appropriate cases, safety of child victims, as well as the safety of their families and witnesses who testify on their behalf, from intimidation and retaliation;
- through avoiding unnecessary delay of cases and the execution of orders or decrees granting compensation to child victims.

Also, in terms of the Protocol, "States Parties shall ensure that uncertainty as to the actual age of the victim shall not prevent the initiation of criminal proceedings, including investigations aimed at establishing the age of the victim. That the conduct of the criminal justice system, with children victims of unlawful acts described in the present Protocol, is in the best interest of the child and that it shall be priority for everyone involved. "States Parties shall take, as well, measures to ensure appropriate training, in particular legal and psychological training, for persons who work with victims of unlawful acts prohibited under the present Protocol and to adopt measures to protect the security and integrity of those persons and/or organizations involved in the prevention and/or protection and rehabilitation of victims of such unlawful acts.

International labour organization (ILO) Convention no. 182 on the Worst Forms of Child Labour adopted in 1999 in Geneva, along with Recommendation 190 concerning the prohibition and direct action for the abolition of the worst forms of child labour, it is also of paramount importance in this area.[21] This treaty applies to all persons younger than 18 years and obliges the parties to take immediate and effective measures to secure the prohibition and elimination of the worst forms of child labour.

[21] *Law on ratifying Convention of ILO no.182 of worst forms of child labour and ILO Recommendation no. 190 of prohibition and immediate action for the elimination of the worst forms of child labour. "Official gazette of RS – international treaties" no.08/03.*

APPLICATION OF SUBSTANTIVE CRIMINAL LAW IN THE AREA OF ICT

General remarks on substantive criminal law

The Criminal Code falls into the category of substantive regulations concerning the character of crime in relation to ICT. This law prescribes criminal offenses in this area. It is important to point out that the original offenses in the sphere of computer crime introduced in the legislative system of the Republic of Serbia amendments to the Criminal Code of the Republic of Serbia in 2003. Given that the number of incrimination in the first legal provisions that dealt with criminal offenses in this area has been very narrowly defined, the current provisions of the Criminal Code have significantly expanded their number and structure, and to a large extent they comply with the Council of Europe Convention on Cybercrime.

The Criminal Code

Etymological aspect

According to the Criminal Code provisions relating to the field of computer crime are contained primarily in the general part of the Code, in Article 112, in the part relating to the meaning of the term in the sense of criminal law. In this manner is prescribed by law what is considered to be a computer, computer data, computer network, computer program, computer viruses and computer system. So, the computer represents every electronic device on the basis of automatic processing and data exchange (paragraph 33, Article 112 of the Criminal Code). Computer data is any representation of facts, information or concepts in a form suitable for processing in a computer system, including an appropriate program based on which computer system performs its function (paragraph 17, Article 112 of the Criminal Code). As a computer network is considered to be a collection of interconnected computers or computer systems that communicate by exchanging data (paragraph 18, Article 112 of the Criminal Code). Computer program shall be considered a furnished set of commands that are used to manage the operations of the computer, as well as to solve a specific task using a computer (paragraph 19, Article 112 of the Criminal Code). A computer virus is a computer program or other set of commands entered in a computer or computer network which is made of replicating itself and is working on other programs or data to a computer or computer network by the addition of a program or a set of commands to one or more computer programs and data (paragraph 20, Article 112 of the Criminal Code). The computer system is any device or a group of interconnected or dependent devices of which one or more of them, according to a program, performs automatic processing of

data (§ 34, Article 112 of the Criminal Code). This represents part of the definition of certain terms used in the Criminal Code and their significance in terms of the provisions of the Code, which are related to the field of computer crime.

Offences against the Confidentiality, Integrity, and Availability of Computer Data and Systems

This group of offenses is a direct result of the implementation of the Convention on Cybercrime – CETS 185. Prescribing criminal act under title: Unlawful acts with the data (displacement and disruption of data and system interference)[22] on the computer, the CETS 185 provides it in terms of intentional partial or total damage, deletion, destruction, changes content, or compression[23] of the original data(art. 4). This act may at first glance look like an illegal approach, but must be understood primarily as a complement to him: illegal access to (in order to modify the data) to the commission of the offense. The procedures described in Part illegal access, such as "Trojan horses" and "logic bombs," as the ultimate goal have unauthorized treatment of data on your computer, which includes sending them to the author of the malware or a third party - purchaser (for further abuse, the most common to create zombie computers even, networks of the same). It should be noted that this does not incriminate damage and deletion of data, such as, for example, virus damage, but to the traditional forms of manipulation are added acts that lead to similar consequences. An example is the provision of data – if the virus randomly changes the contents of the document the damage can be compared to deleting files.

The act of data changes is linked to intrusion into a computer network or system, which is defined as the intentional, serious and unauthorized manipulation of computer system input, transmission, damaging, deleting, destroying, changing or compressing computer data. The act incriminates blanket provision, citing a series of actions, covering every situation that implies disabling operation or modification of computer systems or networks. It is understood that in this act is included the physical server shutdown, as well as DoS (Denial of Service attack, this refers to a corresponding computer network for illegal intrusion into its data) and virus. The intent is necessary and must be included unauthorized computer network or system to make this act existing. In the case of this act perpetrators in order to increase the amplification consequences are increasingly applying botnets, large groups of infected zombie computers that have had a strong attack on the computer.

CETS 185 prescribes Illegal access (hacking) (Art. 2) information contained in a computer or computer system, in order to seize the information, change it or destroy.[24] For this Act, therefore, is needed intention, so that the signatory states can have the option to criminalize only the specific actions that lead to illegal access to a computer or network. A typical example of such work is the insertion of "Trojans" into someone's computer.

[22] This criminal act is covered in Serbian law system by art. 298, 299, 301, 302, CC of RS.

[23] In Internet related identity theft, A discussion paper, Prepared by Marco Gercke, www.coe.int/cybercrime it is determined as act which negatively influences on accessibility of data to wider circle of people who have access to media on which it was stored

[24] More criminal acts cover this in CC RS: article 298, article 299. article 300.

Illegal access without authority, often, is the first act of a combination of actions (as elements of complex crimes), for example, phishing[25] or identity theft. The Convention does not incriminate the method in which this act will be realized, but remains neutral in terms of technology used, and the basic requirement is premeditation and unauthorised access.

Specific crimes, prescribed by the statutory criminal law, are primarily those relating to the security of computer data. The Criminal Code prescribed those in Chapter XXVII (Articles 298-304a).

Damage to computer data and programs (Article 298 CC)

This criminal offense has the basic two serious forms. The basic form consists in the unauthorized deletion, modification, damage, concealment, or otherwise suppression of computer data or programs. The act therefore can only be done in relation to computer data or programs, and with more alternative activities planned, with the aim of fully or partially disabling the use of computer data or programs. For this offense is punishable by a fine or imprisonment up to one year. The first serious form of this act if there is an action taken which has caused damage in excess of four hundred and fifty thousand dinars. Amount of damage caused represent the qualifying circumstances for which is prescribed a punishment of imprisonment of three months to three years. The most severe form of the offense for which is prescribed a punishment of imprisonment of three months to five years, if there is an action taken which has caused damage in excess of one million five hundred thousand dinars. Tools used in committing this offense shall be confiscated if they are in the property of the offender. The intention of the legislator was that by the prescribing of this crime protect the integrity of these components in computer technology against unauthorized operation.

As can be seen, the offense can be done alternatively in several ways: 1) by deleting, or 2) changing, so that a computer program or data is completely destroyed or changed to become useless to continue the execution of intended function, or 3 .) damaging, by which program or data are partially destroyed and reduced its use value, or 4) concealing, when it comes to concealing of a computer program or data, and the act can be done in any other way that makes the program unusable for its purpose.[26] It is important to understand that under other modes of making it unusable of means and making unavailable, so in this way incriminate cases the functioning of various backdoor or trojan programs which are specific programs on the computer disguise, as preparatory work for, say, computer extortion.

The implication of this act is to make useless programs or data. The act is done by taking any of these actions to the achievement of prescribed outcomes. If more action is taken towards an object, or a computer program or data, it will be realized only one offense. The perpetrator of this section may be any person, in respect of culpability required intent. For proper qualification of the criminal offense,

[25] Definition can be found at: http://www.coe.int/t/dghl/cooperation/lisbonnetwork/meetings/Bureau/TrainingManualJudges_ en.pdf

[26] Ljubisa Lazarević, „Komentar Krivičnog zakonika Republike Srbije“, Savremena administracija, Beograd, 2006, p. 745.

it is necessary to determine whether the perpetrator acted without authorization, the exact time and place of the offense, the manner in which the offense was committed – whether in terms of physical access to the computer program or data, or the offense is committed within the computer network internally or via the Internet, and, if made by another computer, with the help of the programs, as well as the consequences that have occurred, or if the object of criminal act has been made unusable. It is necessary to identify and attribute the offender, or whether it is official or responsible person within a legal person, or a person who was on the basis of a law regulated relations in power to any set way manipulate a computer program or data, to update or change it.

For proper qualification work it is necessary to establish several important facts. First of all, it is necessary to determine the real offender, or whether the perpetrator acted without authorization or been authorized to take certain action, then the exact time and place of commission of the offense, the manner in which the offense was committed (internal or external attack) and within that to whether the offender used certain equipment (and which) during the commission of the offense, the nature and severity of consequence, and so on.

The most common form of execution of this act is the demolition of websites, which is an everyday activity of hacker groups. According to the unwritten rules of hacking, the object of attack is only part of the site, usually the title page, which is being changed so that it leaves the hacker group signature, message or greeting, but in addition to blocking accesses other site content. From this kind of attacks from are not protected sites of educational institutions, Ministries, Parliament, Serbian Orthodox Church, etc.. Attacks on websites are taking place continuously, but to the public eye come only those attacks that were successful.

Computer sabotage (Article 299 CC)

The offense does a person who enters, destroys, deletes, modifies, damages, conceals or otherwise renders unusable computer data or program or destroys or damages a computer or other device for electronic processing and transmission of data with the intent to prevent or significantly hinders the process of electronic and data that are important for public authorities, public services, institutions, companies or other entities. From the legal definition can be seen that there are two objects of attack. First, it's a computer program or data, while the second object of the attack is a computer or other device for electronic processing and transmission of data. By performing this crime are damaged state agencies, public authorities, institutions, companies and other entities, and law prescribes a prison sentence of six months to five years.

With regard to the prescribing of this offense protects computer technology intended for electronic processing and transmission of data that are important for public authorities, public services, institutions, companies or other entities that crime will not exist if it was made towards the computers that are not relevant to these subjects. It is important to distinguish this act from the previously explained criminal offense Damage to computer data and programs. Although the actions of these two acts are very similar, there are a number of specific features that must be observed when qualifying

offense in particular, with of course a far greater consequences in the case of the crime of computer sabotage.

The perpetrator of this section may be any person, in respect of culpability required intent. The main feature of the act is the intention of the offender by taking actions that prevent or hinder the electronic processing and transmission of data relating to the aforementioned. It is important to determine whether it caused the damage - the destruction of or damage to computer data or programs, by taking some of the alleged actions and the consequences if not performed, it is necessary to identify all the foregoing for the purpose of later prosecution, given that it is possible that the consequences manifest and later in the work of these devices.

As with previous criminal offenses, for the proper qualification of this act is necessary to establish several important facts: the attributes of the offender, then the exact time and place of commission of the offense, the manner in which the offense was committed (internal or external attack) and in part on whether the offender used certain equipment (and which one) during the execution of the work, the type and severity of the consequences, and so on.

Creating and inserting computer viruses (Article 300 CC)

The offense has a basic and a more severe form. The basic form does a person who makes a computer virus with intention of inserting it into someone else's computer or computer network. The act is done therefore torque making this virus with the intent to be inserted in someone else's computer or computer system, regardless of whether such intention was realized in this case. In this sense, the question is whether it is necessary to provide a source code or it can be taken as a basis on which to create new forms of viruses with modifications that may be made by any person. We think that it is already by creating a base, which in itself is not malicious it has provided opportunity for further work towards the creation of the virus, given that on the Internet there are a lot of DIY videos. This provides both a means and an opportunity for the exercise of this act. For this form there is prescribed a fine or imprisonment up to six months. A severe form of the work does a person who enters a computer virus into someone else's computer or computer network, thereby causing damage. For this type of legislator foresaw a fine or imprisonment up to two years. A device and a means to make the forms of this offense shall be seized.

Criminal Code in Article 112, paragraph 20 defines the meaning of the term computer virus. There were several reports against unknown perpetrators due to insertion of the virus, and police and prosecutors are working to discover their identity. In comparative practice so far has been more action against persons who have created and spread computer viruses. Thus, in 2005 in the German city of Verdun eighteen-year-old hacker was sentenced to a suspended term of imprisonment of 21 months, because he wrote and left the network Sasser worm, which in 2004 for only a week of existence has infected nearly 20 million computers around the world.

The fact that the case law in relation to this offense does not exist in any case does not mean that this type of activity does not exist on the territory of Serbia. On the

contrary, it becomes clear that in this area there is a dark figure committed criminal acts, which directly indicates insufficiently developed awareness of the general public as well as scientists and experts in this field.

Other Computer Related Offences

Computer Related Forgery (Article 301 CC)

Computer forgery provided by CETS 185 applies only to intentional, unauthorized insertion, modification, deletion or hiding of computer data, which as a result has change of the data content, regardless of whether they are on the way to get a different purpose and meaning, or become unusable, and with the intention that such data could be later used as the authentic in legal traffic. States are given the option to provide for a special type of intent to commit fraud in order to have this crime.

The subject of computer counterfeiting, as the object of attack, are only data and the Convention requires that, in terms of intentional part (*Mens rea*) of offenses where data elements are concerned, include two categories of documents: public and private documents. Forgery is defined as the intentional, unauthorized insertion, deletion, alteration, or concealment of computer data, as well as any other interference with the operation of a computer system, in order to obtain an unlawful material benefit for himself or a third person.

In the criminal law of the Republic of Serbia Article 301 is titled computer fraud. The act has a basic, two serious and one particular form. The basic form of the act does a person enters incorrect data, omissions entering correct data or otherwise conceals or falsely presents information and thus affect the result of electronic processing and transmission of data in order to obtain for him(her)self or another person unlawful material gain for the second time and causes property damage. The offense is done at the time the enforcement action was taken with the intent to obtain for him (her)self or another unlawful material gain or to cause another kind of property damage. For the basic form of act law has prescribed fine or imprisonment up to three years. There are two serious forms of act, depending on the amount of the illegal gain. The first serious form exists when there is an acquisition of a property in the amount of four hundred fifty thousand dinars, and it is punishable by imprisonment of one to eight years. Another serious form exists when there is a material gain exceeding one million five hundred thousand, and it is punishable by imprisonment of two to ten years. A special privileged form of this criminal act exists there when the action execution take only the intention to damage the other person. For this form law says that it is punishable by a fine or imprisonment up to six months.

The offense of computer fraud should be distinguished from criminal charges of fraud (Article 208 of the Criminal Code) and insurance fraud (Article 208a CC both belong to the group of offenses against property Title XXI of the Criminal Code). These two types of fraud can be performed using computer technology, provided that in such circumstances, both offenses are fundamentally different from computer fraud. So, Fraud does a person with intent to obtain for himself or another unlawful material

benefit brought by false representation or concealment of facts in a misleading or maintain other person in error and thereby instigate to to do or not do something that could damage his or her or someone else's property, while insurance fraud does the person who with intent to obtain for himself or another unlawful material benefit brought by false representation or concealment of facts, opinions and giving false statements, submitting a false judgment, submitting false documents or otherwise mislead or maintain in error somebody in connection with insurance and thus it instigate this person to do or not do something to detriment of his (or her) own or someone else's property.

The intention of the legislator was that prescribing a criminal offense Computer fraud protects the credibility and integrity of the data being electronically processed or transmitted electronically. It is necessary to determine in each particular case and the intent of the perpetrator, which consists in the fact that, for him (her) or for other illicit material benefit, and thereby cause other property damage.

Since the action of the offense is defined alternatively as entering incorrect data or omission in entering correct data or any other concealment or misrepresentation of data, offense is done when taken some of mentioned actions, with the existence of the described intentions and when there has been caused property damage, where it is not necessarily due to the actions taken to have illegally obtained gains. This offense may be committed premeditated by any person who undertakes legally prescribed action.

For proper qualification of the crime and its successful proving it is necessary to determine the time and place of the offense, the exact action that was taken, and the manner in which incorrect data is entered. About the entered data it is necessary to determine their untruthfulness, what is the falsity in real and how did it influence to the result of electronic processing and transmission of data, then if it is a failure of accurate input data,[27] how it is omitted, or in any other way is concealed or falsely displayed data, and to influence the result of the processing and transmission. It is necessary to determine and whether the data entered via physical access to the device eligible for transfer or electronic data processing or is it done through a network, what is the amount of material gain to be included in the intent of the perpetrator and then, what is the amount of damage. To prove the offenses referred to in paragraph 4, it is necessary to determine the type of damage that was included in the intention, whether such damages has occurred, it is necessary to determine the means by which the crime was committed and, if possible, make their seizure.

In recent years, electronic commerce becomes the dominant way of doing business in Serbia. The business segment transactions are carried out electronically and that opens up many possibilities for abuses by which may be affected all economic actors if there isn't effective protection of the integrity and authenticity of electronic data during their processing.

In previous domestic case law, there were several cases of prosecution of perpetrators of this crime, and the examples given show that computer fraud is becoming increasingly common crime. Thus, the Office of Cyber Crime launched an investigation against the suspect T. A for reasonable suspicion that during 2007 and 2008 on two occasions he was through using computer systems entered into bank systems in

[27] In that case criminal act is done through omissive action and that omission has to be in course of omission of impute for such important data, or data which can cause some negative result for electronic procession of data.

Australia and Switzerland, and issued false orders for the transfer of funds, which were in the amount of 51,990 CHF, and tried from a Swiss bank without authorization to transfer funds in the amount of 19,000 USD.

Since Serbia has a large number of sports betting, which have a wide network of branches and whose business is inconceivable without computer networks often it is the abuse of such systems. Perpetrators are in different ways trying to influence the outcome of the electronic data processing and using given software solutions, forge played ticket.

Unauthorized access to a protected computer, computer network and electronic data processing (Article 302 of the Criminal Code)

Through the act of unlawful interception of communications, the Convention FTC is trying to leverage the treatment of electronic communication with telephone communications and, in this way, introduces criminalization of electronic communications interception. Issue at stake is the unauthorized interception of personal data (Convention speaks of non-public) transmitted between two computer systems, data communications, in content, but also on traffic,[28] including electromagnetic emissions from a computer that carries this information (article 3). Public data transmission and other ways of obtaining such data are absent from these charges. The non-public communication according to the explanatory report on the Convention[29] includes those situations where the nature of the process of transmission is confidential. Private individual communication (such as sending and receiving e-mail or download from Internet sites) can generally be considered non-public. The Convention gives countries the option thus to define criminal act with obligatory requirements of an intention. As in the previous case, this fact is important primarily because of the possibility that someone without their knowledge, or at least without any intention, came into the possession of someone else's data on a computer network. The objective is to protect the integrity of non-public communication.

It is important to note that the application of this work is very limited because the criminalization is focused on intercepting the transfer process, and thus cannot be extended to the moment when the person who intercepts transfer the same data stores on some kind of medium. Incriminated is only the process of interception of data transmission and not preservation. Example for interception give us "key loggers" and " screen loggers". A special problem exists in cases where the interception of data is not performed by technical means – because this work can be defined as any form of obtaining data in the process of transfer, but article 3. does not cover acts of social engineering, and, therefore, this act cannot be when accomplished counted as criminal act covered by art. 3.

The criminal act has a basic and two serious forms. The basic form does person who in violation of the protection measures, unauthorized breaks into computer or computer network, or establishes unauthorized access to electronic data processing.

[28] Stable internet address http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.16.
[29] Explanatory report nr.60.

The plot of this act is committed without authorization, in violation of planned security measures. For this form is punishable by a fine or imprisonment up to six months. The first severe form, which is punishable by a fine or imprisonment up to two years, does the person who records or uses data obtained in the through commitment of basic form. The most severe form of act exists if due to actions taken while committing basic form is caused an impasse or serious disruption of electronic processing functioning and transmission of data, or network or other serious consequences have occurred. For this form of offense perpetrators are punishable by imprisonment of up to three years.

Through prescribing of this offense shall be protected computers, computer networks and data to be processed electronically.

The criminal act (*actus reus*) of this crime consists in the unauthorized accessing into computer/computer network or unauthorized access to electronic data processing or use of data obtained in these ways. This offense may be committed by any person who possesses specific expertise, given that it is a protective barrier to overcome before the accessing to a computer or computer network. The perpetrator of the criminal act undertakes act of committing with the intent, which covers unauthorized accessing a computer or computer network, using data obtained in the above manner and the possible occurrence of consequences set out in paragraph 3 of Article 302 of the Criminal Code.

The perpetrator of the offense referred to in paragraph 2, may be the person who committed the offense specified in paragraph 1, but it could be any other person who has come into possession of data. If an individual has taken the actions specified in paragraphs. 1 and 2, then there is criminal liability of such person only to paragraph 2, considering that the action referred to in paragraph 1 are only preparatory work. Perpetrator of the act referred to in paragraph 1 may only be a person who is not authorized to engage in computer or electronic data processing approaches.

In order to properly qualify a criminal offense, it is necessary to determine the time and place of the offense; authority of the perpetrator, if it comes to offense from paragraph 1.; the way they overcome barriers, as well as the way in which access to a computer or computer network; then, for what purposes the data were collected, and in particular, what constitutes the most serious consequences, if it is performed (if it has stopped or serious disruption of functioning electronic processing and transmission of data, or network or other serious consequences).

Object of protection of this crime are protected computer or computer network or data that are processed electronically. The consequence of the offense is the unauthorized intrusion or access to, or use of the data thus obtained. It is necessary that the perpetrator with no awareness that unauthorized uses – involves a breach in computer security measures, or unauthorized access to EOP. If the owner specifically protect this connection, each device and program used to make this kind of connection by the person who controls it is assumed that it participates in the commission of the offense. If we do not secure access to it (computer or a network) a consequence of the offense exists, then it is a criminal act prescribed in art. 304 of the Criminal Code of RS. (or is it subject only to private suits).

In each case it is necessary to accurately determine what measures of protection are violated and how, which is the important feature of this offense. A separate issue

is the question of obtaining information (user names and codes) for the execution of this crime, as well as their re-sell and offer for sale. These acts are not criminalized as a separate criminal offense, and may represent a specific form of identity theft. It can be subject of article 225 of CC. Special attention must turn to the determination of the existence and consequences of its weight because of it depends on the qualification of the work.

Criminal offense of unauthorized access to a protected computer, computer network and electronic data processing may be similar criminal offense Espionage (Article 315 CC, Chapter XXVIII – Criminal acts against the constitutional order and security of the Republic of Serbia), if the perpetrator breaking into computer systems came to secret military , economic or official information or documents. Secret are those military, economic or official information or documents which by law, regulation or other decision of the competent authority based on the law declared to be secret, and whose disclosure would cause or might cause adverse effects to the security, defence or for political, military or economic interests of the country (paragraph 6, Article 315 of the Criminal Code). Therefore, it is important in each case to determine the intention of the offender, the importance of the attacked computers/computer networks, especially the type of data in relation to the collection of which there is no intent of the perpetrator.

Preventing and limiting public access to the computer network (Article 303 of the Criminal Code)

The act has a base and a more severe form. The basic form of the work for which is punishable by a fine or imprisonment up to one year, does a person who makes an unauthorized preventing or hinders access to a public computer network. If the same act is committed by an official in the discharge of his duty, it is a more severe offense for which a punishment of imprisonment could be of up to three years. In the second case, it is actually a special form of the offense of abuse of powers by public officials which prevents or interferes with another individual or legal entity unimpeded access and use the public computer network.

Criminal Code in Article 112, paragraph 18 defines the meaning of the term computer network. The legislature prescribing this part of protecting public computer network accessible to all persons, and that citizen's use every day as part of various business and private activities.

This offense may be committed by any person who undertakes enforcement action which was premeditated. The condition is that the perpetrator must act without authorization, because crime does not exist unless there is a legal basis for preventing a person to access a public computer network.

The plot of the offense is determined alternatively, respectively, the offense will be taken if any activity that prevents (completely disable) or hinders (confuses) access to a public computer network, or if the above activities are carried out by public officials.

In order to properly qualify a criminal offense, it is necessary to establish a network feature (if it comes to a public computer network, available for everyone to

access or not); whether the offender acted without authorization, or is the prevention/obstruction of access to a public computer network carried out on some kind of legal basis; time and place of the offense, and so on.

To prove the criminal offense referred to in paragraph 2, it is necessary to establish status of a certain public official of the perpetrator and the committed action. In practice, it is necessary to pay attention to whether the alleged offense was committed in the function of some other offense or is accompanied by even an act which by its elements of a being of another criminal offense, in which case we can have question of their mutual relations and connections.

One of the most common ways to prevent or restrict access to a public computer network is the DoS attack and its specific manifestations called DDoS (Distributed DoS). To this type of attack are exposed all the information systems in the world, with respect to the above program performs detection of unprotected or inadequately protected computer, so there is no space of our country which has been spared the adverse effects of this form of cybercrime. A particularly dangerous type represents PDOS attacks (Permanent denial of service) that can permanently damage the hardware on servers with remote access. The attack is based on the use of "firmware system update" that server sends over a network or the Internet, and who is able to trick the hardware and flash any part of the system, which could lead to permanent and complete hardware fails.

During 2008, in Serbia were more DDoS attacks. We will single out examples of attacks on the websites of the Serbian Orthodox Church, which is considered one of the fiercest attacks ever rendered, as well as knockdown of Internet presentations radio show "Hourglass".

DoS and DDoS attacks are very dangerous and usually lead to serious financial losses for companies, institutions or agencies whose system were attacked. It is true that the identity of the perpetrators is almost impossible to establish, since the attacks carried out with infected computers that are connected to the botnet networks, whose owners in most cases and are unaware of what is going on with their computer, especially since attackers still changing and faking IP addresses from which attacks suggest. We are aware that in the territory of Serbia there is a vast number of undetected cases in relation to those registered and that the cyber space in the domain of every state, including Serbia is exposed to this type of attack. All of this should be an additional incentive for further investment of resources and efforts to mitigate the effects of the consequences that may occur.

Unauthorized use of a computer or computer network (Article 304 of the Criminal Code)

CETS 185 provides for the criminalization of the misuse of the device. The severity of the occurrence of various high-tech devices that allow the realization of abuses by diverse users of this kind of technology devices becomes subject to these charges. Performing various offenses which carry very vicious and insidious ways of inflicting the consequences to victims or to damage persons as a mandatory part of

offenses is facilitated through such devices. Here lies the *ratio* for incriminating of this criminal offense. States - Parties are undertaking obligation (article 6 of Convention) to punish any intentional illegal manufacture, sale, possession, lending, obtaining, distribution and any other way of making available to unauthorized persons any "device", this includes computer programs (designed or adapted primarily for the purpose of committing any offenses referred to in Art. 2 of the Convention), computer passwords, access codes, and any other similar form of data with by which is possible to do the offenses set forth in Articles of the Convention (2-5).

Thus defined problems in the Convention are very cleverly packaged as a combination of constraints on the devices, which as the main purpose have execution of criminal act, with the combination of the mental element of "the existence of intent to use the same for the commission of acts referred to in article 2-5 of the Convention."

The criminal act does an unauthorized person who uses a computer or computer network with intent to obtain for him (her) self or another unlawful material gain. This criminal offense is specific in that it is the prosecution of the offender is initiated by private citizens, and the law prescribes it punishable by a fine or imprisonment of up to three months.

The perpetrator of this crime can be any person who acts with direct intent. The plot of the offense consists in the unauthorized use of a computer or computer network, where the intent of the perpetrator is aimed at obtaining (for him/her or another) illegal profit.

However, in the case of this criminal act authorized officers are required to take actions within its jurisdiction and to gather the necessary evidence, if there are grounds to suspect that, in connection with the acts that fall into this crime was committed with (or as a part of) any other criminal offense for which prosecution is done *ex officio*, in which case are applied the powers and provisions relating to the filing of criminal charges.

To the commission of offenses in this area benefits the fact that awareness of the dangers that can come from the Internet still isn't sufficiently developed. Citizens often leave detailed personal information or data related to the business segment on various Internet sites, unaware of the possibilities that these data may become subject to abuse at any time. Number of crimes like this is growing daily.[30] As for the detection and prosecution of these crimes and their perpetrators, there is a big dark figure, which tells us that a very small percentage of the criminal acts are discovered and understood.

Producing, obtaining or providing to the other means to commit offenses against the security of computer data (Article 304 CC)

The criminal act is done by a person who possesses purchases, sells or gives to another the computers, computer systems, computer data and programs for execution

[30] Compare with the results published in Žarković, M. Drakulić, M. Miladinović, S. Urošević, V. Batrićević, A, Lukić V. Ivanović, Z. Drakulić, R. Jovanović, S. Janković, Đurašković, M. Stojičić, S. Milanović, L. *Veze Cyber kriminala sa iregularnom migracijom i trgovinom ljudima*, (there is a English version of this book and two cd of bilingual character) Ministarstvo unutrašnjih poslova, Urednik Vladimir Urošević, 2014.

of all previously analyzed offenses from the Chapter XVII of the Criminal Code. Items that are used for this act are subtracted, and the offenses are punishable by imprisonment of six months to three years. It also stipulates that the prosecution of this act is undertaken by a private complaint.

Offender can be any person acting willfully with intent to supply, sell or give to other for use computers, computer systems, computer data and programs in order to commit offenses against the security of computer data. If it comes to creating of these elements of information systems, we can see that it is necessary that a particular person as perpetrator possesses professional knowledge and thereby act with the intent to commit the crimes alleged.

The plot of the offense is determined alternatively, that person may: 1) possess or 2) manufacture or 3) obtain or 4) sell or 5) to give to the other for use computers, computer systems, computer data and programs to commit criminal acts from Chapter XVII of the CC. From of the this crime qualifications we can infer that it shows that only the possession, production, supplying, selling or giving to another, is in itself a criminal offense, regardless of whether there was a crime against the security of computer data. In this segment, it is important that there is an intention to commit the alleged crimes. In line with this, it is particularly important to determine the intent of the perpetrator of the crime, as well as his status and the circumstances under which he acted, then the type and content of computer data, programs and systems, the reasons for their possession (especially if they are harmful), the time and circumstances of making , acquisition, sale or delivery of the second and other essential information needed to determine the motives of actions and whether in this case there was any commitment the crime, and the criminal liability of the offender. Items that are used for this act must be seized.

Content-Related Offences

To display, acquisition and possession of pornographic material and a minor for pornography (Article 185 CC)

CETS 185 as a criminal offense "child pornography" (politically and ethically more correct term is material that depicts child abuse or exploitation of minors in pornography) criminalizes: a. production of "child pornography" (materials that exploit minors for pornographic purposes) for intended distributing through a computer system;

b. offering or otherwise making available "child pornography" through a computer system;

v. distribution or broadcasting of "child pornography" through a computer system;

g. obtaining of "child pornography" to self or others, through a computer system;

d. possession of "child pornography" on a computer system or on a medium for the transmission of computer data.

CETS 185 aims to assist the harmonization of the legal systems of the Member States and to influence that all members understand the seriousness of this phenomenon.

The Convention also contains some provisions that are broader than any comparable solutions in national legislation. Thus, the age limit which persons are considered children set to 18 years, with the possibility that the state, by making a reservation on this Article of the Convention, the same cuts at 16 years of age. Then, criminalized the activities in which within content appear persons for whom we can reasonably be assumed that they are younger than 18 years, or who present themselves as such, as well as other graphical content (drawings, cartoons etc.) That can represent a person under the age of prescribed limits in a pornographic context. The Convention leaves the possibility of a reservation for each member state, and for this we can say that it is very innovative.

In Serbian legislation this crime belongs to Chapter XVIII of the Criminal Code – Criminal offenses against sexual freedom. The offense does a person who, to a minor: sells shows or publicly displays or otherwise makes available any text, pictures, audio-visual or other objects of pornographic content or shows pornographic show. Person shall be punished by a fine or imprisonment up to six months (paragraph 1 of Article 185 of the Criminal Code). If someone uses a minor to produce pictures, audio-visual or other objects of pornographic content or for pornographic performance, shall be punished with imprisonment from six months to five years (paragraph 2 of Article 185 of the Criminal Code). If the offense referred to in paragraphs 1 and 2 of this Article is committed against a child (younger than 14 years of age), the offender shall be punished for the offense specified in paragraph 1 by imprisonment of six months up to three years, and for the offense referred to in paragraph 2 by imprisonment of one to eight years. Whoever obtains for him(her)self or another, possesses, sells, shows, publicly exhibits or in electronic or otherwise makes available pictures, audio-visual or other objects of pornographic content resulting from exploitation of a minor, shall be punished with imprisonment of three months to three years (paragraph 4 Article 185 of the Criminal Code). Items that are used for this work shall be seized.

By prescribing this act the legislator intended to protect the physical, mental and sexual integrity of children. In Article 112 of the CC defines the concepts relevant to the analysis of this crime. So, a child is a person below the age of fourteen years (paragraph 8). A minor is a person who has attained the age of fourteen up to the eighteen years of age (Section 9). Minor is a person who has not attained the age of eighteen (paragraph 10). In this segment, the Code contains an important omission, since it provides no definition of pornography. The distribution of pornographic material to the eighteenth century was not criminalized. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse in the art. 20 provides a definition and it is a part of our law system because of its ratification.

It is governed by a number of alternative actions to commit the offense referred to in paragraph 1. The act can be carried out against the juvenile or the child, and to sell, display, publicly exhibits or making available in any other way, texts, images, audio-visual or other objects of pornographic or displaying pornographic performances. Offender acts with intent.

The act referred to in paragraph 2 consists in the exploitation of juvenile or child to produce pictures, audio-visual or other objects of pornographic content or for pornographic performance, including abuse of a minor or child, often not even aware of

this situation or consequences. In terms of culpability of the offender it is required that he or she was acting with intent.

The thing that is specific for the offense determined in paragraph 1 and paragraph 2 is that they can be committed against the juvenile or the child, which is a novelty in comparison to the previous legislation. If any of the actions performed against a child, the legislator has foreseen as severe form of this act and with more severe punishment.

In paragraph 4, as part of act are prescribed the following activities: obtaining for self or another person, possession, sale, display, publicly display, as well as electronically or otherwise making available images, audio-visual or other objects of pornographic content generated by exploiting a minor. Another novelty is the inclusion in the act of committing the two essential activities, such as obtaining for self or another person and possession of said material. In previous legal solutions, these forms were not included in the concept of the offense, which was a significant omission given that the different ways of obtaining, especially online downloads of such material at the same time makes it available for other users. The same can be said for mere possession, which in many ways may become available to a wider range of people. The term of the object of attack in this form is the part of a minor, which means that it can only be a person who has not attained the age of eighteen years. In terms of culpability of the offender, and in this form of work is required intent.

It is important to emphasize the fact that in the case of this offense comes to minors, which require special attention in treatment, taking into account their age, specifically psychophysical state and the process of development and maturation, whether it comes as a juvenile offender or such person as a witness or damaged. Another problem can arise in cases that would be paradox, in which the perpetrators and victims are minors who are in a relationship, due to, specific, low motives. Particularly interesting is the case of so-called. sexting. In such cases, account must be taken of the purpose of punishing such conduct as resocialization terms of initiating legal proceedings and imposing sanctions to two minors with all implications to their personalities. It is within the framework of solving the crimes that have connotations present in this criminal act where is of great importance international police cooperation. We will see that the recent increase in collaborative activities in these crime areas.

Sexual exploitation of children does not constitute an ordinary crime, but serious violation of fundamental human rights and freedoms from the application of physical and psychological violence as the main methods of criminals disrupting harmonious and undisturbed growth and development of personality, because the victims are helpless and thus easily subject to various forms of psychological manipulation. Combating "child pornography" on the Internet is a major challenge for the police and the judiciary, especially in transitional countries such as Serbia, because criminals are constantly perfecting ways of committing the offense in order to further develop-spec, providing faster and easier access to pornographic content, with the greatest possible anonymity of clients.

From the results shown it can be concluded that the various forms of abuse of children and minors in the area of "child pornography" can be found in all countries, and this is one of the most common forms of misuse of computer technology for

such purposes. In addition to repressive measures, provided for in Article 185 of the Criminal Code, a social response should primarily be focused on preventive activities, because this segment requires high quality education of children, juveniles and adults about safe use of the Internet, prompt notification of all phenomena of positive and negative connotations in this sphere, exploring the threats posed to the Internet, especially to the parents whose children have access to a global computer network, and adequate social attitudes to criminal behaviour in this area.

As far as the labour process and the method of the persons whose victims are minors and children it has its peculiarities. Judicial council chaired by a judge who has acquired special knowledge in the field of child rights and criminal protection of minors, adult perpetrators stand trial following criminal offenses prescribed by the Criminal Code, if the injured party in criminal proceedings is a minor: Display of pornographic material and abusing children for pornography (Article 185).[31] The public prosecutor who has acquired special knowledge in the field of child rights and criminal protection of minors initiates proceedings against adult perpetrators of other criminal offenses prescribed by the Criminal Code, in accordance with the provisions of this part of the law, if it deems it necessary to specially protect the juveniles as victims in criminal Procedure Code. The criminal proceeding against the accused for offenses described is carried out under the provisions of the Code of Criminal Procedure. The investigation conducted investigating judge who has gained expertise in the area of child rights and criminal protection of minors. In the investigation of criminal offenses against underage persons participates specialist officers of the Interior, who have acquired special knowledge in the field of child rights and criminal protection of minors when certain actions are entrusted to these agencies.

When conducting the trial for crimes committed against minors, the public prosecutor, the investigating judge and the judges in judicial council will treat the injured taking into account their age, personality traits, education and living circumstances, especially trying to avoid the potential adverse consequences proceedings on his or her personality and development. Hearing of minors shall be conducted with the help of a psychologist, counsellor or other professional.

If the witness is examined as a minor who is injured or damaged by the criminal act referred to in Article 150 of the law, the test may be carried out twice, and exceptionally repeatedly if necessary to achieve the purpose of the criminal proceedings. In the case of a minor examines more than two times, the judge is obliged to pay special care to protect the personality and development of minors.

If, due to the characteristics of the offense and the personality traits of a minor, deems it necessary, the judge will order that the minor is heard using technical means for transferring image and sound, and a hearing to be conducted without the presence of the parties and other participants in the proceedings, in room where the witness is located, so that the parties and persons entitled to receive them, ask questions through the judge, psychologist, counsellor, social worker or other professional advice.

[31] Beside this criminal act there are more crimes in this group: aggravated murder (article 114), instigation to suicide and helping in committing suicide (article 119) aggravated injury (article 121); Kidnapping (article 134); Rape (article 178); sexual intercourse with a helpless person (article 179); sexual intercourse with a child (члан 180); sexual intercourse with a abuse of power (article 181); Forbidden sexual acts (article 182); Pimping and facilitating of sexual intercourse (article 183); and others.

Minors as witnesses-damaged may be questioned also in his or her apartment or room, or an authorized institution-organization, and qualified for testing of minors. When examining a witness-injured party, the authorities may order the implementation of measures of witness hearing through using a video link.

When a minor is heard in the above-mentioned cases, the trial will read the record of his or her testimony, or playing a recording of the hearing.

The minor as damaged must have a legal representative at the first hearing. In the event that a minor does not have an attorney, one will be appointed by a decision from the list of lawyers who have acquired special knowledge in the field of child rights and criminal protection of minors set by the court president. Representation costs are borne by the budget of the Court.

Criminal proceedings for offenses under Article 150 of the JMC are urgent.

Forcing a minor to witness sexual acts (Article 185a)

The law also stipulated the basic form as follows: "Whoever induces a minor to attend rape, sexual intercourse or an equal act or other sexual acts (it is prescribed prison from six months to five years and a fine)." Paragraph 2 defines a severe form: if the offense was committed by force or threats, or against the child, (imprisonment of one to eight years). The perpetrator of this crime can be any person, but by the nature of things, a special circumstance carries weight when it comes to a person who is in congenial relations with a minor. The plot of the offense is a single act of attending by minor of such act. A special case here is related to the situation of "indirect presence" when using broadband Internet connection such activity displayed a juvenile or child. To prove these offenses due attention must be directed to the existence of evidence of sexual acts to which the juvenile was present, as well as traces of which can be related to its monitoring of such material. Such traces in the case of audio-visual record will remain on juvenile's computer and servers, through which have been shown, when it comes to the high-tech crime. For this reason it is very important to conduct the investigation by absolutely respecting the rules *lege artis*, and also browse and search of computers and the information stored in them. The question of specifying actions of minors in a given case must be also determined.

Utilization of the computer network or other means of communication to commit offenses against sexual freedom of a minor (Article 185.b CC)

Since the computer network often misused for the purpose of performing or concealment of crimes against sexual freedom of minors, the Criminal Code in Chapter XVIII, in Section 185b has regulated the criminal act of computer network or other means of communication for execution offenses against sexual freedom of minors. The act has a base and a more severe form. The basic form does a person with intent to commit a criminal offense under Art. 178. Paragraph 4 (the crime of rape - if the offense is committed against a child); 179. Paragraph 3 (The offense of sexual intercourse of

disabled person – if the offense is committed against a child); 180. c. 1 and 2. (The offense of sexual intercourse with a child – if it was done to the promise of a child (paragraph 1) and if it is due to the threat of serious bodily injury to a child, or if the offense is committed by more than one person or the offense resulted in the pregnancy (paragraph 2)); 181. c. 2 and 3. (The offense of Sexual Intercourse by Abuse of Power – if the act was executed by a teacher, educator, guardian, adoptive parent, stepfather, stepmother, or other person who abuses his position or authority commits incest against a minor entrusted to him for the sake of learning, parenting, custody or care (paragraph 2) if the offense is committed against a child (paragraph 3)); 182, § 1 (the crime of unlawful sexual act - if the above mentioned situations are performed another sexual acts or act); 183. Paragraph 2 (The offense of procuring and facilitating sexual intercourse - if it allows sexual intercourse, an act equal or other sexual acts with a minor); 184. Paragraph 3 (The offense Solicitation of Prostitution – if the specified offense execute against a minor); 185, paragraph 2 (The offense of displaying, obtaining and possessing pornographic material and a minor for pornography) and 185a (incitement of minors to witness sexual acts) of the Code, using a computer network or other means of communication with a minor agrees meeting and show up at the place of the meeting. For this form of criminal act is prescribed that the perpetrators could be sentenced by imprisonment of six months to five years, provided that the offender is punished and fined. A severe form of criminal act is if previously described basic form of same offenses is done against a child, and then the offender is punished with imprisonment of one to eight years.

The plot of the offense consists in arranging a meeting with a minor, or the child which is a severe form of the act in question, and the appearance of the place of the appointment. The formulation of Article 185.b shows that the action of committing the crime is determined cumulative, because its existence is necessary for the execution of both actions by the offender: 1) arranging the meeting and 2) appearance at the agreed place.

The offender can be any person who acts with direct intent, where it is necessary to determine the intention of performing by the Code enumerated offenses. It is obvious that the intention of the legislator was sanctioning of committing any form of criminal behavior in relation to sexual freedom and the minors and children, where the possibilities of computer technologies provide a significant contribution. That is why this article of the Code covers every intention of carrying out criminal acts against sexual freedom, if it is directed against a child or a minor if the offender in furtherance of a criminal offense uses computer technology.

Other offenses that are related to the misuse of ICT

In addition to these criminal acts against the security of computer data, we should mention the crimes: Displaying, acquisition and possession of pornography and the exploitation of minors for pornography under Article 185 of the Criminal Code. Misuse of computer network or other means of communication to commit offenses against sexual freedom of a minor of Article 185.b CC, Counterfeiting and abuse of credit cards in Article 225 of the Criminal Code, Fraud under Article 208 of the Criminal Code, as well

as the unauthorized use of copyrighted works or objects of related to authors rights under Article 199 of the Criminal Code, according to the provisions of the Convention on Cybercrime grouped with computer offenses and which, by their nature they are, in national legislation, fall under the jurisdiction of the Prosecutor's Office for combatting cybercrime, in accordance with Article 3 of the Law on Organization and Jurisdiction of Government Authorities in the fight against cybercrime.

Computer Related Fraud

Forgery and misuse of credit cards (Article 225 CC)

This criminal offense belongs to Chapter XXII of the Criminal Code - Criminal offenses against the economy. The offense does a person who forges a false payment card or alters – counterfeits a genuine payment card with intent to use it as genuine or that such false card uses as real, is punishable by imprisonment of six months to five years and a fine. Qualified forms of criminal act exist where there are obtained unlawful material benefit when using cards, for which a prison sentence of one to eight years and a fine, and if the offender is illicitly earned in excess of one million five hundred thousand dinars, by imprisonment of two to twelve years of imprisonment. A person who unauthorized uses of someone else's card or confidential information that uniquely regulate that card in the payment system shall be referred to the penalties provided for every severe form of work. A special form of act does person who obtains a fake bank card in order to use it as genuine, or who obtains information in order to use them to make fake credit cards, which will, in this case, be punished a fine or imprisonment up to three years. The fake payment cards will be subject to seizure.

By prescribing this offense legislator had the intent to protect payment cards as a means used in the payment system and have the same function as money. In recent years, misuse of credit cards (which is called a payment card), took on a very large volume, with the daily emergence of new, more sophisticated ways of committing this criminal behavior.

The criminal act in paragraph 1 shall be determined alternatively, consisting in making fake credit cards – forging, counterfeit – real alteration of the payment card with intent to use such rights or fraudulent use of payment cards. Forging means making fraudulent payment cards from items that previously were not the original payment card, while reversal, contrary to the previous one, involves rewriting the original credit card. Usage implies placing these cards in circulation and their use. The act is done by creating or modifying payment card with the intent to use it (or them) as a real (meaning that the very act of use, may be missing), but also by use of such cards. The act referred to in paragraph 4 consists of the unauthorized use of someone else's card or confidential information that uniquely regulates the card in the payment system, which means that it is real payment card, used by an unauthorized person, and for that reason this case qualifies as misuse of credit card. The plot of the offense referred to in paragraph 5 is also determined alternatively consisting obtaining fraudulent payment card with intent to use such card as real one or obtaining data with intent to use it to

make (forge) fraudulent credit card. For this type of act is regulated by the mildest punishment, bearing in mind that the person does not participate in the creation or modification of a payment card, or already procured a fake bank card or collect data that will be used in its making.

With regard to the type of crime, if it comes to creating and modification of the payment card, the offender can be any person who has the necessary professional and technical skills and equipment. This condition is not required in case of a sole use of such cards. In terms of criminal intent, it is necessary on the side of the perpetrator have the criminal intention.

To prove this offense is necessary to determine the time and place of execution, that the card being used is false, how it is made and by which technical means. Especially has to be paid attention to possible acts of complicity, because this crime and its actions, and the manner of its execution, may involve more than one person with different responsibilities within the criminal group – purchasing blank cards, purchase of equipment, procurement codes, making false payment or alteration of real payment card, the subsequent use of the traffic distribution or for use in traffic and so on. When a criminal offense in paragraph 1 is perpetrated, it is necessary to determine the criminal intent of perpetrator that the modified payment card was to be used as real. It is necessary, if possible, to determine when and where these cards were used, and the amount of damage caused by their use. When the criminal acts referred to in paragraph 2 and 3 is perpetrated, it is necessary to determine whether and in what amount the acquired material gain. For the criminal offense referred to in paragraph 4 it is necessary to establish a way of obtaining and usage of such cards and whether the perpetrator acted without authorization. For the criminal offense referred to in paragraph 5, it is necessary to determine in what way were obtained false payment card, whether it is purchased with the intent to use, and what data are obtained, in which way, the circle of people, whether they are purchased with the intention of making fraudulent payment cards and how, by whom and where such cards should be made.

As mentioned before, the execution of these offenses requires good organization and action of the offense takes place in several stages. Misuse of credit cards comes by perpetrators first purchase with the card information using various fraudulent methods (skimming, stealing pin codes, Lebanese mouth) then selling of the same information over the Internet to "end users" who make counterfeit cards inserting those records on Blanc ("white") cards. These cards are not generally used in countries where data were stolen, and in practice the perpetrators of these criminal acts usually strangers. Counterfeit cards are commonly used at ATMs.

There are several ways you can obtain information from debit and credit cards. Some of them are phishing, farming, skimming,[32] Lebanese mouth,[33] using hacking tools (malicious programs) and the like.

In addition to the organized crime groups which are concentrated in certain states or areas that have a clear and organized structure, there are many criminal groups

[32] Reading of digital characteristics of the card and its recording for further unauthorized use by perpetrator.

[33] In card insertion dor at the ATM is put device which jams card within it. Then to the victim comes friendly chance bywalker and tries to help by asking for code, and after unsuccessful attempt to unjam it now has the right code and the card.

that form around certain common interests and then last for some time, from several months to several years. These groups are formed depending on the needs and interests of their members. As the easiest method to communicate those groups chose forums and Internet sites with limited access to help when performing illegal activities to protect from criminal prosecution, and at the same time provide a place where they can share experiences, where they can buy and sell the means of execution offenses. Distribution of credit cards, the possibility of their use and availability of modern information technologies, has made them extremely attractive for a large number of criminals and criminal groups around the world. In particular, they become vulnerable markets where payment cards are being introduced into the payment system, where there is not enough experience in e-business and where there is no system to prevent such abuse, as well as the state where the standard is very high, and where there is developed a system of on-line banking and trade.

Payment cards can now be used for cash withdrawals at ATMs, bank counters, for payment of goods and services at retail locations equipped with POS (Point of sale.) terminals or imprinters, for payment in electronic commerce and payment for goods ordered by mail and telephone. Payment by debit card can be made through the Internet without going to the bank or to the dealer, out of the house, both at home and abroad. It is on the Internet there is the greatest danger to electronic data with debit cards being compromised.[34] We will see that in the physical environment poses a great danger – to fraudsters is enough that they are physically handed over the card and while you are fussing with various tricks they can swipe your card through any of their devices and record the data from the magnetic stripe (information, account and card). There are various systems that serve as protection – New Mastercard – by providing temporary generated numbers on the card to Jitter technology that uses a stop - start or jitter motion and if the ATM has skimming device installed it prevents the capture useful information about such movements. A special form of protection is the new EMV chip embedded in the MasterCard (MasterCard) that always gives when communicating with the authentication server dynamic element identification. Further forms of training payments go towards mobile payments (via cellular or satellite telephones, Wireless, phone), or tokenization, encryption or both ends of the communication connection (end-to-end encryption).

Specialized Internet sites and forums on the internet very often represent a suitable place for the offering of computer viruses on sale, as well as other services, including the software tools designed to provide information on payment cards, electronic tutorials designed to train individuals who want to obtain information on payment cards, and even information about payment cards such as debit card numbers, CVV2 numbers (Card Verification Value 2 - the three-digit number located on the back of the card), the type of payment cards, payment cards and validity of the names and surnames of the user, as and other data on the residence of the owner of the payment cards, electronic address of the owner, zip code, property on the basis of which the user is located at the base of some electronic stores, the date when the purchase is made, the IP address of the user, which is the same used for the purchase, the type of Internet browser used, as well as information on whether the user – client is still active client

[34] Urosević, V. „Misusse of payment cards and computer frauds“, *Legal informator* no. 9/2009, Belgrade p.4.

of electronic stores. In these forums are only offered as initial data bidders, which are nothing more than the initial contact (ICQ, MSN, email address, phone number or other contact information). After exchanging information with interested parties that are not binded neither the bidders nor the person concerned, users are directed to a safer Internet sites and forums (where access is protected by passwords) and where they offer a serious business.

The most common for purchase over the Internet is for the customer today that they need to have electronic data on credit card such as card number, validity (date of when the card is valid) and CVV2 number. This information on payment cards perpetrators of crimes over the Internet come in several ways, but the most widely used are:

1. Sending unsolicited messages (Spam)
2. Phishing
3. Pharming
4. The theft of payment card data from the database of electronic stores

Basic forms of counterfeiting and misuse of credit cards are:

- misuse of stolen or embezzled (lost) payment cards
- abuse of undelivered payment cards
- unauthorized use of someone else's payment card
- forging and use fraudulent payment cards
- obtaining data for making fake credit cards,
- abuse and fraud of traders,
- misuse by the user.

Card forums have become very popular as a place and a way to share knowledge and skills needed to carry out these crimes, as well as for sale data on payment cards, which were obtained in this way. Each day, hundreds of information regarding the stolen, fraudulent or other payment card is marketed by criminals who are engaged in the commission of offenses in this area to Card forums. Specialized forums connect cards and their customers. They buy the first test data, try them to see if they function properly, and if they are satisfied, they then buy a larger amount of these data, in order to further commission of offenses. These data can then be used for fraud related to classical forms of abuse such as downloading sums of money from ATMs using fake debit cards or purchase of goods, as well as for all other types of fraud such as "card not present" on the Internet.

There are many such forums, but the police service of many states failed to follow the activities on some of them, and to infiltrate the police officers in this virtual environment in order to monitor the activities of their members. Such activities of police forces on the other side in several cases have resulted in the discovery and arrest of the founding members of carders forums. One such forum was the Shadow Crew. This forum was in operation from August 2002 to October 2004. On it the users were offered information and data relating to the purchase or sale of digital personal or banking information (SSN - social security numbers, Damp card, CVV2 numbers), as well as falsified documents required for commission of criminal offenses in the field of economic crime. Users were given certain privileges through active participation and

contributions tutorials within the discussion groups. The forum content is offered for English and Russian language and it was mainly aimed at users in the United States and Eastern Europe. In the US, they are mainly engaged in hacking, and members from Russia and Romania were experts in the manufacture of fake payment cards and misuse.

Fraud (Article 208 CC)

Given that there are numerous ways of carrying out fraudulent activities on the Internet, it is reasoned that in this segment is also included the criminal offense of fraud under Article 208 of the Criminal Code.

This criminal offense belongs to Chapter XXI of the Criminal Code – Crimes against property. The offense does a person with intent to obtain for himself or another unlawful material benefit brought by false representation or concealment of facts bring somebody in a misleading or maintain him or her in error and thereby instigate him or her to damage his or someone else's property do or not to do something that would result in the same way, is subject to a imprisonment of six months to five years and a fine. The act has a privileged form of two qualifying forms. Privileged form of the act for which a punishment of imprisonment of up to six months and a fine is prescribed, where a person had only intended to inflict damage to another person. The first severe form of work if there is a material gain or causing a loss in excess of four hundred and fifty thousand dinars, and the offender is liable to imprisonment of one to eight years of imprisonment. Another serious form of criminal act if the material gains or causing a loss in excess of one million five hundred thousand dinars, and the offender in this case is punishable by imprisonment of two to ten years of imprisonment.

The plot of the offense is leading a person to do, or not do, something that is harmful to his (her) or another's property. Instigating represents the facilitating of decision making of the other person to take an action or to refrain from doing so and it must be directed to the property. The condition for the existence of this offense is that it is damaged person was under the influence of wrong notions about a fact something there was done or failed to do so and thereby damaged his (her) or someone else's property. It is necessary to determine the intent of the perpetrator of the offense, which consists of obtaining for self or another unlawful gain. Offender can be any person who must act with intent.

It has been mentioned that the development of the Internet as the best known and most popular global computer network expansion caused many crimes. In the domain of frauds characteristics of communication and correspondence on the Internet have provided excellent opportunities for a number of fraudulent forms. Many credible observers often point to the emergence of the Internet has not brought forms of fraud that did not exist before, but it has created unlimited opportunities for their exercise. Today the victim of fraudulent activities through the Internet can be every person, every business segment if (and in most cases it is) at the very same start is connected on the Internet.

Perpetrators are using the convenience that it provides to them almost total anonymity, and the fact that the digital financial flows, which usually run over more than one country, which are very difficult to monitor and determine the final destination of the funds. The sociological profiles of victims vary widely; a victim of fraud done online can be almost everyone, which is why it is necessary to always be on guard, because the perpetrators of such crimes develop new ways to improve the performance of their criminal activities and changing the target group of its activities. Groups of these criminals are very well organized, specialized for certain regions, and in order for Internet scams to be successful, criminals are using a wide variety of methods to obtain information about potential victims, to the creation of their social profiles.

Scams on the Internet are present in Serbia and that tells us an example of two people who were conned and damaged in this way for several thousand euros, with the organizers of fraud that still are not yet discovered. The victims received e-mail notification that they are going to get millions of cash prizes abroad. Having responded to the initial message, the victims were sent to more detailed information about how to raise the gain, contract forms that needed to be filled, the instructions for opening an account abroad at which the award will be paid, even activation codes for accounts where the money is, information about the people who were supposed to have received awards in this way, but even amounts of "taxes" to be paid and the account number to which the reward payment is going to be paid. When the victims paid the required amount, their resources are diverted to multiple other accounts abroad, in a way that monitoring of cash flow made it impossible.

In 2008 and 2009, at the territory of the Republic of Serbia were reported from victims' nine offenses of fraud with elements of "Nigerian scam" against unknown perpetrators. By these offenses were damaged citizens of the Republic of Serbia and companies from our territory, and the total property damage amounted to more than 60,000 euros.[35]

A special method for obtaining illegal profit is also through creating fake Web sites designed for buying goods. An example of this is the case of the Special Department of the Higher Court in Belgrade for the fight against cybercrime in criminal proceedings against six persons during 2003 who have made site www.escroweurope.net creating falsely prejudice in the appearance, content and web site address listed corrupted misleading to communicate with legitimate escrow service that provides mediation services when carrying out market transactions on the Internet, which are implemented only after the delivery of the purchase. The defendants had published false ads content and misrepresentation of facts that they as sellers possess certain goods to be delivered after payment, and that as the customer they will upon order – deliver goods to the seller after payment of that order, and in that way they would bring and maintain in error larger number of damaged American citizens and thus they instigated victims to at their expense through specialized services DHL, FedEx or UPS to send the goods concerned, or that as customers pay for the goods to the defendant as alleged dealers did not own, they were damaged through transaction service by using Western Union money, or by usage of credit card. The value of goods and money which the defendants have obtained in this way amounts to tens of thousands of euros.

[35] Urošević, V.: „Nigerijska prevara u Republici Srbiji", Bezbednost, Br. 3/2009, God. LI, Beograd, p. 152.

Unauthorized use of copyrighted works or objects of related rights (Article 199 CC)

Group of offenses against intellectual property that is specifically prescribed and covered by the Convention on Cybercrime, is contained in the Criminal Code under Chapter XX and belongs to the domain of the Prosecutor's Office to combat cybercrime, in accordance with Article 3 of the Law on Organization and Jurisdiction of Government Authorities in the fight against cybercrime. In the group of offenses against intellectual property are included the following acts: Infringement of moral rights of authors and performers (Article 198 CC), Unauthorized use of copyrighted works or objects of related rights (Article 199 CC), unauthorized removal or alteration of electronic information on copyright or related rights (Article 200 CC) infringement of patent rights (Article 201 of the Criminal Code) and unauthorized use of design (Article 202 of the Criminal Code). In this segment will be represented the most common criminal offense in practice – Unauthorized use of copyrighted works or objects of related rights, with regard to the piracy with the emergence and development of computer technology undergone expansion and has taken on global proportions.

The offense is committed by a person who publishes, records, reproduces, or otherwise publicly discloses in whole or in part the work of authorship, interpretation, videogram, broadcast, computer program or database, which is done for the offense is punishable by imprisonment up to three years. To the same penalty shall be accountable person who puts into circulation, or with the intention of traffic keeps unauthorized copied or unauthorized put into circulation copies of copyright works, interpretations, videograms, broadcasts, computer program or database. If the previous two types of acts are committed with the intent to obtain financial gain for self or another, carries a prison sentence of six months to five years. A person who produces, imports, distributes, sells, rents, advertises for the purpose of sale or lease or holds for commercial purposes devices or items whose main or predominant purpose is of removing, bypassing or circumventing of technological measures intended to prevent infringement of copyright and related rights, or when such equipment or facilities used for the purpose of infringement of copyright or related right, shall be punished by a fine or by imprisonment not exceeding three years. Items from the previously mentioned three forms of this crime will be seized and destroyed.

The plot of the offense is alternatively set as unauthorized publication, recording and reproduction, or disclosure otherwise authorship, interpretation, videogram, broadcast, computer program or database.

Under term of filming is considered to make a photographic or other recording of authorship, interpretation, videogram, broadcast, computer programs or databases, while the reproduction of making copies of the above listed items, where for the existence of a criminal offense is not of a significance sole number of copies, but is of significance for the competence to act in this criminal act, within the meaning of Article 3 of the Law on Organization and jurisdiction of Government Authorities in the fight against cybercrime. It is about jurisdiction of state agencies to act.

In paragraph 2 of this Article it is prescribed the action that builds on paragraph 1, which is manifested in the trafficking or unauthorized keeping with the intent of placing on the market of all the above cases, where the term marketing authorization involves their making available to the public, through sale, exchange, dispersal, gift, etc.

The perpetrator of this crime can be any person, considering that for its perpetration is not required specialized knowledge in the area of computing.

Piracy is very profitable, because sales revenue significantly exceeds the amount of funds invested, and in practice we have so far met several criminals who are dealing with this type of criminal activity, realize a large income. With the increasing number of Internet users and the introduction of higher-speed Internet rate, pirates have moved their operations to the Internet, which is discussed in a large number of sites from which you can order new bootlegged movies or computer games. More and more the perpetrators of these criminal acts can't physically find pirated copies, but they are on order above content downloaded from the Internet and then sell them to clients. In 2008, the Office of the fight against cybercrime were filed 319 criminal charges against 332 persons for committing a total of 379 offenses relating to violation of intellectual property, and seized a total of 131 232 optical discs and 50 technical devices.

The fact that greatly contributes to the prevalence of this crime is that people have no idea about the amount of damage that it causes. Buying cheap pirated discs, citizens believe that denying the arrival of powerful software companies like Microsoft, or the Hollywood film industry. The truth is, however, quite different. According to a study of the International analyst company IDC (International Data Corporation), in 2007 the piracy rate in Serbia was 76% and decreased by about 2% compared to 2006. It is estimated that due to such high rates of piracy domestic economy suffered a loss of $ 72 million, mostly through unpaid tax debts.

Perpetrators of crimes against intellectual property courts usually impose a suspended prison sentence, although in 2008 the Special Department of the District Court in Belgrade sentenced two perpetrators to prison, and that the defendant Ž. D. verdict K1 16/08 to imprisonment for a term of six months, and the defendant MJ verdict K1 17/08 to imprisonment for a period of eleven months. These persons were multiple recidivists, a previously convicted solely because of crimes against intellectual property.

An interesting example is the judgment of the District Court in Belgrade K1 VTK No. 19/08, in which the defendant J. W. and MS sentenced to a suspended term of imprisonment of six months' probation with a term of two years, as from 21 June 2005 until November 2007 at the premises of Excalibur net doo Kraljevo via wireless Internet network, unauthorized put on the market over 500 copies of copyright works - films, music and software, in order to thereby obtain pecuniary benefit themselves, so as to FTP server companies Excalibur net doo Kraljevo was putting copyrighted works - films, music, computer programs and other multimedia content and to the users of Internet services provided by their company, for a monthly fee of 10 to 20 euros, allowed to undertake specified activities.

As far as proving it is very important to establish a connection between the person who is the perpetrator and objects that are *corpora delicti* of the crime. The

connection can be established in e.g. comparing the digital characteristic time of occurrence, time of transfer to certain holders – the media, the specific work of authorship or video footage of the communication or interpretation of someone else's copyright work. An important feature is that the perpetrator is aware of the fact that it is a work of authorship and interpretation as well as knowingly publishing under his (her) own name or someone else's. In essence, it is essential that there are elements of deception or misrepresentation that the interpretation of the author's work or work of a person who publishes or a third party and not the victim. Thus, the perpetrator can be anyone.

Pirates for their actions misuse companies hosting storage files on their servers like Rapidshare, Megaupload and others. Before uploading original file is split into several smaller parts using some of the programs to share such as "Winzip", "ARJ" "FileSplitter" or "HJSplit", which is then protected with password. Small files obtained in this way usually do not have the original title of the film or program, making it difficult to detect illegal content. Links that lead to these files are found on websites and forums specializing in the exchange of pirated content. These companies provide possibilities to its customers at any time to report abuse, but they do not deter pirates to continue to raise illegal contents, causing that the servers of these companies today are considered the main sources of piracy on the Internet.

Another very popular way of sharing files that are abused for piracy represent torrents, programs that are based on "P2P" (Peer to Peer) technology, which is a direct connection between two computers to exchange data between users. A connection is established between users who have a certain file on your computer called "seeders" and clients who are looking for the same so-called "leeches" and in this way are usually exchanged various facilities: large video files, music and software works. To initiate the file download "leecher" launches torrent, a program that establishes a connection to a central server – "trackers" which contains information about "seeder". After that, the client establishes multiple simultaneous "P2P" connection with "seeder" and starts downloading the required file from multiple locations at once. A feature of this process is that the user that downloads files at the same time becoming "seeder" or shares the same files with other users.[36] Courts impose suspended prison sentences to the offenders against intellectual property usually.

In this section, entitled Application of substantive criminal law in the area of ICT, are presented the offenses against the security of computer data, as well as crimes in other areas, which are covered by the Council CETS 185 (and thus qualified as work in this field) and thereby, as such, is very common in national and comparative practice. In order to comprehensively inspect and analyse the substantive criminal law framework applicable to offenses related to the misuse of ICT, it is necessary to analyse the compliance of the domestic substantive criminal law with the provisions of the Convention, and thus to get the answer the question of how the requirements of the Convention have been met. Given the fact that the full implementation of the Convention requires the successful fight against ICT crime, in the following section is presented the degree of harmonization of offenses in this area prescribed in the Penal Code with the provisions of the Convention.

[36] "BitTorrent (protocol)", Wikipedia, Internet, http://en.wikipedia.org/wiki/BitTorrent_(protocol), 10.05.2009.

CONFORMITY OF SUBSTANTIVE CRIMINAL LAW PROVISIONS OF THE SERBIAN COUNCIL OF EUROPE CONVENTION ON CYBERCRIME

When it comes to compliance of substantive criminal law provisions with Serbian Council of Europe Convention on Cybercrime, in the previous section was emphasized that the provisions of the Criminal Code, as well as its latest amendments significantly expand the number and structure of offenses in this area, compared the earlier law from 2003, and to a large extent they comply with the Convention. Although provisions determining offenses against the security of computer data are not fully complied with the provisions of this Convention, the Council of Europe, may be initially concluded, with some reservations, that the Criminal Code together with statutory legal text in this field – the Law on Organization and Jurisdiction of Government Authorities for the fight against cybercrime, provides elementary legal framework for public administration in criminal justice matters relating to the misuse of ICT.

Starting from the article 112 of the Criminal Code, it is recognized that those specific amendments to the legal text cover the basic concepts of defining the elements of a computer system, and provided for by the Convention – computer data, computer network, computer program, computer virus, computer and computer system. Criminal Code, however, doesn't recognize the definition of provider – the provider of services, as provided for in Article 1 (c) of the Convention, nor the definition of data traffic, as provided for in Article 1 (d) of the Convention. On the given dates, as well as the terms of the electronic processing and transmission of data, public computer network, computer services, etc., can be inferred indirectly, in the description of specific crimes.

As for specific offenses in the field of computer crime the provision relating to illegal (unauthorized) access under Article 302 of the Criminal Code, in accordance with the requirements of Art. 2 of the Convention.

With regard to Art. 3. Convention – illegal eavesdropping, or illegal interception of communication it can be concluded that in the Criminal Code is not intended that provision to fully regulate this type of work. A certain similarity exists with the art. 302 CC - Unauthorized access to a protected computer, computer network and electronic data processing, keeping in mind that the work consists in an unauthorized access to a computer, computer network or electronic data processing, and paragraph 2, provided the recording or the use of in that manner obtained data. Given that CC has no express provision, it is not clear whether under this offense can be subsumed situation and interceptions (in) public transmission of computer data.

In terms of art. 4. Convention - Data interference in CC there is no single provision that would fully regulate the criminal offense of Data interference. Certain elements which correspond to the interference computer data can be found in Articles 298 and 300 of the Criminal Code. In the first case, it is the damage to the computer data and programs that can be achieved by deleting, changing, damaging, concealing

or otherwise suppression of computer data or program, while in the second case comes to the design and introduction of computer viruses. The above provisions do not fully follow the content and meaning of art. 4 of the Convention, since it includes some (manual) manipulation of programs and data, on the one hand, and the disruption of data caused by viruses, on the other hand, but does not include other ways of interfering in the details, such as the use of some other malicious program - a computer worm or Trojan horse.

With regard to Art. 5. Convention - jamming system, it is recognized that Art. 298 and 300 of the Criminal Code of qualitatively fit the description of the crime, in the same extent that they are represented in the previous section. And here we can conclude that the above provisions do not fully follow the concept of the Convention, particularly in the area of usage and some other malicious program – a computer worm or Trojan horse, since there it is in the Criminal Code stipulated only criminal act related to the creation and introduction of computer viruses. In the context of interference with a computer system can be extracted and criminal act of computer sabotage (Art. 299 CC), which includes a variety of manipulative acts in relation to computer data, program, sole computer or other device for electronic processing and transmission of data within system of state bodies, public agencies, institutions, businesses, and so on.

As for the art. 6. Convention – Misuse of devices within the CC there are provisions which only partially meet the requirements of these offenses. In fact, art. 302 - Unauthorized access to a protected computer, computer network and electronic data processing art. 304 - Unauthorized use of a computer or computer network, as well as art. 199 para. 4. CC - Unauthorized use of copyrighted works or objects of related rights in certain segments include important issues foreseen by the Convention. Art. 302. CC criminalizes illegal access to data, but does not cover the preparatory actions envisaged by the Convention, art. 304. CC criminalizes unauthorized use of computer networks and services, but not including other tortious acts that fall under Art. 6 of the Convention. In the end, art. 199 para. 4 criminalizes actions in terms of equipment and devices aimed at removing, bypassing or circumvention of technological measures intended to prevent infringement of copyright and related rights, which means that this provision is limited to the infringement of copyrights which are not on the list of offenses to which this article Convention applies.

Criminalization of computer counterfeiting, the way it was done in the art. 7. The Convention has not yet been provided for in the Criminal Code.

In terms of article 8 of the Convention - computer fraud, of importance is art. 301 of the Criminal Code (computer fraud), which corresponds to the aforementioned article of the Convention. In both provisions provides for actions that involve some interaction with the computer data in order to gain illegal profit, thus causing damage to others. However, the provision of Art. 301. CC does not contain all of the offenses referred to in Art. 8 of the Convention, and could be judged as incomplete in terms of content and concept of the Convention.

Art. 9. The Convention applies to offenses related to "child pornography". In accordance with the context of the above provision, Art. 185 CC - displaying, acquisition and possession of pornographic material and exploiting minor for pornography

and 185.b CC - Utilization of computer networks or other means of communication to commit offenses against sexual freedom of a minor, can be identified as terms that correspond to the above-mentioned article of the Convention and to criminalize acts related to production and distribution of "child pornography". Unlike systematics incrimination provided for in the Convention, the provisions relating to this matter, which are prescribed under the Criminal Code, can be found in Chapter under the Title - Crimes against sexual freedom, which are displaced compared to a group of offenses against the security of computer data, by which in certain way was given secondary importance to the misuse of computer technology in this field, and in practice that is not the case.

In terms of article 10 of the Convention – offenses related to infringement of copyright and other related rights, the provisions of article 198 CC - Infringement of moral rights of authors and performers, art. 199 CC - Unauthorized use of copyrighted works or objects of related rights and art. 200. CC - unauthorized removal or alteration of electronic information on copyright and related rights all can be identified as those correspond to the provisions of the Convention, provided that it doesn't include all the elements that are included in article 10 of the Convention.

After analyzing the offenses prescribed in the Criminal Code of Serbia and the Council of Europe Convention on Cybercrime, especially after a comparative analysis of compliance of the above provisions of the two acts, it is evident that CC still hasn't reached a high level of compliance with the provisions of the Convention.

APPLICATION OF THE LAW OF CRIMINAL PROCEDURE IN THE AREA OF ICT

General remarks on procedural criminal law

The Code of Criminal Procedure[37] as other types of regulations in Serbian criminal law contains provisions of procedural legal character, by which are predicted procedural mechanisms and powers of all participants in the criminal proceedings in terms of identifying offenders, evidence collection, prosecution and trial.

According to this Code, criminal acts in the field of ICT abuse do not constitute a basis for the creation of a special criminal-procedural form, but only the basis for the organization and responsibilities of special state agencies who participate in their detection, prosecution and trial. There are no special features in terms of procedural regulations that are given to them. [38] Because aforementioned specialization of authorities in combating these crimes, there was adopted the Law on Organization and Jurisdiction of Government Authorities in the fight against cybercrime. [39] Given that the procedures for acts in the area of computer crime do not change the process structure (process phases and stages), but only certain provisions of process subjects or to the process actions, it cannot be considered as a special criminal procedure form, but only on procedural variability. There are four sets of criteria for establishing procedural variability:

a.) the seriousness of the offense;

b.) the type of offense;

v.) the type of criminal sanctions or other criminal measures;

g.) the subjects of criminal procedure.

According to this distribution criteria the criminal act of computer crime (hi – tech) could be subsumed under the criterion according to type of criminal offense, and in this group could be classified as criminal offenses of organized crime, corruption and other very serious crimes, war crimes, and so on.

Provisions of the Criminal Procedure and evidence in proceedings for offenses in the field of ICT

Within the procedural provisions for offenses in the area of computer crime have special significance provisions governing the finding, collection and provision of evidence.

In connection with the execution of these acts there appear special kinds of traces, as future evidence, which by their nature differ from the so-called classic evidence

[37] Official Gazette of RS", no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013.

[38] Brkić, S.: „Krivično procesno pravo II", Pravni fakultet u Novom Sadu, Novi Sad, 2010, p. 304.

[39] Official Gazette of RS", no. 61/05 i 104/09.

appearing in connection with the commission of offenses of general crime, such as electronic (digital) evidence. One of the shortcomings of the current Code of Criminal Procedure is that it does not give precisely the definition of evidence, and consequently the definition of electronic evidence. Electronic evidence is information or information important to the investigation, which is stored or transmitted using a computer. The aforementioned evidence has the same value as all other physical evidence, and investigators must follow exactly the same procedural rules as well as for extraction of all the other evidence. However, what one must not lose in sight of in terms of electronic evidence is their specificity, which arises from their nature, and that is that they are very sensitive, or easily can be modified, deleted or otherwise destroyed. Also, electronic evidence can be stored on a single computer, computer network or remote server outside the territorial jurisdiction of the authority that should collect them, can be visible or invisible, which, in addition to the aforementioned possibilities of their ease of modification or destruction, to deliberate, and due to improper handling, imposes a number of specific features in their acquisition.

The basic principles of obtaining electronic evidence imply that any action authorized persons must not be altered content of data to be reviewed. The above principles it is necessary to consistently apply in each case in order to preserve the integrity of the evidence to be obtained, documented process of obtaining that allows you to repeat the process if the need arises later in the process, which ensures its probative force of the law.

Considering that the facts constitute grounds for a decision on the existence or non-existence of the crime, as well as the criminal responsibility of the perpetrator, it is necessary to bear in mind the specifics of electronic evidence, which may be of great importance to fully establish the facts.

CETS 185 in this segment has paid attention to the importance of the specifics of electronic evidence in that respect contains special modes that allow or facilitate the collection of this type of evidence. In contrast to the Convention, the Code of Criminal Procedure does not provide for specific procedural rules and authority of state bodies in this field, but the general procedural rules apply as in the case of collection of other evidence. This approach certainly raises the question that the above-mentioned segment requires specification of a process approach.

It has already been pointed out that proceedings for offenses in the field of ICT is a process variability, which in terms of the process of proving the relevant facts in the proceedings indicates that, there are absent specific (highly specific) powers and mechanisms of state authority responsible for prosecuting these types of crimes. According to the Criminal Procedure Code activities provided are:

1) The hearing of the defendant (Articles 85 - 91);

2) Examination of witnesses (Articles 91 - 113);

3) Expertise (Articles 113 - 124 and 127-133) - Expert IT professionals with the possibility of hiring an expert advisor (Articles 125-126.);

4) A crime scene investigation (Articles 133 - 138);

5) Documents (articles 138-140).;

6) Samples (articles 140.-143).

7.) Accounts and suspicious transactions checking (Article 143 of 147).

8) Dealing with things unknown owner (Article 154);

9) Search of premises and persons and seizure of evidence (Article 152 members 155.- 160.)

10) Temporary seizure of items (articles 152 and 147-Article 153) and

11) Special evidential measures (Article 161-188).

In this context, the Criminal Procedure Code provides for the obligation of all state agencies to the courts and other agencies participating in criminal proceedings to provide the necessary assistance, especially when it comes to detecting crime and finding the perpetrators. The Code also provided special evidentiary action or measures (item 11 of the previous paragraph). It was determined that these actions are applicable to organized crime offenses, criminal procedure as a kind of form that also falls into the category of process variability.

Under the terms of Article 161 of the Code special evidentiary action under Article 166 (Secret surveillance of communication) can be determined for the following crimes related to the hi-tech crime: displaying, acquisition and possession of pornographic material and abusing a minor for pornography (Article 185 para. 2 and 3 of the Criminal Code), inciting national, racial and religious hatred (article 317 of the Criminal Code), as well as the unauthorized use of copyright works or subject matter of related rights (Article 199 of the Criminal Code), damage to computer data or programs (Article 298, paragraph 3, of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud (Article 301 paragraph 3 of the Criminal Code) and unauthorized access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code).

If the Public Prosecutor doesn't initiate criminal proceedings within six months from the day when he was familiarized with the material collected by using a special evidentiary action, or if it states that it will not use that material in the process, and that for the suspect he or she will not start the proceedings, the preliminary proceedings judge shall issue a order about the destruction of the collected material.

In terms of looking at the level of harmonization of criminal procedural legislation of Serbia with the provisions of the CETS 185, it is necessary to give a detailed overview of all implemented solutions and all solutions that are not yet included in national procedural framework.

The difficulties that arise when investigating and prosecuting offenses in the field of ICT

In the text below, keeping in mind the specific offenses in the area of ICT, as well as the peculiarities of national legislation in this area will be discussed difficulties that occur during the investigation and prosecution of these offenses, with a particular focus on the issues that almost always occur in practice.

The transnational character of the offenses in the field of ICT and international cooperation among different legal systems

The offenses in the area of ICT are characterized by significantly expanded area of criminal activity that does not require the presence of the perpetrator at the scene of the crime. Specific spatial category is characterized by global and transnational scope that transcends territorial control of nation states. Users of computer technology without control can move in the virtual IT world, regardless of national boundaries. Illegal activities can be carried out regardless of the time dimension, and regardless of where the offender is located. Therefore, a large number of crimes in this area are related to their nature, for a number of countries, combinations that may arise in this are almost endless. Often in these situations are raised questions of ability to prosecute offenses whose enforcement action were taken on the territory of several countries simultaneously, or ways of prosecuting the perpetrator or perpetrators of the act in the state on whose territory it was committed is not punishable. In these cases, there is no universal solution or single answer.

The transnational character of the cybercrime acts creates the need for effective international cooperation. When it comes to effective fight against this type of crime, is invaluable to have a good legislation in the field of international legal assistance. Global instruments of international law to regulate the cooperation in this field don't exist. Regarding the situation in Serbia, the Law on Mutual Legal Assistance in Criminal Matters, failed to regulate specific aspects of mutual legal assistance in criminal matters in the field of ICT which, more than any other, the rate in treatment of crucial importance for the successful conduct of criminal proceedings. It goes without saying that the absence of adequate international cooperation, particularly with offenses which have a distinct transnational line, definitely contribute to their development and stimulation.

Relativity principles "*ignorantia juris non excusat*"

Relativization of the principle that ignorance of the law does not excuse, as well as the principle that ignorance of the law harms (*Ignorantia iuris nocet*) does not lead to the suppression of their application, or to the simplification of their meaning. The point of certain discrepancies is that in the field of computer crime, there are situations when persons who commit acts of certain offenses don't need to be aware of what they do, or have no intention to harm anyone or acquire certain illegal material (or other) benefits. It may happen that a person via electronic mail system is virus infected and thus infects all other e-mail addresses that are stored within the computer, and that doing so was not aware of the presence of malware on their own computer. It can also happen that by an e-mail people come into the possession of illegally procured materials disseminated (eg, illegally downloaded film), and so on. If these actions do not represent everyday practice, but sporadically, their social danger practically is non-existent, and therefore does not represent a reason for initiating court proceedings in this case.

The necessary level of expertise

In order to in properly identify the material facts and take the right stand on specific issues in the process, the judge, the prosecutor, the local police have to have an enviable knowledge of the matters concerned. However, states rarely implement specialization and special training for judges and others involved in combating crime in the area of ICT, although in practice many procedures have shown that experts can't interpret the facts in a way that the judge without any knowledge could understand sufficiently that based on them decide on someone's criminal responsibility.

Determining the identity of the offender

The question of the identity of the offender in the area of computer crime can be very difficult to answer due to the fact the computer can be manipulated by another person, even when the owner is working on that computer. To solve the problem of determination of real perpetrator of the crime, investigative actions must be carried out thoroughly, which again points to the necessity of a certain degree of prosecutor and the police expertise while conducting the investigation. This should especially be kept in mind because the majority of computer fraud has been brought to perfection of manipulation of other people's computers that must be very carefully handled with possible suspects until they came to the unequivocal knowledge that they in any way could be involved in the perpetration of the crime.[40] Also a very big problem could be built up by the difficulties in detecting the offender who committed the act of using the public network and a laptop computer. Specifically, as a result of the development of new Internet communication capabilities, it has become quite possible that someone uses a public network available in public areas, Internet cafes, or for purposes of certain abuses advantage of the ability to access an open network of another user. In such cases, the perpetrator is almost invisible and it nearly impossible to trace, because in terms of locations and IP addresses available to any person.

The question of the validity of electronic evidence

In the event that the data of current provider is not sufficient to connect to a specific person committed a criminal offense, the question is how valid is the hard disk, flash memory and other electronic evidence, especially in cases where judges, prosecutors and other relevant actors do not have adequate level of knowledge in the field of information technology. Because of the importance of issues of electronic evidence, the European Union has implemented from 2005 to 2007, a project entitled "Eligibility of electronic evidence in court. The project included an analysis of legislation and court proceedings in sixteen member states of the European Union. Analysis showed that the laws in some jurisdictions had no definition of electronic evidence, while

[40] Case that shows complicity that can occur: http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars> (May 01, 2009)

others contain such a definition, but in it they are not the most accurate. The common conclusion is that in all jurisdictions electronic evidence is commonly tied with classic evidence for its strength and electronic documents from paper documents, electronic signature with a personal signature and e-mail with the postal mail. When it comes to procedural rules, both in civil and in criminal matters, there weren't established common standards for the collection, preservation and performance of electronic evidence in court. Mainly were used analogies in relation to the classical proof, although some countries like the United Kingdom and Belgium have defined rules for the collection of computer evidence.

Other relevant issues

In the field of ICT prosecution of offenses may also pop-up other issues related to the procedures, the offender, legal aspects etc. Among the more prominent dilemmas is how to deal with juvenile offenders as with the level of psycho-physical development which could be insufficient to understand the significance and consequences of actions done. It is true that almost all legislation containing provisions that formal juvenile offenders provide specific, primarily educational treatment. However, keeping in mind the specific area of computer crime with possible catastrophic consequences to which those actions can lead, which almost every minor who possesses a certain, often basic knowledge of IT field, could contribute – the question of efficiency of classical criminal law in relation to minors could be posted.

In accordance with this dilemma, it is necessary to devise adequate preventive activities in the field of computer crime, considering that repression measures in this segment are not the best solution, moreover in some situations it is completely pointless. Important question is how to handle recidivism, or how to prevent it and to divert the recidivism of such offenders (in the case of minor offenses) and steer them in socially useful work, through alternative sanctions and the stimulation of creativity, rather than punishment.

The analysis of these specific evidentiary actions provided by CPC and issues that were in process practices put aside, it is evident that legislation in Serbia hasn't adopted procedural measures or procedural powers of authorities that during the collection of evidence provide an adequate level of understanding of the sensitivity and importance of electronic evidence. It was alleged that during the proces of solving criminal act in computer (hi-tech) crime can't be applied special investigative methods that are legally applicable only to offenses of organized crime, corruption and other serious criminal offenses. Therefore, in the process of detection and prosecution of criminal offenses ICT, by the competent national authority are enforced the provisions of CPC regarding the regular procedure, applicable to all other crimes.

In order to comprehensively inspect and analyze criminal-procedural framework relating to offenses related to the misuse of ICT, it is necessary to analyze the compliance of the national procedural criminal law with the provisions of the Convention, and thus answer the question of how the requirements of the Convention have been met.

Compliance procedural criminal law with the provisions of the Serbian Council of Europe Convention on Cybercrime

With regard to the compliance of the criminal procedure law of Serbia with the provisions of Council of Europe Convention on Cybercrime, the situation is as follows. The mechanism of the emergency protection of stored computer data provided by article 16 of The Convention is an instrument that allows the competent authorities of protecting computer data to ensure that they aren't erased, or otherwise compromised before they get a chance to be provided for the purposes of criminal proceedings. The national legal framework on the application of this mechanism could be explained through the application of the provisions of Articles 168[41] and 286[42] of the Code. These provisions provide for the possibility of only partial fulfilment of the requirements of the Convention. In other words, they do not represent a complete basis for the immediate expedite protection of stored computer data. On the other hand, the requirements of the Convention in the context of measures relating to the obligation to protect the integrity of computer data in a period not exceeding 90 days, as well as the obligation to maintain the confidentiality of such proceedings, are not prescribed in our procedural legislation, at least not in criminal procedure.[43]

The intention of the Convention creators in respect of the following measures envisaged by Article 17 – expedited preservation of data and partial disclosure of traffic data is that it actually bridges the separation of orders for expedited preservation of data and the obligation of handing over such data. In domestic law, paragraph 2 of Article 168 of the Code partially corresponds to the Convention rules. Partially because the provision applies to the passive behavior of postal, telegraphic and other companies, firms and individuals registered for the transmission of information, or referring to their "duty to facilitate the implementation of surveillance and recording of communication and, with confirmation of receipt, to submit letters and other shipments."

The purpose of the measures referred to in Art. 18 of the Convention – production order, is that to authorize the competent authorities of a Member State to order persons in its territory or providers to submit certain information that they own or control, or to hand over subscriber information regarding the services that such service provider owns or controls. Criminal Procedure law of Republic Serbia recognizes only the already mentioned Article 168 of the CPC, which does not correspond to the described purpose of this measure due to the fact that it applies only to companies and persons registered for the transmission of information, but not to any person who possesses certain information. The provision of the CPC which regulates the temporary

[41] Section 2 article 168 of CPC regulates production order, where the court (functionaly judge of pretrial procedure) issues an order to bind companies of postal, telegraph and other services registered for transfer of information to facilitate to state agency (determined inthat order) enforcement of surveillance and recording of communication, and to facilitate production of letters and other shipments, with receipt of receiving

[42] Article 286 of CPC provides police powers. If there are grounds for suspiction for criminal act which is prosecuted *ex officio* police has obligation of taking measures which are neceserry for finding the perpetrator, to prevent the perpetrator or accomplices from hiding or escaping, to find and secure traces and objects that could serve as evidence, and to gather all of information which could help further in proceedings

[43] As it can be inferred from previous elaborations these measures are existing in other related legal documents as ELC and others.

seizure of objects (Article 153), also does not match the requirements of the Convention with respect to that is limited to the confiscation of the objects themselves.

Measure under Article 19 of the Convention – the search and seizure of computer data stored, was prescribed primarily due to the fact that national legislation often does not cover the procedure search and seizure in terms of data, but only in terms of objects. As in the previous article stated, according to the CPA, it is not problematic the possibility of search and seizure of objects in their physical form, in sense that it could be computer or server, but there is no possibility of search and seizure in terms of the data, which in practice rarely causes problems, and complications. But that is also covered in Serbian CPC provided a little awkward among special investigative measures as Automated (computer assisted) search of computer and other data under the article 179.

The following measures stipulated in Articles. 20 of the Convention – the collection of traffic data in real time, allows the authorities to collect real-time and recorded data traffic of certain communications transmitted over a computer system. This measure is not governed by the provisions of the CPC. As noted above, under the terms of Article 161 of the Code special evidentiary action under Article 166 (Secret surveillance of communication) can be determined for the following offenses: unauthorized use of copyright works or subject matter of related rights (Article 199 of the Criminal Code) damage to the computer data and programs (Article 298, paragraph 3, of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud (Article 301 paragraph 3 of the Criminal Code) and unauthorized access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code). However, measures of secret surveillance of communication can be carried out only under legal standards, on the one hand, and on the other hand, it is just one in a series of evidentiary actions. Other measures are not adapted to the specifics of work in the field of ICT.

Measure of the interception of content data is prescribed in Art. 21 of The Convention build on the previous measure, and also gives the opportunity to the competent authorities to act in real time, when the need arises. This feature can be very important when the competent authorities know communication partners, but do not have data on the type of information that is exchanged. Based on the previously described statutory provisions in Serbia, this measure is not strictly covered by the provisions of the Code.

The measures of the Convention, in the opinion of the international community, are a necessary minimum standards that must be met in order to create the conditions for successfully combating cybercrime and that, as such, should be implemented in national law, but to any country that has signed and ratified Convention it has left the possibility of making a reservation on the implementation of certain measures, particularly those relating to the collection of data on real-time traffic data and interception of content. The purpose of the reserve is to enable the Parties to establish certain conditions and limitations for implementation and application of the Convention powers which shall provide for adequate protection of human rights and freedoms in accordance with international obligations.

From the analysis of the procedural provisions laid down in our CPC and the measures envisaged in the Convention on Cybercrime, it is recognized that compliance of the provisions of criminal procedure legislation in Serbia with the Convention substantially lags behind the compliance of criminal – the substantive provisions.

INDEX

SELECTED BIBLIOGRAPHY

Books:

Bainbridge, David Introduction to Computer Law, Pearson Education Limited, London, 2000.

Bjelić Predrag, Elektronsko trgovanje – elektronsko poslovanje u međunarodnoj trgovini, Beograd, Institut za međunarodnu trgovinu i privredu, 2000.

Brkić, S.: „Krivično procesno pravo II“, Pravni fakultet u Novom Sadu, Novi Sad, 2010.

Cohen, Jehoram Tobias *Copyright in non-original writings past - present - future?*, in: Intellectual Property and Information Law, Kluwer, 1998.

Ćorović, Vladimir *History of the Serbs*, („Glas srpski”, Banja Luka “Ars Libri”, Beograd, 2001)

Dimitrijević, Predrag, Pravo informacione tehnologije - osnovi kompjuterskog prava, SVEN, Niš, 2009.

Drakulic M., Jovanovic S., Drakulic R., 2010, *Establishment CSIRT-a in Serbia, Incorporation of Broadcaster according to Serbian Broadcasting Law* article presented at the conference 12h International symposium FOS, SymOrg 2010, Zlatibor, 2010.

Drakulić, M. Računarsko pravo, Beograd.

Dworkin Gerald, Judicial Control of Copyright on Public Policy Grounds, in: Intellectual Property and Information Law, Kluwer, 1998.

Efraim Turban, at all, Electronic Commerce : A Managerial Perspective, New Jersey, 2000.

Garzaniti, L. J., & O'Regan, M. (Eds.). (2010). *Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation*. Sweet & Maxwell, Limited.

Group of authors, „Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala“, Savet Evrope, 2008

Komlen-Nikolić Lidija et alia, Suzbijanje visokotehnološkog kriminala, Beograd, 2010.

Komlen-Nikolić, L.; Gvozdenović, R.; Radulović, S.; Milosavljević, A.; Jeković, R.; Živković, V.; Živanović, S.; Reljanović, M.; Aleksić, I.: „Suzbijanje visokotehnološkog kriminala“, Udruženje javnih tužilaca i zamenika javnih tužilaca Srbije, Beograd, 2010

Koumantas Georges, *Reflections on the concept of intellectual property*, in: intellectual property and Information Law, Kluwer, 1998.

Lazarević, Lj.: „Komentar Krivičnog zakonika Republike Srbije“, Savremena administracija, Beograd, 2006

Mina Zirojević, Zvonimir Ivanović, Zaštita prava intelektualne svojine u sektoru informaciono – komunikacionih tehnologija, Institut za uporedno pravo, Belgrade, 2016

National Information Technology and Internet Agency, *Analysis of legislative framework for e-Government in Serbia*, 2006.

Overbeck Wayne, Belmas Genelle, Major Principles of Media Law, Stamford: Cengage Learning, 2011.

Prlja, D. i Reljanović, M.: „Pravna informatika“, Pravni fakultet Univerziteta Union, Javno preduzeće Službeni glasnik, Beograd, 2010

Prlja, D. Reljanović, M. Ivanović, Z. *Internet pravo,* Institut za uporedno pravo, Beograd, 2012.

Prlja, D. Reljanović, M. Ivanović, Z. Krivična dela visokotehnološkog kriminala, Institut za uporedno pravo, Beograd (2011).

Schafer Arthur, Privacy - A Philosophical Overview, Aspects of Privacy Law, Edited by Dale Gibson, Toronto,1980.

Sofaer, Abraham D Seymour E. Goodman (ed.), The Transnational Dimension of Cyber Crime and Terrorism, Hoover Press, 2001.

Spasić Ž. Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011.

Spasić, Darko *Digital certificate as digital identity of Internet users*, Serbian Post Company, 2006.

The Law on Territorial Organization of the Republic of Serbia, *Official Gazette RS,* nr 129/2007.

Van Duyn J. A., The Human Factor in Computer Crime, Los Angeles, 1985.

Vidoje Ž. Spasić, Autorska dela u digitalnom okruženju, Niš, 2011.

Vuksanović, Emilija „The role of bankcard industry in transition of Yugoslav Economy", *Proceedings of theInternational Conference ICES 2002. Sarajevo, Bosnia-Herzegovina, October 17-18, 2002*.

Warren Samuel, Brandais Louis, The Right to be Left Alone, Harvard Law Review, 1890. (G.L. Simons, Privacy on the Computer Age).

Žarković, M. Drakulić, M. Miladinović, S. Urošević, V. Batrićević, A, Lukić V. Ivanović, Z. Drakulić, R. Jovanović, S. Janković, Đurašković, M. Stojičić, S. Milanović, L. *Veze Cyber kriminala sa iregularnom migracijom i trgovinom ljudima*, (there is a English version of this book and two cd of bilingual character) Ministarstvo unutrašnjih poslova, Urednik Vladimir Urošević, 2014.

Articles

Ivanović, Z, Branković, A. *Analiza primene normi o zadržavanju podataka Konvencije CETS 185 u Srbiji,* u Zbornik radova sa nacionalne konferencije BISEC 2012, (Ур. Nedžad Mehić) Univerzitet Metropolitan, Beograd

Ivanović, Z. u Harmonizacija zakonodavstava Republike Srbije sa pravom ЕУ, *Analiza harmonizacije propisa u oblasti VTK,* IMPP, IУP, HSS Beograd, 2012, str.795-808,

Jankovic, M.Lj. ; Dukic, M.L. A proposal for telecommunications strategy in Serbia IEEE Communications Magazine, Aug. 2005, Vol.43(8), pp.1-4[Peer Reviewed Journal]Liu, Y. L. (2011). The impact of convergence on the telecommunications law and broadcasting-related laws: A comparison between Japan and Taiwan. *Keio Communication Review*, *33*, 43-67

Korać, S.: „Suzbijanje dečije pornografije na Internetu: EU standardi", Centar za bezbednosne studije, Godina II, Br. 11/2008, Beograd

Krone, J., & Pellegrini, T. (2012). Changing paradigms in network neutrality and its effects on public sector broadcasting online services: Germany's case. *Issues of Business and Law*, *3*, 73-84.

Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, Vol.9484, pp.161-177,

Pisarić, M., Surveillance of electronic communications in republic of Serbia

Prlja, D.; Reljanović, M.: „Visokotehnološki kriminal – uporedna iskustva", Strani pravni život, br. 3/2009, Institut za uporedno pravo, Beograd

Radulović, S.: „Specifičnost pribavljanja elektronskih dokaza o izvršenju krivičnih dela visokotehnološkog kriminala", Revija za bezbednost, br. 12/08, godina II, Centar za bezbednosne studije, Beograd

Serbia Telecommunications Report 2017, Business Monitor International, London;

Tintor V. Milićević, V. Janković, M. Radunović, J. Liberalization of the mobile telephony market in the Republic of Serbia, Technology in Society Volume 31, Issue 4, November 2009, Pages 384-398

Urosević Vlada, „Misusse of payment cards and computer frauds", *Legal informator* no. 9/2009, Belgrade.

Urošević Vlada, „Nigerijska prevara u Republici Srbiji", Bezbednost, Br. 3/2009, God. LI, Beograd.

Urošević, V.: „Nigerijska prevara u Republici Srbiji", Bezbednost, Br. 3/2009, God. LI, Beograd

Vuksanović, Emilija „The role of bankcard industry in transition of Yugoslav Economy", *Proceedings of the International Conference ICES 2002. Sarajevo, Bosnia-Herzegovina, October 17-18, 2002*, pp. 767-775.

Internet sources:

Aćimović, B.: „Žestok DoS napad na pet gigantskih sajtova", Linux.rs, <http://www.linux.rs/content/view/112/20/> (May 7, 2009);

Arstechnica: http://arstechnica.com/tech-policy/news/2007/04/child-porn-case-shows-that-an-open-wifi-network-is-no-defense.ars> (May 01, 2009)

BIRPI, http://en.wikipedia.org/wiki/BIRPI poslednji put pristupljeno 24.01.2012

BitTorrent (protocol), Wikipedia, Internet, http://en.wikipedia.org/wiki/BitTorrent_(protocol), 10.05.2009.

Broadcasting Act, http://www.minoritycentre.org/library/broadcasting-act-republic-serbia-amandments.

Budde, stabile internet address https://www.budde.com.au/Research/Serbia-Telecoms-Mobile-Broadband-and-Digital-Media-Statistics-and-Analyses.

Centr, www.centr.org.

Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5, 2010)

Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013)

Creative Commons, Internet address: http://creativecommons.org.rs/faq. 6.11.2010.

Dusollier Séverine, *Scoping Study on Copyright and Related Rights and the Public Domain*, WIPO, 2010, Internet address: http://www.wipo.int/ip-development/en/ agenda/pdf/scoping_study_cr.pdf, 6.11.2010.

E uprava: https://www.euprava.gov.rs/en/aboutserbia.

EFF (*Electronic Frontier Foundation* http://www.eff.org, 01.10.2014.

Elitesecurity, www.elitesecurity.org/forum/230.

Guidelines for the cooperation between law inforcement and Internet service providers against cybercrime; Internet addres http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_activity_Interface2008/567_prov-dguidelines_provisional2_3April2008_en.pdf

Icann, www.icann.org.

IFAP, http://www.ifap.ru/library/book294.pdf, 01.07.2012.

Internodium www.internodium.org/node/1824.

ITU, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf p.19. 14.03.2010.

ITU, Stable internet address http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-toolkit-cybercrime-legislation.pdf.

Jelić Ivan, Zajednica u savremenom informatičkom društvu, 2006, Internet address: http://www.bos.rs/cepit/idrustvo2/tema14/zajednica.pdf , 4.11.2010.

Lorenzo Valeri, et alia, Handbook of Legal Procedures of Computer and Network Misuse in EU Countries (2006), and national reports available at Internet address: http://www.coe.int/cybercrime , 01.08.2014.

Nate Anderson, *World's Worst Internet Law*, http://arstechnica.com/news.ars/post/20060804-7421.html, 01.10.2014

"Podignuta optužnica protiv autora Sassera", Mikro-PC World; <http://www.mikro.co.yu/main/index.php?q=vestiarhiva&godina=&mesec=&ID=6192> (May, 7, 2009)

Ratel, stable Internet address: http://www.ratel.rs/upload/documents/Pregled_trzista/RATEL_Annual_Report_2015_eng.pdf..

Ratel, stable Internet address: https://www.ratel.rs/upload/documents/Pregled_trzista/Q3%202017%20ENG.pdf.

Ratel, stable Internet address: *https://www.ratel.rs/uploads/documents/empire_plugin/5bd194d2428d3.pdf*.

Register of national Internet domain of Serbia – RNIDS. Internet address:

Regulation on the content and manner of submitting notification on concentration, http://www.kzk.gov.rs/kzk/wp-content/uploads/2016/11/01-Regulation-on-the-content-

Regulatory Agency for Electronic Communications and Postal Services RATEL, can be found at stable internet address: http://www.ratel.rs/upload/documents/Pregled_trzista/Pregled%20trzista_2016.pdf.

Regulatory Agency for Electronic Communications and Postal Services RATEL, can be found at stable internet address: http://www.ratel.rs/upload/documents/Pregled_trzista/Ratel%20Pregled%20trzista%202014.pdf.

Reliefweb Stable internet address: https://reliefweb.int/report/serbia/unhcr-serbia-update-6-12-november-2017.

„Softverska piraterija oštetila budžet za 72 miliona dolara“, Danas, 09.05.2008.; <http://www.danas.rs/vesti/ekonomija/softverska_piraterija_ostetila_budzet_za_72_miliona_dolara.4.html?news_id=92482> (May 10, 2009)

Spasić Ž. Vidoje, Autorska dela u digitalnom okruženju, Pravni fakultet u Nišu, Niš, 2011.

Stable Internet address : http://www.wipo.int/treaties/en/convention/trtdocs_wo029.html , 25.01.2014

Statista, stable Internet address: https://www.statista.com/topics/2802/serbia/.

Statistical Office of the Republic of Serbia**,** can be found at stable internet address: http://webrzs.statserb.sr.gov.yu/axd/drugastrana.php?Sifra=0018&izbor=odel&tab=152

Statistical Office of the Republic of Serbia, stable Internet address http://popis2011.stat.rs/?page_id=1221.

Statistical Office of the Republic of Serbia, stable Internet address http://popis2011.stat.rs/?page_id=1221

The National Security Agency/Central Security Service, USA, http://www.nsa.gov/index.shtml, last accessed on 13.03.2014

Documents

Act on Mutual Legal Assistance in Criminal Matters, “RS Official Gazette”, no. 20/2009

Berne Convention for the Protection of Literary and Artistic Works, text of the Convention is accessible on internet address: http://www.wipo.int/treaties/en/ip/berne/index.html last time accessed 25.01.2014.

Constitution of the Republic of Serbia, Official gazette RS, nr. 98/2006, available at. http://www.srbija.gov.rs/cinjenice_o_srbiji/ustav.php?change_lang=en

Convention Establishing the World Intellectual Property Organization signed in Stockholm 14. July 1967.

Convention establishing the world intellectual property organization, internet address: http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?doc_id=131054&file_id=190032#p50_1504 , last accessed 22.11.2020.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (ETS No.108, the 28 January 1981, Entry into force: 1.10.1985).

Convention on Cybercrime, Council of Europe, Budapest, 23. XI 2001.; European Treaty Series (ETS) - No. 185 <http://conventions.coe.int/Treaty/en/Treaties/Word/185.doc> (August 5, 2010)

Council of Europe, http://conventions.coe.int/Treaty/en/Treaties/Html/132.htm last accessed on 21.09.2014.

Criminal Code, “Off. Gazette of RS”, no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, Official Journal L 077 , 27/03/1996.

Law on Amendments to the Criminal Law of the Republic of Serbia, “ Off. Gazette of RS “, no. 39/2003

Law on Organization and Jurisdiction of Government Authorities in the fight against cyber crime, “RS Official Gazette”, no. 61/05 and 104/09

Law on protection of competiton: http://www.kzk.gov.rs/kzk/wp-content/uploads/2011/07/law-on-protection-of-competition2.pdf.

Law on ratification of Berne Convention for protection of literary and works of art, Official Gazette of SFRY, nr. 14/75 and Official Gazette of SFRY, – International treaties nr. 4/86.

Law on Ratification of the Convention on Cybercrime, “Official Gazette”, no. 19/2009

Law on ratification of *WIPO treaty of copyrights*, Official gazette of FRY – international contracts, nr. 13/2002.

Law on ratifying Convention of ILO no.182 of worst forms of child labour and ILO Recommendation no. 190 of prohibition and immediate action for the elimination of the worst forms of child labour. “Official gazette of RS – international treaties” no.08/03.

Law on ratifying of The Convention on the Rights of the Child, ”Official gazette of SFRY – International contracts”, no. 15/90

LCRR, Official gazette of RS nr. 104/2009, 99/2011 i 119/2012. Off. Gazette of RS", no. 85/2005, 88/2005 - corr., 107/2005 - corr., 72/2009, 111/2009 and 121/2012

Offences against the confidentiality, integrity and availability of computer data and systems, Title 1, Section 1, Chapter II, Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013)

Official gazette of RS, nr. 72/2011, 101/2011, 121/2012, 32/2013 i 45/2013.

Official gazette of RS, nr. 85/2005, 88/2005 - change, 107/2005 - change, 72/2009, 111/2009 and 121/2012

Official gazette of Federal Republic of Yugoslavia, br. 31/93

Official gazette of Republic of Serbia no. 44/2010, 60/2013 – Constitutional Court decision and no. 62/2014.

Official gazette of Republic of Serbia nr. 44/2010,

Official gazette of Republic of Serbia nr. 60/2013

Official Gazette of RS Nr. 42/09.

Official gazette of RS nr. 62/2014

Official Gazette of RS Nr. 65/2011.

Official Gazette of RS", no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013.

Official Gazette of RS, no. 61/05 and 104/09.

Official gazette of RS, nr. 24/2007, 31/2007, 38/2010.

Official gazette of RS, nr. 26/2008.

Official gazette of RS, nr. 50/2009.

Official gazette of RS, nr. 57/2004.

Official gazette of RS, nr. 113/2013.

Official gazette of RS, nr. 120/2004.

Official gazette of RS, nr. 127/2003.

Official gazette of RS, nr. 26/2008.

Official gazette of RS, nr. 41/2009 i 95/2013).

Official Gazette of RS, nr. 42/02, 97/04, 76/05, 79/05 - other Law 62/06, 85/06 and 41/09.

Official Gazette of RS, nr. 42/02, 97/04, 76/05, 79/05-second version, 62/06, 85/06 and 41/09.

Official gazette of RS, nr. 51/2009.

Official gazette of RS, nr. 83/2014.

Official gazette of RS, nr., 28/2009 i 47/2009.

Official gazette of RS", nr. 19/2009.

Official gazette of Socialist Federal Republic of Yugoslavia, br. 29/78, 39/85, 45/89 – Decision of Constitutional Court of SFRY and 57/89,

Official gazette of State Union of Serbia and Montenegro, br. 1/2003 – Constitutional charter.

Official Gazette RS - International treaties", Nr. 4/10.

Official Gazette RS - International treaties, Nr. 4/10

Procedural part of Convention: Articles. 14-22., Council of Europe, Convention on Cybercrime, ETS No. 185 – Explanatory Report; <http://www.conventions.coe.int/Treaty/en/Reports/Html/185.htm> (December 20, 2013).

Protection of Intellectual property in Serbia, internet address: http://www.scribd.com/doc/56780927/za-sitita-intelektualnesvojine, last accessed 20.02.2014.

The Code of Criminal Procedure, "Off. Gazette of RS", no. 72/2011, 101/2011, 121/2012, 32/2013 and 45/2013

The Law on Territorial Organization of the Republic of Serbia, *Official Gazette RS,* nr 129/2007

The Law on the Official Use language and alphabet, Official gazette *RS*, No. 45/91, 53/93, 67/93,48/94, 101/2005 and 30/2010.

The Law on the Official Use language and alphabet, Official gazette *RS*, br. 45/91, 53/93, 67/93,48/94, 101/2005 i 30/2010.