CHILDREN IN THE INTERNET: PROTECTION AND PARENTS' PERCEPTION

LJUBOJEV, N.; GLUSAC, D. & RADOSAV, D.

Abstract: *The authors of this paper are analyzing the legal frameworks relevant for the protection of children as Internet users in the Republic of Serbia. The need for further harmonization of national legislation with international trends in the field of child protection on the Internet is emphasized as well as with the obligations arising from international documents and the process of European integration. Although a significant progress in the protection of children on the Internet in the Republic of Serbia began with the process of harmonization of the national legislation with the European Union, the authors suggest further improvement of institutional and legal framework at both national and local levels. Accordingly, an interdisciplinary research including parents' perception on the necessity of protection of children on the Internet was carried out within this paper.*

Key words: *protection of children, Internet, information and communication technologies*

Authors´ data: Assoc. Prof. **Ljubojev**, N[adezda]*; Full Prof. **Glusac**, D[ragana]*, Full Prof. **Radosav**, D[ragica]*, *University of Novi Sad, Technical Faculty "Mihajlo Pupin" Zrenjanin, Djure Djakovica bb, Republic of Serbia, nadezdaljubojev@gmail.com,glusacdragana.zr@gmail.com, dolores023@open.telekom.rs

This Publication has to be referred as: Ljubojev, N[adezda]; Glusac, D[ragana] & Radosav, D[ragica] (2017). Children in the Internet: Protection and Parents' Perception, Chapter 09 in DAAAM International Scientific Book 2017, pp.105-120, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-12-9, ISSN 1726-9687, Vienna, Austria
DOI: 10.2507/daaam.scibook.2017.09

1. Introduction

Fast development of Information and Communication Technologies (ICT) has totally changed the world we live in, especially the world of children. Today, children at the same time represent a "digital generation", as well as a vulnerable group of the Internet users, who are facing potential risks. Nowadays, children start to use the Internet at an early age, accessing it via various devices (computers, tablets, mobile phones). (Karuovic at al., 2010) It is estimated that there will be 50 thousand new users between the age of 5 and 17 in the Republic of Serbia (RS) by the end 2017 (Children's Safety on the Internet, Report for Serbia, Telenor Group and the Boston Consulting Group). Research shows that younger children use the Internet for entertainment (playing games, listening to music, watching videos, series and movies), while the older ones mostly use social networks (Stevanovic at al., 2014).

A special attention is directed to the safety of children on social networks. In fact, four-fifths of the children aged between 10 and 18 have a profile on some of them (Popadic & Kuzmanovic, 2013). Facebook, Twitter and Myspace are only some of the most popular social networks in the RS. The main issue that follows the appearance and expansion of social networks is the *privacy* issue. The research shows that Facebook is most commonly used social networks and it also provides options for privacy protection, but the users in RS do not use them so often (Stevanovic at al., 2014). Research in Europe, by Livingstone at al. shows that social networks are very popular among children and adolescents in Europe. Moreover, it seems to be their favorite Internet activity, as 77% of children aged 13 – 16 and 38% children aged 9 – 12 have their profiles on social networks (Livingstone at al., 2011).

The fact is that children are often bigger experts than their parents in this field. (Glusac at al., 2015) On the one hand, parents tend to improve their children's educational perspective by using the Internet and, on the other hand, they are worried because of the risks that follow the use of the Internet and social networks (Livingstone & Bober, 2013). According to Livingstone & Haddon, the most important advantages of the Internet are the promotion of creativity and activism, inclusion into community, the availability of education and information, while the greatest risks are exposure to sexually explicit, offensive, violent, extremist and racist contents, commercial exploitation, manipulation and deception, an invasion of privacy and unwanted contacts (Livingstone & Haddon, 2008). Therefore, considering the value and educational potential of the Internet, which are probably not exploited enough, (Pardanjac at al., 2014; Cisar at al., 2010) the fact is that it is often being talked publicly about dangers and risks of using the Internet, in order to focus the attention on protecting and ensuring safe usage of these ways of communication.

However, the expansion of the Internet as a free IT space, unfortunately, opens another space where content circulates freely and carries potential risks for children. Whether those risks refer to the possibility of children getting in touch with unfamiliar people, to personal information abuse or other risks, there is a need for training everyone, and especially children and their parents, for using virtual space safely. But, not enough attention is paid to this issue in Serbian society, which is evidenced by a small number of organized educations on how to be safe on the Internet, especially

when it comes to the education of parents. That is why the data collected in the research based on this subject can have a great influence on recognizing the individual and social importance of this issue. It is essential to realize the amount of parents' perception on the safety of children on the Internet.In this regard, a part of the data from the research from 2016 is included in this work, and the sample of 83 parents of school children aged 11 – 15 from the narrower region of RS, Autonomus Province of Vojvodina (APV). Parents' perceptions about the necessity of protection of children on the Internet and the attitude of parents regarding the safety of their children on the Internet were examined, because the human factor cannot be singled out from this kind of relationship to the world where their children live and their eventual practical operations.

2. The Risks of Using the Internet for the Child

With the increasing availability of ICT and the increasing involvement of children in the world of communications and the Internet, the risks of their potential exposure to various inappropriate content (sexual, pornographic, violent), manipulation, abuse and exploitation are also increasing.The data point to the fact that the RS, in the true sense of the word, has become an information society.The introduction of Internet and mobile telephony has long passed 50% of the total population, and the use of the Internet at the daily level includes more than 75% of the internet population. Statistical data for the RS indicate that the presence of computer in households has increased from 55.2% to 64.4% in the period from 2012 to 2015.In the same period, the penetration of Internet in households was even more intense (from 47.5% to 63.8%), while in mobile phones, the situation in the RS is within the framework of European trends (85.8% in 2012, 91.4% in 2015) (Republic Institute for Statistics - Use of Information and Communication Technologies in RS, 2015).

Internet and mobile communications have become an indispensable part of the active time for many children aged 7 to 18 - within the households, in educational institutions, in peer groups, etc. Consequently, there are Internet risks, and the exposure of children to disturbing content is evident. All of the above data indicate that the population of children is in a modern, technological environment where their Internet access devices are readily available, either as part of the home or as part of their personal mobiles. Within this, it is a fact that almost 95% of households in RS with children at this age have some form of internet connection (UNICEF Study on the Level of Awareness of the Potential Risks and Internet Abuse among Parents of Children Aged 8 to 17 years, 2016). Moreover, he further emphasizes the potential exposure of this generation of Internet users to various forms of risk and danger.

Computer integration has many faces and forms: from internet, mobile phone, computer integrated manufacturing, e-technologies and many many others (Katalinic, 2010).

Nowadays, children are exposed to various risks in the cyberspace: child pornography, child trafficking (McCABE, 2008), cyber-bullying and other risks for children in ICT. However, given that exploiting and abusing children for pornographic purposes, as well as data privacy, have been recognized as main risks of children using

the Internet, the work of entities that are dealing with other risks on the Internet has been marginalized (Sapic, 2016). Jenkins, 2001, points a police action "Armagedon" in which at the end of 2011 eighteen people suspected of buying sexual abuse of children were arrested in Serbia (Jenkins, 2001). Police authorities of the Ministry of Internal Affairs of the Republic of Serbia (MIA RS) and the Department for Cybercrime were involved in the international police operation "Delego", during which a person from Novi Sad, who was found with 10 gigabytes of child pornography, was arrested (Sapic, 2016).

However, risky behavior on the Internet also includes other risks for the children on the internet and social networks. For example, with the development of the Internet and social networks, addiction develops due to the increased time spent on the Internet (Kiesler, 1997). In a relatively short period, the Internet has become the most popular media among children. They gain excellent IT knowledge at an early age and because of that they are prone to the influence of this new media.It is also troubling that the children Internet users entrust their personal information to strangers. The risk of violating privacy is obvious, considering the anonymity of the Internet. The fact is that, by taking part in the Internet communities and even by searching the Internet, every user loses his privacy to a certain extent. Whereby the children are more likely to disclose their personal information. According to the research, even 31.1% of boys and 27% of girls aged from 9 to 15, point out that they shared their personal data on the Internet (e-mail address, phone number and even their home address) (Dowell at al., 2009). Potential consequence of revealing personal information on the Internet can lead to unwanted contacts out of the network, which can bring a child in physical danger. Also, social networks could be used for violence promotion.

When it comes to the category of the risky contact, it is important to point out that „cyber-bullying“, i.e. harassment and bullying on the Internet, deserves a special attention because of negative consequences that it has on the individual, its emotional and social functioning. Cyber-bullying exists when a person or a group of people uses the Internet, mobile phones, online games, social networks or any other form of ICT in order to threaten, harass or humiliate another person. Based on the knowledge of experts in this field, it is the fact that this type of bullying can also happen in contact with peers and school friends and that is why it is harder to control this type of risk on the Internet by using Internet filters. According to the official statistics of the National Crime Prevention Council in USA, half of the American teenagers are victims of cyber-bullying, while the research also shows that 81% of them consider it amusing.Therefore, representatives of the European Commission and 17 social networks (including Facebook, Myspace, etc.) signed a contract according to which they will protect children from cyber-bullying and violence on the Internet together. In the USA, governors of 49 American states signed a contract about child protection with social networks (Ruzic, 2011). This measure is understandable because cyber-bullying is happening often via social networks. Another type of risky contact is sexual harassment on the Internet, which has become more common with the appearance of web cameras and programs for instant messages (Mitchell at al., 2003). With the advent of social networks, which enable sharing photos, videos and texts, the risk of this type of contact has been increasing. Apart from cyber-bullying, the exploitation of children

on the Internet, i.e. the exploitation via ICT, which implies exploitation, violence, abuse and molestation of children by adults or peers, includes sharing indecent content with children, recruiting children for illegal activities, e.g. grooming, sexting and other types of violent behavior which threaten the children's rights. Grooming is a process in which children are persuaded or encouraged to participate in interactions of sexual content via the Internet or phone devices, whereby they are exposed to unwanted pornographic contents. In Akdeniz's theory, in 2008, however, in the 1990s, the development of a worldwide Internet network, apart from a number of benefits it provided to users, set this medium as a key variable through which sexual abuse of children emerged beyond the "traditional" criminality, with the demands of radical modification of techniques of suppression and prevention (Akdeniz, 2008). Author Stanic, 2008, points to the increasingly frequent abuse of mobile phones, which in line with the growing technical performance have an increasingly serious role in the distribution of child pornography (Stanic, 2008). And author Moore considers that the phenomenon of distribution of amateur photographs and video materials in SMS or MMS messages, so called, sexting, which becomes a common and popular phenomenon among the teenage population (Moore, 2010). Sexting represents sending disturbing contents (explicit texts, photos, videos) via ICT to another person (most frequently via SMS, MMS, e-mail, Facebook, Myspace and other social networks and chat-rooms). Based on the research carried out by the Provincial Ombudsman, data were received from the police departments (PD) in APV, i.e. from the police stations on their territory, about the number of reported, denied and processed cases during 2011 and 2012. The data shows that two cases of child exploitation on the Internet were reported on the territory of PD Zrenjanin. One case was about cyber-bullying, wherein perpetrators were children, and the other case referred to sexting (Exploitation of Children on the Internet: Research Report of the Provincial Ombudsman).

While in the world, and especially in the EU, research on Internet risks related to children and their protection on the Internet are very numerous and frequent, the first more systematic research of this type related to children in the RS was realized in 2012, at the Institute for Psychology University in Belgrade with the support of UNICEF and Telenor.The research was based on a survey and it included 34 schools (17 elementary and 17 high schools), i.e. 3786 pupils, 3078 parents and 1379 teachers. Women were more prevalent among parents and teachers. According to the survey data collected, 62% of older elementary school pupils and 84% of high school students were exposed to risks in cyber space in 2012 (Popadic & Kuzmanovic, 2013). Based on this research, it was determined that the most widespread risks are: accepting friend requests from strangers (43% of elementary pupils, 71% of high school students), sharing personal information on profiles (29% of elementary pupils, 39% of high school students) and responding to messages from strangers who want to get in touch with the child (27% of elementary pupils, 47% of high school students). It can also be noticed a higher readiness of older children to meet in person with the people that they get to know on the Internet. During 2014 and the first half of 2015, the Net Patrol, an online mechanism for reporting digital violence within the Safe Internet Centre Serbia, received 1690 reports for abuse and harmful contents for children which were forwarded to the Department for Cybercrime within the Ministry of Internal Affairs of

the Republic of Serbia and to INHOPE, an International Association of Internet Hotlines, for further investigation and treatment (The Center for Safe Internet Serbia, Work Report 2014-2015, Child Safety on the Internet in Serbia).Thereby, most of the reports sent to the Net Patrol by users, refered to the web pages that are not registered in Serbia.Apart from Net Patrol, all sorts of digital violence could be reported at the Provincial Ombudsman website.

Thus the Internet can be a potentially unsafe space. Risks for children on the Internet are getting more diverse, and more frequent in modern society. Therefore, they are necessary adequate and efficient measures of prevention and child protection and because of that, numerous legal acts and regulations have been adopted, both within the international law and national legislation. Parents, as the most important factor in education of children, need to be aware of the children's behavior on the Internet, so they could ensure the benefits of its usage.

3. Legal Aspects of Child Protection on the Internet in the Republic of Serbia

By enacting the Law on the Ratification of the UN Convention on the Rights of the Child ("Official Gazette of SFRY - International Agreements ", No. 5/90 and" Official Gazette of the FRY - International Treaties ", No. 4/96 i 2/97), RS committed itself to taking measures to prevent and ensure the protection of children from all forms of domestic violence, institutions and the broader social environment.The Convention on the Rights of the Child (CRC) was adopted on 20 November 1989, by the Resolution 44/25 of the United Nations General Assembly. To date, the CRC has 194 States Parties, making it one of the most widely ratified international treaties.The CRC is the first international legal document which contains the catalog of all the children's rights. Article 1 of the CRC defines "child" as any person "below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." Importantly, the CRC leaves open the option for States to adopt lower or higher ages of majority, thus giving States Parties some leeway in defining childhood. By the Article 19 CRC, it is prescribed that member states have to undertake all the adequate legislative, administrative, social and educational measures, in order to protect the child from all forms of physical and mental violence, violation or abuse, neglecting or careless attitude, bullying and exploitation, as well as from sexual abuse, while the child is in care of parents, legal guardians or any other person responsible for the child.CRC prescribes all member states are bound to protect the child from all forms of sexual exploitation and sexual abuse (Article 34 CRC).

The RS is a signatory to two European Council conventions: Convention on Cybercrime (adopted in Budapest in 2001) and Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) which regulates the prevention and fight against sexual exploitation and sexual abuse of children, protection of the rights of children who have become victims of sexual exploitation and sexual abuse, as well as the promotion of national and international cooperation in the fight against sexual exploitation and sexual abuse of children**.**The Lanzarote Convention came into force in 2010 and RS, by its ratification at the same year, became a contracting state, which means it has overtaken very clear obligations in

implementing the Convention and in overall child protection from all forms of sexual exploitation.The Convention on Cybercrime from 2001 represents the first international document where child pornography and computer systems are explicitly associated. Among other things, its importanceis alsoin creating special state authorities specialized for fighting against cybercrime. After the ratification of the Convention on Cybercrime and the Additional Protocol, in RS, ("Official Gazette of RS", No.19/2009) there were renewed the Criminal Procedure Code ("Official Gazette of RS", No. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013 i 55/2014) the Law on Organization and Jurisdiction of the Government Authorities in Suppression of Cybercrime ("Official Gazette of RS", No.61/2005 i 104/2009) and the Criminal Code (CC) ("Official Gazette of RS", No. 85/2005, 88/2005 - 107/2005 - 72/2009, 111/2009, 121/2012, 104/2013, 108/2014) The Special Prosecutor's Office for Combating High-Tech Crime (Special Prosecutor's Office) was established by the Law on Organization and Competence of State Authorities for Combating High-Tech Crime from 2005. In particular, the Prosecutor's Office is responsible for the prosecution of perpetrators of criminal offenses of high-tech crime and it is competent to act on the entire territory of the RS. Pursuant to the provisions of this law, the High Court in Belgrade for the territory of the RS is competent for dealing with high-tech crimes, while the second instance court is in charge of the Appellate Court in Belgrade. Also, by the provision of the Law on Organization and Jurisdiction of State Authorities for Combating High-Tech Crime, within the Ministry of the Interior, a High-Tech Crimes Service has been established, which acts on the orders of the Special Prosecutor. However, after adopting the Law on Information Security (LIS) ("Official Gazette of RS", No. 6/2016) jurisdiction of these authorities should be expanded according to its provisions. In RS, people from all social structures act as perpetrators of these criminal acts, so a single profile of the offender cannot be created (Sapic, 2013).

One of the relevant documents for protecting children from violence is the General Protocol on Protection of Children from Abuse and Neglect, which was adopted by the Government of the Republic of Serbia. However, there is no law in RS that regulates the safety of children on the Internet specifically, although according to changes in the CC, article 185 b, stipulates that it is a criminal act “using computer network or communicating via other technical means, in order to commit sexual assaults against minors”. The one who is intended to commit a crime of: Raping (Article 178, paragraph 4), Sexual intercourse with a helpless person (Article 189, paragraph 3), Sexual intercourse with a child (Article 180, paragraphs 1 and 2), Sexual intercourse by abuse of position (Article 181, paragraphs 2 and 3), Illicit sexual acts (Article 182, paragraph 1), Procuring or enabling sexual intercourse (Article 183, paragraph 2), Facilitating prostitution (Article 184, paragraph 3), Dissimulating, obtaining and owning pornographic material and exploiting children for pornography (Article 185, paragraph 2) and Persuading minors to witness sexual intercourse (Article 185 a) use computer network or communicate via other technical means, in order to settle a meeting with a minor and actually show at the agreed place, will be punishedfrom six months to five years in prison. If this act was committed against a child, the prison sentence would be from one to eight years (Article 185). If this act was committed against a child, the prison sentence would be from one to eight years.

The most important change is that the CC, for the first time, considers as a criminal act owning and obtaining photos, audio-visual recordings or other items of pornographic content created by exploiting minors.In RS, the Decree on the Safety of Children was adopted in the use of ICT (Regulation), on the basis of which the National Contact Center for Child Safety was established on the Internet. The Decree is in accordance with the Law on the ratification of the United Nations Convention on the Rights of the Child, the General Protocol of the Government of Serbia for the Protection of Children against Ill-treatment and Neglect, and the EU Strategy for a Better Internet for Children in 2012.

In the National Youth Strategy for the period from 2015 to 2025, it is stated that the development of security culture (including cyber as well) is one of the strategic goals.However, this only refers to the children older than fifteen. At the beginning of 2016, in the RS was adopted the LIS, Body for the Coordination of Information Security (Body for Coordination) and a work group for writing the Strategy for the Development of Information Security, so there was created a space for improving legal and institutional framework. However, LIS refers only to legal entities and it is predicted that its numerous issues would be regulated by subordinate legislation. When LIS was adopted, it had all started from the need to improve legal and institutional framework for the information security and the need to increase the level of awareness in citizens about incidents and risks in cyberspace. LIS predicts founding of the National Centre for Prevention of Safety Risks in ICT systems (Computer Emergency Response Team (CERT).The National CERT received authority over collecting information, classifying information about incidents and risks, raising public awareness and cooperation with public and business entities (Article 15). It is also necessary that children are recognized as a vulnerable group in the Strategy for the Development of Information Security and that the special working groups, that will be formed within the Body for Coordination, carry out the evaluation of former projects. In theory, this is considered to be a precondition for formulating a unique approach to the issue of children's exposure to safety risks on the Internet and for creating a coordinated national campaign, which should contribute to the raising of knowledge of children, parents, guardians and teaching staff about safe ways of using the Internet (Sapic, 2013).

The problem of protecting children on the Internet is covered by the US and EU countries. Given that the United States had the largest number of users on the Internet, it was this country that began its work on protecting children on the Internet through legal regulations in 1996 (Kleinhans, 2004). After several failed attempts to restrict children's access to harmful information on the Internet, the US Congress passed the Children's Internet Protection Act (CIPA), which concerned schools and libraries. According to CIPA schools and libraries must take care of the safety of children on the Internet. CIPA includes security measures against the visual display of incompetence, child pornography and childbearing material (Chih, 2003). Today, almost all EU countries have filters installed in computers to prevent children from accessing pornographic sites. The EU has also advocated controlling illegal activities on the Internet by increasing the number of Internet users. Thus, the Council of Europe has proposed to European countries to ratify the Convention on the fight against cyber

crime. Article 9 of this Convention refers specifically to offenses related to child pornography.With the Decision of the European Parliament 854/2005/EC of 2005, the Internet Safe Plus program was launched, which aims to ensure the safe use of the Internet and new technologies, especially for children. In Germany, the Bundestag has passed a law allowing providers to block sites with child pornography.The identical laws were adopted in Great Britain, Italy. The Recommendation of the Committee of Ministers of the Council of Europe (2001) 16 on the protection of children against sexual exploitation has recognized that advertisements and the media, in particular the Internet, play a major role both in dissemination and in preventing the occurrence of sexual exploitation of children. The recommendation refers to the establishment of a national mechanism to provide regular information on best practices and the most effective measures to prevent sexual exploitation of children. A special section refers to the Internet and states that it is necessary to include internet providers in raising awareness of sexual exploitation through the use of ICT and its risks, especially on the Internet. The Resolution of the Parliamentary Assembly of the Council of Europe 1307 (2002) on sexual exploitation of children points to the problem of sexual abuse of children, which is deteriorating with the emergence of the Internet, due to the fact that it provides anonymity and ease of use, as well as the fact that the way of establishing contacts is unlimited. The Assembly requests each Member State to provide funds for the fight against crime through computers, in particular child pornography, and in order to establish a personnel and technically equipped police unit consisting of persons trained in the field of children's rights and ICT. At the same time, cooperation with national and international Internet experts needs to be improved in order to develop appropriate technical and legal means to protect children from illegal and harmful content related to sexual exploitation.

South East Europe countries joined in the fight against cyber crime by adopting a joint statement in Ljubljana in 2002. Subsequently, in Belgrade the same year, at the International Conference on Telecommunication Development, the representatives of the governments of the member states signed the "eSEE Agenda+ for The Development of Information Society in SEE 2007-2012" - Stability Pact, Electronic South Eastern Europe Initiative "eSEE". Among other things, the signatories of the Agenda commit themselves to combating illegal content, spam, increasing the number of Internet users in their countries, allowing access to the Internet in schools and public institutions. In the countries of Southeast Europe, the document "Initiative for the Development of the Information Society 2007-2012" was adopted.

The harmonization of the RS legislation with the European is in progress, within the process of accession of the RS to the EU. In the context of accession negotiations with the EU, cyber-related issues were mainly in Chapter 24: Justice, Freedom and Security. A report on the European Commission's Coverage of Chapter 24 of May 2014 stresses that the fight against cyber crime in the RS is at an *early stage*. It has also been established that the RS has established a special service responsible for combating high-tech crime within the Ministry of Interior, as well as the Special Prosecutor's Office for the Fight against High-Tech Crime, ratified the Council of Europe Convention on High-Tech Crime and largely aligned with the EU Directive on attacks on information Systems. In addition, it was concluded that further amendments to the

regulations are necessary in order to fully align with the EU acquis in the area of combating cybercrime.

4. Parents as Entities of Protecting Children on the Internet

When it comes to children, the role of parents in the safe use of the Internet and Internet content is significant.The research of the Institute for Psychology University of Belgrade 2012 showed that children are aware of the fact that there are ways to protect their privacy on Internet, which should serve as a base for further steps (Popadic & Kuzmanovic, 2013).The same research indicated that girls and older pupils are more interested in learning about the ways of protection on the Internet, comparing to the boys and younger pupils. There was also identified a lack of awareness of parents and teaching staff about concrete measures of prevention and protection from the risks.

Research in both the world and RS indicates the importance of parents in creating an appropriate environment for good "digital" development of children. As much as it is the true conclusion of many authors that children have much more advanced IT skills and knowledge in this area, it is so true that parental, life experience is an invaluable resource that can help children's digital skills and knowledge in a good, safer way. Namely, a noteworthy study by the Belgrade Institute of Psychology found that almost 65% of parents of children aged 8 to 17 believe that internet and mobile communications are an unsafe and dangerous place for their children (Popadic at al, 2016). In the same research, although almost 73% of parents consider that they have the competence and knowledge to respond adequately to dangerous and risky situations, this is not absolute (UNICEF Study on the Level of Awareness of the Potential Risks and Internet Abuse among Parents of Children Aged 8 to 17 years, 2016). In addition, slightly more than 50% of parents consider themselves sufficiently, but not absolutely able to provide help and support to their child in such "crisis" Internet situations. Only slightly more than 50% of parents of children at this age use some of the mechanisms for monitoring and controlling internet content and mobile communications that their children use (UNICEF Study on the Level of Awareness of the Potential Risks and Internet Abuse among Parents of Children Aged 8 to 17 years, 2016).The survey shows that most of this control is done mainly on the basis of elementary forms of monitoring, viewing and analyzing the content of child communication in different forms and forms of internet and mobile communications. Considering that previous research in this field has shown that parents' awareness of the need for internet protection of their children at a low level, it was expected that in the last 5 years there was a higher level of internet competence of the parent population, and that due to the increase of the media and the general social significance of the topic also influenced the change of the parents' awareness as a target group, which would significantly change the attitude of the parents towards this topic and partly influence their behavior, but this did not happen.

Although it is considered that insufficiently defined space for public-private partnership is a serious flaw in the existing legal framework, (Abusara, 2013) the only comprehensive public-private partnership exists in the form of the Safer Internet Center and the campaign “Click Safely” which involves the competent ministry, telecom

operators and other actors, as well as the Foundation Fund B92, in the project for reporting illegal and harmful online content (Rizmal at al., 2006). Within the campaign "Click Safely", which is being carried out by the competent ministry under the name "Think Before You Post", trainings for the teaching staff, pedagogical-psychological services and parents' councils were organized in all schools in RS. Mid-2010, the company Telenor Serbia signed an agreement with the MIA RS about the strategic cooperation, with the goal to install filters for blocking access to illegal websites with elements of sexual abuse of children. In 2009, the Ministry of Telecommunications and Information Society, within its jurisdiction, took the initiative for improving the safety of children on the Internet in the form of the previously mentioned project of starting the website "Click Safely", where children and parents could find different informational, educational and entertaining contents, from which they could learn something more about the safe use of the Internet.

5. Methodology and Research Results

In order to measure the attitudes of parents in the narrower area of Serbia, Autonomus Province of Vojvodina, a research has been conducted for the purpose of researching the perception of parents regarding the safety of their children on the Internet, as well as the need for implementing measures for the protection of children on the Internet.The research goal is to establish the opinions and behavior of the parents in context of the new life environment for their children, and to be aware of the necessity of their own personal involvement in it, in order to prevent its negative effects. The quantitative method which was used to carry out the research is a survey in a narrowsense, about attitudes and opinions of the examinees' parents. Conducting of this quantitative research enabled precise measuring and quantifying of the relevant indicators.The value of this survey is limited because the information received in it depends on honesty of the examinees' parents and their ability to answer fairly to the questions asked. It is possible that the survey method is subject to epistemological and social limitations, in the sense that the examinees do not answer how they really mean, but according to the social values or their unawareness of the matter. That is why a survey is considered only as one of the phases in the research process, without neglecting other aspects of the research. The information collection technique is an indirect survey, or a questionnaire in paper.

The parents were asked what activities their child is doing online, how much time they spend on a computer, and whether they know what the child is doing specifically, and whether they consider if some of these activities are risky. We were interested in our parents' views on whether they felt they were sufficiently instructed in the ways of safe use of the Internet and whether they felt they needed institutionalized support to protect their child. Also, parents were asked if they knew the legal and institutional framework for protecting their children on the Internet.

The questions were closed-ended with the simplest form of YES/NO answers, as well as with one or more offered answers. There was also given a possibility to write additional answers which were not offered, but a parent found them true.

In this interdisciplinary research, experts in the field of legal and ICT sciences were involved, but the research showed that there is a need to involve other experts, for example in pedagogical science, which would expand research. In this sense, it is important to have an insight into the perception of parents about the need to protect children on the Internet, but also how much parents are able to adequately control the behavior of children on the Internet and social networks, whereby the control, "in the broadest sense, can be operationalized as a process of monitoring and directing / regulating children's behavior and activities" (Stattin & Kerr, 2000). This process is related to the active search of the parents for information on children's activities and the establishment of clear rules of behavior that should be the basis for safe Use of the Internet (Zukovic & Slijepcevic, 2015).

The part of research was also shown in (Glusac at al., 2017) indicated that parents allocated their "conventional and usual social fears and concerns in a new, unknown cyberspace". Simply put, the impression is that parents just moved their familiar and traditional fears to the one, relatively new and, to them, insufficiently familiar context, as it was detected in the research carried out by UNICEF in 2016, about the level of awareness, potential internet risks and misuse among the parents of children aged between 8 and 17. Parents expressed concern that their children are threatened on the Internet and that they need help in this field.

In addition to these indicators, it is an interesting part of the questionnaire that asked parents whether they were aware of any inconveniences that their children had experienced on the Internet. 8 types of experiences were offered: getting to know unknown people live, viewing pictures of sexual content, viewing images of aggressive content, experiencing insulting and degrading, insulting or abusing the child, misusing personal data, unplanned cash expense. A huge percentage of parents (as much as 57%) said that they do not know if their child experienced an unpleasant experience on the Internet, and 20% did not experience any child's inconvenience. 23% of them shyly chose one of the options that their child had unpleasant experiences on the Internet, and only one parent linked this testimony with the next one, asking for a statement about the unpleasant consequences of violence on the Internet over their children, that is, the child was upset after an experience. Here we have obvious confusion and lack of knowledge of parents about the activities their child is experiencing. In the survey, the majority decided to use the help the school would provide mostly in terms of educating parents, but also worry about massive answers from parents who consider that they do not need training because they do not want to interfere with the "child job", that everything is a game, a harmlessness, and that inconveniences happens "there to someone far away, not exactly to us". This attitude is worrying, and it even more points to the need for an institutionally organized and mandatory training of parents about the dangers on the Internet and the necessity of their involvement. What surprised, however, is the dominance of parents' responses that they do not "interfere" with the activities of their children on the Internet at the moment, or that they do not undertake concrete activities to protect their child (55%). Only 11% of them check that the child behaves on the Internet, and as many as 48% say that they do not know if they are able to help their child to protect himself from Internet dangers. The obtained results showed

that most parents are not familiar with the legal and institutional framework for protecting their children on the Internet.

We conclude that the vast majority of parents is confused i.e. uninformed about the ways of protecting children and the fact they need institutional help for it.

6. Conclusion

National legislation should also regulate the protection of children on the Internet as vulnerable groups in the new security area. Also, it is important to include child protection on the Internet in the future Strategy for Development of Information Security of the RS, which would lead to the strengthening of the legal framework and the capacity of institutions that deal with children. There is no national or national law that regulates the safety of children on the Internet specifically, but the changes of the Criminal Code from 2003 defined that exploiting the computer network or communicating with other technical means for the commission of criminal offenses against sexual freedom against a minor person (Article 185 b) is defined as a criminal offense punishable by law. The shift was made by the adoption of the Decree on the Safety of Children in the use of ICT, on the basis of which the National Contact Center for Child Safety was established on the Internet.

In domestic regulation and strategic framework, computer systems and ICT are mentioned only as a medium, i.e. the way for sexual exploitation of children. Thus, the competent executive bodies approach this topic primarily from the criminological point of view, and are more focused on the treatment of this problem of punishing perpetrators of the criminal offense of sexual exploitation of children who have also used ICT and suppressing this phenomenon after it has already happened, rather than its prevention by informing children and parents and educating on proper use of ICT and appropriate preventive care. Cyber bullying, characteristic for more and more frequent peer violence through ICT among children, as well as grooming and sexting, are not recognized in any way as individual types of violence against children through ICT. These types of electronic violence are important in legal regulation for two reasons: that systematic information and education of children and their prevention can be done, but also that their direct and indirect victims could be provided with adequate assistance and protection. In this regard, in order to prevent and protect against violence against children through ICT, it is necessary to improve the existing legal framework and positive legal regulations of the RS implement obligations from the accepted international treaties that the RS has entered into, as well as to further align the legal system of the RS with EU acquis in this area.

When it comes to children, the role of parents in the safe use of the Internet and Internet content is significant. In order to measure the attitudes of parents in the narrower area of RS, APV, a research has been conducted for the purpose of researching the perception of parents regarding the safety of their children on the Internet, as well as the need for implementing measures for the protection of children on the Internet.We conclude that the vast majority of parents is confused i.e. uninformed about the ways of protecting children and the fact they need institutional help for it.

The research confirmed the need for more interdisciplinary research in this field. It has also showed the benefits and challenges of close cooperation of legal professionals and ICT experts.

7. References

Abusara, A. (2014). A comprehensive cyber awareness campaign – a 'Prequel' to strong and lasting cybersecurity PPP in Serbia. pp. 4.

Akdeniz, Y. (2008).Internet child pornography and the law: national and international responses. UK: University of Leeds.

Cisar, S. M. Radosav, D. Markoski, B. Pinter, R. Cisar, P. (2010) Computer Adaptive Testing of Student Knowledge, Acta Politecnica Hungarica,Vol.7, No.4, pp.139-153.

Chih, W. (2003). Internet censorship in the United States stumbling blocks to the information age, IFLA Journal, 29 (2,4,5).

Convention on the Rights of the Child. New York, 20 November 1989. United Nations, Treaty Series, Vol. 1577.

Dowell, E.; Burgess, A. & Cavanaugh, D. (2009). Clustering of Internet risk behaviors in a middle school student population. Journal of School Health, Vol. 79, No. 11, pp. 547-553.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems replacing Council Framework Decision 2005/222/JHA. 14.8.2013. L 218/8.

Eksploatacije dece na internetu: izveštaj o istraživanju Pokrajinskog ombudsmana, (2013). Pokrajinski ombudsman, Futura, Novi Sad. Exploitation of Children on the Internet: Research Report of the Provincial Ombudsman, (2013). Provincial Ombudsman, Futura, Novi Sad.

Glusac D.; R Makitan V.; Radosav D. & Milanov D. (2015) Adolescents' informal computer usage and their expectations of ICT in teaching - Case study: Serbia, Computers & Education, Vol. 81, pp. 133-142.

Glusac, D.; Ljubojev& N. Radosav, D. (2017). Parents' perception of the needs for implementing measures for child protection on the Internet, Proceedings of International Conference of Information Technology and Development of Education VIII (ITRO 2017), Zrenjanin, Serbia, June 22, 2017.

Jenkins, P. (2001). Beyond Tolerance: Child Pornography on the Internet, New York.

Katalinic, B. (2010). Engineers For Knowledge Based Society, Annals of DAAAM for 2010 & Proceedings of the 21st International DAAAM Symposium, Katalinic, B. (Ed.), ISSN 1726-9679, Vienna, Austria, EU, 2010, Vol. 21, No. 1, Published by DAAAM International.

Karuovic D., Radosav D., Glusac D., (2010). Educational Game Model for Pre-School Children, Chapter 12 in DAAAM International Scientific Book 2010, pp. 107-116, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-74-2, ISSN 1726-9687, Vienna, Austria.

Kiesler, S. (ed) (1997). Culture of the Internet, Mahwah, Nj: Lawrence Erlbaum Associates. 463 pp. ISBN 0 8058 1635 6.
Kleinhans, Ch. (2004). Virtual child porn: the law and the semiotics of the image, Journal of Visual Culture, Vol. 3. No 1.
Livingstone, S. & Haddon, L. (2008). Risky experiences for children online: Charting European research on children and the Internet. Children & Society, Vol. 22, No. 4, pp. 314-323.
Livingstone, S.; Olafsson, K. & Staksrud, E. (2011). Social networking, age and privacy. EU Kids Online, London.
Livingstone, S. & Bober, M. (2013). Regulating the Internet at home: contrasting the perspective of children and parents. In: Digital Generations: Children, Young People, and the New Media, D. Buckingham and R. Willett (Ed.), pp. 93-113, Routledge, New York.
McCABE, K. (2008).The role of Internet service providers in cases of child pornograph and child prostitution, Social Science Computer Review, Vol. 26, No. 2.
Mitchell, K.; Finkelhor, D &Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact and prevention. Youth & Society, Vol. 34, No. 3, pp. 330-358.
Moore, R. (2010). Cybercrime: Investigating High-Technology Computer Crime. Elsevier, New York.
National Crime Prevention Council URL, Available from:http://www.ncpc.org/newsroom/current-campaigns/Cyberbullying. Accessed:2.07.2017.
Pardanjac, M.; Eleven, E & Kaurovic, D. (2014). Increase of User Motivation in Teaching Realized Through Distance Learning, Chapter 10 in DAAAM International Scientific Book 2014, pp.131-144, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-98-8, ISSN 1726-9687, Vienna, Austria.
Popadic D & Kuzmanovic D. (2013). Korišćenje digitalne tehnologije, rizici i zastupljenost digitalnog nasilja među učenicima u Srbiji, UNICEF/Institut za psihologiju Filozofskog fakulteta Univerziteta u Beogradu. Popadic,D& Kuzmanovic D. (2013). The use of digital technology, the risks and the representation of digital violence among students in Serbia, UNICEF/Institute of Psychology, Faculty of Philosophy, University of Belgrade.
Popadic, D., Pavlovic, Z., Petrovic, D. & Kuzmanovic, D. (2016) *Global kids online Serbia: Balancing between Opportunities and Risks. Results from the Pilot Study*, Belgrade: University of Belgrade. Available from: www.globalkidsonline/serbia.
Rizmal, I.; Radunovic, V. & Krivokapic, DJ. (2015).Vodič kroz informacionu bezbednost u Republici Srbiji", Centar za evroatlantske studije – CEAS, Misija OEBS-a u Srbiji, Grid studio, Rizmal, I.; Radunovic, V. & Krivokapic, DJ. (2015). Information Security Guide in the Republic of Serbia ", Center for Euro-Atlantic Studies - CEAS, OSCE Mission in Serbia, Grid studio, Available from: http://www.osce.org/sr/serbia/272206?download=true. Accessed:12.09.2017.

Republic Institute for Statistics (2015). - Use of Information and Communication Technologies in RS.
Ruzic, N. (2011). Zaštita djece na Internetu, Nova prisutnost, Vol. 9, No. 1, pp. 155-169. Ruzic, N. (2011). Protection of children on the Internet, New Presence, Vol. 9, No. 1, pp. 155-169.
Sapic J. (2016). Bezbednost dece na internetu u Srbiji: Izloženost bez koordinisane zaštite, Centar za istaživanje javnih politika. Sapic, J. (2016). Child Safety on the Internet in Serbia: Exposure without coordinated care, Center for Public Policy Research.
Stevanovic, M.; Mitovski, A.; Zivkovic, D.; Strbac, N.; Zivkovic, S.; Mladenovic A. & Vaskovic S. (2014). Internet navike dece školskog uzrasta u nekim selima borske opštine, Sinteza, Singidunum University, Beograd, pp. 354. M. Stevanovic, A. Mitovski, D. Zivkovic, N. Strbac, S. Zivkovic, A. Mladenovic, S. Vaskovic, (2014). Internet habits of school children in some villages of Bor Municipality, International Conference Synthesis, Singidunum University, Belgrade, pp. 354.
Stattin H. & Kerr, M. (2000). Parental Monitoring: a reinterpretation, Child Development, Vol. 71, No. 4, pp. 1072-1085.
Stanic, I. (2008). Djecja pornografija. Pedagoška stvarnost, 3-4, pp. 324-346. Stanic, I. (2008). Child pornography. Pedagogical Reality, 3-4, pp. 324-346.
The Center for Safe Internet Serbia, Work Report (2014-2015), pp. 7. Child Safety on the Internet in Serbia.
UNICEF Study on the Level of Awareness of the Potential Risks and Internet Abuse among Parents of Children Aged 8 to 17 years, (2016). Ipsos.
Zukovic, S. Slijepcevic, S. (2015). Roditeljska kontrola ponašanja dece na internetu i socijalnim mrežama, Nastava i vaspitanje, br. 2. pp.239-254. Zukovic, S. Slijapcevic, S. (2015). Parental control the behavior of children on the Internet and social networks, Teaching and Upbringing, Vol. 64, No. 2, pp. 3.
Akcioni plan za sprovođenje prioriteta iz "eSEE Agenda+ za razvoj informacionog društva u Jugoistočnoj Evropi za period 2007-2012." ("Službeni glasnik RS", broj 29/09). Action Plan for Implementation of the Priorities from the "eSEE Agenda + for the Development of the Information Society in South East Europe for the period 2007-2012" ("Official Gazette of the Republic of Serbia", No. 29/09).
*** http://www.bezbednost.org/upload/document/akcioni_plan_za_poglavlje_24_-_mart_2016_.pdf., Accessed:10.10.2017.