INTERNET CHILD EXPLOITATION

Regional Report
April 2013
Save the Children is the world’s leading independent organisation for children.

**OUR VISION** is a world in which every child attains the right to survival, protection, development and participation.

**OUR MISSION** is to inspire breakthroughs in the way the world treats children, and to achieve immediate and lasting change in their lives.

In memory of all children who suffered from exploitation over the internet, to all the people who protect them, to all children.

© Save the Children 2013
Author: Save the Children
Project Leader: Ljiljana Siničković
Consultant: Tommaso Diegoli
Graphic Design: Arch Design

This publication was produced within the Project of Prevention of Exploitation of Children in South East Europe the implementation of which was supported by the Ministry of Foreign Affairs of the Kingdom of Norway.

Research was conducted in cooperation with the members of the network of Ombudsman for Children of South-East Europe: Provincial Ombudsman of the Autonomous Province of Vojvodina, Ombudsman for Children of the Republika Srpska and Ombudsman of the Republic of Montenegro.
## Contents

### INTRODUCTION

3

### METHODOLOGY

4

- Background, Topic and Territorial Span 4
- Rationale 4
- Goals, Objectives, Structure 4
- Data Collection Methods and Sources of Information 5

### DEFINITIONS OF KEY CONCEPTS

8

### 1. LEGISLATION AND IMPLEMENTATION

9

- International Standards in Child Protection from Exploitation via ICT – Overview of Relevant Documents 10
- National Legislation and Implementation, Existing Mechanisms and Procedures for Protection – Overview of Relevant Documents 14
- Child Protection Regulations Adopted by ICT Companies – Overview of Relevant Documents 16

### 2. UNDERSTANDING THE PHENOMENON

18

- Experiences and Perceptions of Children Concerning Exploitation Via ICT: Opportunities and Risks 18
  - Experiences and Perceptions of Children Aged 10 to 13 19
  - Experiences and Perceptions of Adolescents Aged 14 to 18 19
- Experiences and Perceptions of Parents, Professionals from Institutions and Civil Society Organizations, ICT Companies, Media Concerning Exploitation of Children Via ICT: Roles and Responsibilities 20
  - Experiences and Perceptions of Parents 20
  - Experiences and Perceptions of Representatives from Relevant Public Institutions Working with Children 22
  - Experiences and Perceptions of Representatives from Civil Society Organizations 22
  - Understanding of ICT Companies 23
  - Data from Law Enforcement Agencies and Ministries 24
  - Media Representation of the Phenomenon 25
- Challenges and Obstacles in the Fight against Child Exploitation Via ICT 26

### 3. FINAL REMARKS

28

- Best Practices in the Area of Prevention and Existing Protection Mechanisms 28
- Recommendations for Advancement in the Prevention and Protection of Children from Exploitation Via ICT 30

### Appendix

32
INTRODUCTION

The deep suffering produced by internet child exploitation has recently resonated in international news. Immense media attention on the theme contributed to challenging many dominant misconceptions equating internet child exploitation to pedophilia and child pornography. Many pushing decision makers were called by their constituencies, mostly parents, to take a stand against cyber-bullying.

While not inherently “evil,” the internet has become a means of exploitation of minors in many different forms, often with tragic consequences. Internet connectivity, mostly associated with the use of social networks and mobile phones, is widespread among children and adolescents across the planet, providing considerable advantages in terms of educational, socialization and participation opportunities. However, Information and Communications Technology (ICT) also represents an ideal tool for predators in that it offers safety, easy access to victims and the possibility of fake profiles. Adults with specific roles and responsibilities in child protection including parents, guardians, teachers, professionals from state institutions as well as representatives from the private sector are faced with the challenge of protecting children from online exploitation while struggling to find a reasonable balance between control and trust.

The Southeast European region is not immune from this phenomenon. In the absence of definitive data on the exploitation of children via ICT, evidence suggests that online child pornography has turned into a billion dollar industry, i.e. one of the most lucrative forms of cybercrime in the region, while cases of sexting, grooming and cyber-bullying are often not adequately recognized as abuse, thus reported and prosecuted.

The present research aims at drawing the attention of the general public in the region and beyond to the phenomenon. This regional report is based on data collected by the Ombudsman of the Autonomous Province of Vojvodina (APV), Human Rights and Freedoms Ombudsman of Montenegro, and Ombudsman of Children of Republika Srpska (RS) based on a common methodology, with the purpose of taking a snapshot of the situation as perceived by stakeholders. Specific recommendations on how to increase the effectiveness of prevention measures and advance the system of protection of children from this dramatic form of abuse of their rights have been developed to show the direction in which stakeholders should move. Although not exhaustive in light of the complex nature of the subject, we hope this research report will stimulate further research and trigger a serious debate on how to effectively combat all forms of online child exploitation.

Ahmed Pjano
Director of Programmes
METHODOLOGY

Background, Topic and Territorial Span

This research comes as the last of three situational analyses on different forms of child exploitation, as part of the Regional Project “Prevention of Exploitation of Children in South East Europe.” The project started in 2010 with the purpose of improving and strengthening the efficacy of the system of child protection from all forms of abuse, neglect, exploitation and violence, including exploitation via information and communications technology (hereinafter ICT). In order to achieve the objective of raising awareness among professionals and public in general on forms, root causes and consequences of child exploitation, the realization of situational analyses on specific forms of child exploitation was envisaged within the framework of this project.

Topic of this analysis are the policies and practices applied in the system of prevention and protection of children from exploitation via ICT, the perceptions of all actors involved including children and adults, and the recommendations for their advancement as expressed by participating Ombudsman Institutions.

The territorial span of this research stretches from Republika Srpska, Bosnia and Herzegovina, hereinafter RS, Autonomous Province of Vojvodina, Serbia, hereinafter APV, and Montenegro, whose Ombudsman Institutions have completed individual reports on their territories based on a common methodology.

Rationale

It appears that children using ICT have improved opportunities to fully enjoy their rights, but may be at the same time in this way exposed to increased risks. For this reason, it is necessary to make the internet a safer place rather than prohibiting its use to minors. In order to do so, there is a need for a more thorough analysis of the grey area between safeguarding full enjoyment of their rights and protecting them from related risks. The rationale behind the present research is thus to gain deeper insight in the intersection between opportunities and risks in child internet use by analyzing the present situation in the territories represented by participating Ombudspersons Institutions, focusing on how to prevent the phenomenon of internet child exploitation. The theoretical standpoint from which this research stems is a rights based one, meaning that it prioritizes the best interest of the child – understood as subject of rights including protection. Results from the present research will be of key importance to develop operational recommendations adopted by local Ombudspersons Institutions participating in the Regional Network to ensure focused lobbying to National Governments and relevant authorities.

Goals, Objectives, Structure

The goal of the present research is to analyze the phenomenon of child exploitation via ICT from a child rights perspective in the countries/entities/autonomous provinces in question. The goal will be attained by identifying areas for improvement of the legal framework, describing how to fill possible gaps in the implementation of relevant legislation, and by developing arguments and recommendations to advance the system of prevention and protection to effectively combat the phenomenon.

Research objectives and related questions to be responded in corresponding sections can be summarized with the following report outline:

1. To achieve a better understanding of the legal framework in place to protect children from exploitation via ICT:
   a. What is the international legal framework for the protection of children from exploitation via ICT?
   b. What is the national legal framework and how are international obligations implemented at the national level? Which protection instruments are available?
   c. Which ethical codes of conduct and policies have been adopted by telephone companies and internet service providers in the countries/entities/autonomous provinces in question? Are these codes and policies adequate from a child rights perspective?

2. To assess the current status of the phenomenon:
   a. How is the exploitation of children via ICT defined? How do involved actors understand it?
   b. Why are some children at greater risk of being exploited using ICT? How well do parents/guardians understand the risks to which children are exposed in virtual reality? Do parents recognize risks? If so, what do they do? What is the influence of parents, educators, and other responsible adults on children’s online safety?

---

4 See also: “Regional Report on Child Begging” (December 2011) and “Regional Report on Sexual Exploitation of Children” (September 2012).
c. What is the situation of child exploitation via ICT in analyzed countries/entities/autonomous provinces? What are the conditions allowing this phenomenon to occur? How does it manifest? In what way do actors involved in its prevention communicate? What are the obstacles to a full understanding of this phenomenon?

3. To identify best practices in preventing and combating child exploitation via ICT and develop related recommendations:
   a. What are the best practices in the area of prevention in the region and abroad? What are the available mechanisms for protection from child exploitation via ICT?
   b. What are the key recommendations and conclusions of Ombudsman Institutions on prevention and protection of children from exploitation via ICT?

Data Collection Methods and Sources of Information

Based on feedback from participating Ombudsman Institutions, a common methodological framework was developed by Consultant appointed by Save the Children to coordinate research efforts. The Consultant developed a set of data collection instruments to assist research teams in APV, Montenegro and RS. Individual Institutions subsequently adjusted research instruments to local needs and peculiarities so as to ensure the viability of data collection and the relevance of key findings for regional purposes. Specific adjustments were made in the areas of language use and sampling.

Research efforts included three main areas of inquiry:

- Desk research on the normative and legislative framework, both national and international on the subject matter
- Data collection and analysis from field work with children, parents, professionals, civil sector representatives, internet providers and telephone companies, ministries focusing on risk awareness and capacities related to exploitation of children via ICT
- Press clipping on media representation of news concerning exploitation of children via ICT.

Since an exclusive focus on quantitative data could not provide sufficient support for analyzing the phenomenon of child exploitation via ICT due to the lack of reliable information on the subject matter, a combination of qualitative and quantitative data collection methods presented itself as a viable approach for this research. Data collection techniques included focus group discussions, individual in-depth interviews, questionnaires, and a press clipping. Except when otherwise stated, field work was completed between November 9 and December 21, 2012.

Field work instruments were designed based on the following criteria:

- **Focus Group Discussions**

  The present research predominantly used focus group discussions as a research method with a variety of actors including children and adolescents, parents, and professionals from state institutions. In this respect, the preference given to qualitative data collection responds to the need to gain insight in personal narrations of individuals and groups on internet child exploitation. In general, the purpose of focus group discussions consisted in getting a reliable snapshot of respondents’ experiences opinions, perceptions, knowledge and intentions, after combining it with quantitative data collection methods. Expert facilitators moderated focus group discussions adjusting communication methods, language, instructions and all other discussion facilitation details to psychosocial, cognitive, cultural, educational and age peculiarities of polled respondents. For each of the abovementioned categories and specific groups of respondents facilitators made the necessary adjustments in each location so as to ensure full understanding of research questions and ensure reliability of collected data. Facilitators placed a special concern on child friendly and age-suitable means of expression in conducting the focus groups discussions with children and adolescents. Discussions were organized in different locations with the widest possible geographical span so as to ensure representation of different communities and diversity in APV, Montenegro and RS. Focus groups targeting parents of children aged 10 to 18 included parents’ councils in schools in the abovementioned communities to encourage them to share their perceptions and experiences in a context in which their role and responsibility would be particularly enhanced. Questions and instructions for the facilitation of focus group discussions with children aimed at gathering the following information: how much time they spend on the internet; what materials they access; their awareness level on internet exploitation; whether they recognize certain inappropriate behaviors; what their experiences are; and the extent to which they share this information with parents/responsible adults; etc. Questions and instructions for the facilitation of focus group discussions with parents attempted to collect answers concerning their role to children and in particular: how much time their children spend online; the extent to which they are aware of the contents their children access on the internet; the extent to which they consider the online world to be dangerous as compared to the physical world; their awareness level on internet child exploitation; to what extent they are aware of the experiences their children have; in which way they protect their children from internet exploitation, and so forth.
The aim of focus group discussions with professionals with a mandate on child protection (including social workers, police officers, judges, prosecutors, educators) was to verify their knowledge and capacity to recognize the phenomenon of exploitation of children via ICT within the framework of their duty and role. Questions asked to professionals revolved around the following themes: recognition of concepts and forms of exploitation of children on the internet; role of professionals in the prevention of and fight against exploitation of children via ICT; their experiences in direct or indirect intervention in concrete cases of internet child exploitation; multi-sectorial collaboration; etc.

- **Interviews with Representatives from Civil Society Organizations**

  The research methodology also included interviews with representatives from civil society organizations which are active in the field of protection of children from internet exploitation and child protection in general. The rationale for including such sample of respondents lies in the fact that civil society organizations feature expertise as well as financial means and for this reason in many cases with their activities they perform the function of filling in the gaps existing within the system of state institutions. Each participating Ombudsman Institution identified the most relevant civil society organizations operating in their geographical areas of jurisdiction. Questions and instructions for such interviews included reference to the following issues: capacities and needs of actors from the civil sector who are active in combating internet child exploitation; what their related activities are; leading trends shaping such activities; existing collaboration with state institutions and private sector companies in the area of prevention of exploitation and protection of children using ICT, and so forth.

- **Questionnaires**

  Research included a set of two questionnaires targeting respectively internet and telephone service providers and relevant state institutions including ministries and/or agencies. The first questionnaire focused on the understanding of roles and responsibilities in the area of prevention of exploitation and protection of children via ICT by representatives from state institutions with a mandate on child protection. The questionnaire included questions about reported, indicted, sentenced and convicted cases of internet child exploitations in general and in the form of sexting, grooming and cyber-bullying as defined in the present report. The purpose of collecting such information from different state organs is to assess their level of collaboration and coordination as well as the use of joint reporting criteria. The second questionnaire was aimed at collecting information on protection mechanisms against internet child exploitation as enforced by and from the perspective of ICT companies. Questions included definitions of exploitation of children via ICT, and roles and responsibilities in the area of prevention and protection as understood by representatives from the information and telecommunications sector. Besides, a number of questions concerned policies, practices and ethical codes of conduct enforced among staff of the abovementioned companies in the area of prevention of exploitation of children via ICT and their protection as well as related joint projects and collaboration in place with state institutions and civil society organizations.

- **Press Clipping**

  Ombudsman Institutions contracted professional agencies to perform a press clipping over a one-month period (November 15, 2012 to December 15, 2012), with the exception of APV, in which the reporting period was the whole year 2012. The focus of such analysis was internet use among children, internet child exploitation and ICT in general. The press clipping included major print media in the countries/entities/autonomous provinces of reference.

For a detailed list of locations, exact periods of polling of research samples, and local adjustments in field work data collection please refer to separate reports from APV, Montenegro and RS. The following table contains a description of polled samples, goals and participation in each research instrument:

<table>
<thead>
<tr>
<th>Source/method / instrument</th>
<th>Sample Description</th>
<th>Goal</th>
<th>Sample Participation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary/qualitative/ focus group discussion</td>
<td>181 children¹ aged 10 to 13, with access to internet</td>
<td>Analysis of the awareness of children regarding the potential risks of exposure to exploitation via ICT</td>
<td>n/a</td>
</tr>
<tr>
<td>Primary/qualitative/ focus group discussion</td>
<td>175 adolescents aged 14 to 18</td>
<td>Analysis of the awareness of adolescents regarding the potential risks of exposure to exploitation via ICT</td>
<td>n/a</td>
</tr>
<tr>
<td>Source/method / instrument</td>
<td>Sample Description</td>
<td>Goal</td>
<td>Sample Participation</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------</td>
<td>-----</td>
<td>----------------------</td>
</tr>
<tr>
<td>Primary/qualitative and quantitative/focus group discussion</td>
<td>133 parents from schools parents councils having children aged 10 to 18 who have access to the internet</td>
<td>Analysis of the awareness of parents concerning potential risks of the use of ICT, and of their willingness to apply specific measures to protect their children</td>
<td>n/a</td>
</tr>
<tr>
<td>Secondary / qualitative/focus group discussion</td>
<td>107 professionals from relevant public institutions including social workers, police officers, judges, prosecutors, educators</td>
<td>Analysis of capacities and links between relevant institutions and their understanding of child exploitation via ICT and protection mechanisms</td>
<td>n/a</td>
</tr>
<tr>
<td>Secondary/qualitative/in-depth interview</td>
<td>6 representatives from civil society organizations that are involved in the fight against child exploitation via ICT in the region</td>
<td>Analysis of capacities and needs of actors from civil society organizations who are involved in the fight against child exploitation via ICT</td>
<td>n/a</td>
</tr>
<tr>
<td>Secondary/qualitative and quantitative/questionnaire</td>
<td>32 internet and telephone service providers in individual countries/entities/autonomous provinces</td>
<td>Analysis of mechanisms for prevention from exploitation and protection of children via ICT, from the perspective of service providers</td>
<td>APV: 25% MNE: 60% RS: 36%</td>
</tr>
<tr>
<td>Secondary/quantitative/questionnaire</td>
<td>33 relevant ministries/agencies including: 7 Police districts, Ministry of Labor and Social Policy, Ministry of Trade and Communication, Agency for Radio Diffusion, Agency for Electronic Communication, Special Unit for High-tech Crime of the District Attorney’s Office, Ministry of Justice (APV); 13 State Courts, 2 Centers for Social Welfare, Upper Court, Ministry of Education and Sport, Ministry of Information Society and Telecommunications, MoI (Montenegro); MoI (RS)</td>
<td>Analysis of reported cases concerning child exploitation via ICT</td>
<td>APV: 100% police districts 33% ministries/agencies MNE: 100% RS: 100%</td>
</tr>
<tr>
<td>Secondary/qualitative and quantitative/press clipping</td>
<td>75 print media operating in research countries/entities/autonomous provinces (period: whole of 2012 for APV, 15/11/2012 to 15/12/2012 for MNE and RS)</td>
<td>Analysis of the treatment of news on child exploitation via ICT through an overview of employed keywords</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Table 1: Overview of research instruments, sample description and participation

---

* Sample size was adjusted in each country/entity/autonomous province based on children’s number.

b The 4 participating internet and telephone service providers account for 80% of market share in the ICT sector in RS.
Subsequent to analyses of legal framework and field work, best practices in the field of prevention initiatives and protection mechanisms against exploitation of children via ICT have been identified at the regional level, with occasional reference to global trends. Furthermore, the report contains a brief discussion of obstacles to the translation of identified best practices into higher standards of child protection across the board, at the legal and societal level as well as in the ICT industry. Finally, key findings from this analysis have been used to develop recommendations for advancement in the protection of children from exploitation via ICT.

DEFINITIONS OF KEY CONCEPTS

**Internet child exploitation:** Exploitation of children on the internet, that is, using ICT, includes violence, exploitation and abuse of children by their peers or by adults. Exploitation involves showing of inappropriate contents to children, recruiting of children for illegal activities, grooming, sexting, cyber-bulling, and other forms of violent behavior endangering the rights of the child.

**Grooming** is a process in which children are encouraged to participate in sexual interactions online, or via telephone devices, usually including exposure to unwanted pornographic contents.5

**Sexting:** Sending of disturbing contents (explicit texts, images, recordings) using ICT to another person (usually using SMS, MMS, email, Facebook or MySpace, but other social networks and chat-rooms as well).6

**Cyber-bullying** occurs when a person or a group of people uses the internet, mobile phones, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else.7

**Actors:** any institution or individual taking part in preventing child exploitation via ICT, including, for the purposes of this research – children, the media, education and social welfare professionals, youth counselors, police, justice, parents’ councils, representatives from civil society organizations and representatives of international organizations, internet service providers and telephone companies.

---

5 Grooming: “The purpose of grooming is to make a victim. Grooming is done to choose a victim, to see if the person may cooperate with sexual abuse because of the imbalance of power and coercion. Grooming is done to make a potential victim feel comfortable enough to be close to an offender, to be alone with an offender, and after the abuse, to keep the behavior a secret.” Cyber-Bullying and online Grooming: helping to protect against the risks, ENISA, European Network and Information Security Agency, 2011

6 “Sexting (a combination of the terms sex and texting) is the act of sending or posting sexually explicit photographs via cellular phones or over the Internet. The behavior has been the subject of intense media speculation in recent years owing to statistics showing its prevalence amongst young people and the legal cases that have resulted from instances of sexting.” Family Online Safety Institute’s (FOSI) Professional Edition of the Global Resource and Information Directory (GRID) http://www.fosigrid.org/family-online-safety/conduct/sexting

I. LEGISLATION AND IMPLEMENTATION

Due to the increasing occurrence and gravity of the phenomenon in today’s society, and to its interconnections with criminal activities, the fight against exploitation of children via ICT should be addressed primarily from the point of view of existing legal regulations. An up-to-date, comprehensive and strict international and national legal framework is crucial to ensure adequate protection of children from exploitation via ICT. For this purpose, international standards of child protection should find adequate compliance with national legal regulations to effectively address the issue from the perspective of prevention as well protection. A number of relevant legally binding acts and measures as well as formal commitments with consumers have been adopted in the region to comply with international child protection standards regarding the use of ICT. However, the international, regional and national normative frameworks in South East Europe currently are not always fully harmonized and often fail to ensure adequate protection the rights of children using ICT, as highlighted in further text (see in particular section 1.b). Based on the analyses developed by Ombudsman Institutions of APV, Montenegro and RS, as well as by an assessment made by Save the Children in conjunction with the Consultant, it may be concluded that in some cases national legal frameworks do not include adequate cybercrime norms to counter the phenomenon as prescribed by international standards.

The following sections contain an overview of international documents followed by their translation into national legal acts and by a brief discussion on ethical codes of conducts of ICT companies operating in APV, Montenegro, and RS. The focus of this overview is twofold. First, of particular interest for the purposes of the present analysis will be a discussion of how international regulations and requirements are actually rendered into national legislation in the countries/entities/autonomous provinces in question, highlighting possible gaps and shortcomings in the acquisition phase and calling for action to improve the national legal framework and advance the system of protection of children from exploitation via ICT. Second, the overview will also contain observations on the standpoint from which relevant legal provisions at the national level were developed, assessing to what extent they are in line with a child rights perspective.

The general principles of prevention and protection of children from exploitation via ICT are influenced by international law standards, in particular by those specifically referring to the fight against cybercrime and children’s rights. Such principles include:

- State obligation to take all appropriate legislative, administrative, social and educational measures
- Extraterritoriality or cross-border prosecution of perpetrators and convictions
- Adequate and specific definition of criminal activities via ICT harming children (child pornography, grooming, luring and inducement of children to harmful activities)
- Child’s best interest
- Transparency of information on risks of ICT use and means of protection from exploitation

Basic children’s rights related to ICT use as specifically laid out in individual international acts (reported below) include:

- Education
- Freedom of expression of children and their participation in decisions concerning them
- Right to seek and give information
- Free time and play
- Protection from violence, abuse and all forms of exploitation including sexual exploitation

[UN Convention on the Rights of the Child (1989)]

- Right to information on the risks of ICT use and on means of protection
- Confidentiality and privacy in court and administrative proceedings

[CoE Committee Ministers Recommendation (91) 11 Concerning Sexual Exploitation, Pornography and Prostitution of, and Trafficking in, Children and Young Adults]

For the purposes of the present report, the best interest of children in using ICT can be essentially outlined as a comprehensive combination of the following items:

- Access to ICT
- Protection against inappropriate content and contacts
- Privacy and confidentiality of personal data
- In case of witnessing in court and administrative proceedings about traumatizing experiences related to exploitation via ICT, psychological assistance and sensitivity so as not to reiterate the trauma
- Exposure to full information on risks of illegal and dangerous behaviors in the use of ICT and to advice as to how to protect from them, if appropriate involving parents/guardians/teachers and other responsible adults.

The following is a brief discussion of the content of international acts selected and listed by relevance to the subject matter. Such acts have been signed and ratified by state authorities having liability over the territories of APV, Montenegro and RS, by which states accept the obligation to receive the norms therein contained into national law.

The UN Convention on the Rights of the Child (1989), and in particular Articles 13, 17, 28 and 31\(^8\) suggest that access to ICT has a key role in current formative, educational and socialization processes in children’s lives worldwide, with potential benefits spanning from increased opportunities for education to recreation and community building as well as for enjoying human rights. Article 34 needs particular mention since it calls for state action to protect children from all forms of sexual exploitation and sexual abuse, specifically mentioning official commitment to prevent:

- The inducement or coercion of a child to engage in any unlawful sexual activity

\(^8\) Article 13: freedom of expression and to seek and receive information; Article 17: access to media; article 28: right to education, being the internet today one of the main gateways to up-to-date information allowing for a full-spectrum education curriculum to match school teaching; Article 31: right to leisure.
The exploitative use of children in prostitution or other unlawful sexual practices

The exploitative use of children in pornographic performances and materials.

The same Convention, particularly in Articles 19, 32, 35 and 36 postulates the obligation of signatory States to take all appropriate legislative, administrative, social and educational measures to protect children from a vast array of risks ranging from economic and sexual exploitation to violence and trafficking, which are in some cases increased by unsafe ICT usage.

The 2001 Convention on Cybercrime of the Council of Europe was adopted as the only binding international act on this issue, for the first time indicating an explicit connection between child pornography and ICT. Its importance lies in the fact that it enriched the current international legal framework with more targeted norms regulating activities made possible by the use of ICT. It also contains guidelines for individual states to develop comprehensive legislative and other measures to combat cybercrime and to establish a platform for international cooperation among State parties to the Convention for the prosecution of illegal activities on the internet and definition of competent jurisdiction. As for the definitions prescribed by the guidelines, the following activities must be established as criminal offences and therefore sanctioned by national law if they are committed intentionally and without right:

a. producing child pornography for the purpose of its distribution through a computer system;
b. offering or making available child pornography through a computer system;
c. distributing or transmitting child pornography through a computer system;
d. procuring child pornography through a computer system for oneself or for another person;
e. possessing child pornography in a computer system or on a computer-data storage medium.


- acknowledges that both children and perpetrators increasingly use ICT;
- prescribes that its signatories take all legislative and other measures to ensure that children in primary and secondary education are informed on the risks of sexual abuse and exploitation and on related means of protection, possibly involving parents/guardians when deemed appropriate. Such information is intended to specifically target higher risk groups and in such cases to focus on the use of ICT;
- encourages an active involvement of the private sector, namely ICT companies, in developing and implementing specialized policies to combat sexual exploitation and abuse of children, and adopting self-regulatory norms;
- clearly defines criminal offences related to exploitation of children via ICT, adding to prior notions the one of “knowingly obtaining access, through information and communication technologies, to child pornography;”
- requires participating parties to take appropriate legislative and other measures to criminalize the solicitation of children for sexual purposes, including an adult’s proposal made by use of ICT to meet with a minor with the intention to commit instances of sexual abuse and exploitation and followed by material acts leading to such a meeting.

The 2000 Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography prohibits the sale of children, child prostitution and child pornography. The Protocol was designed as an appendix to the UN Convention on the Rights of the Child, expanding the concept of protection of children against all forms of exploitation to current developments in the ICT sector, which allowed easier access to pornography via the internet.

---

9 Article 19: States should take all appropriate measures to ensure protection of children from all forms of violence; Article 32: protection from children's economic exploitation; Article 35: protection from child trafficking; Article 36: protection from all forms of child exploitation.

10 The definition of “child pornography” contained in the CoE Convention on Cybercrime includes pornographic material that visually depicts:
   a. a minor engaged in sexually explicit conduct;
   b. a person appearing to be a minor engaged in sexually explicit conduct;
   c. realistic images representing a minor engaged in sexually explicit conduct.

11 The criminal offences indicated in the CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse include:
   a. producing child pornography;
   b. offering or making available child pornography;
   c. distributing or transmitting child pornography;
   d. procuring child pornography for oneself or for another person;
   e. possessing child pornography;
   f. knowingly obtaining access, through information and communication technologies, to child pornography.
Resolution 1099(1996) of the CoE Parliamentary Assembly on the Sexual Exploitation of Children also recognizes the importance of expanding the understanding of child pornography in all its forms so as to encompass those made possible by the use of ICT. Furthermore, it calls for joint action of state members in the fight against child prostitution, trafficking and pornography, as well as for the establishment of the criminal offences of: possession, production and filming of materials depicting child pornography.

With the Recommendation (2001)16 of the CoE Committee of Ministers on the Protection of Children against Sexual Exploitation, internet providers are described as subjects to be necessarily included in the fight against exploitation of children via ICT. Namely, a strong collaboration between internet providers and relevant state institutions is recommended for the identification of sexual exploitation, the response to all means of abuse via ICT, and which can be used with the purpose of sexually exploiting children. In particular, internet providers are encouraged to:

- develop up-to-date ethical codes of conduct in line with ICT trends and advancements to combat child sexual exploitation
- identify misuse of such codes and technologies
- adopt measures to combat and deal with such misuse
- provide parents/guardians/all individuals responsible for children as well as children with information on the risks of sexual exploitation over the internet and on protection measures
- create child protection hotlines and encourage citizens to report cases of child pornography or of incitement to child prostitution on the website, thus enabling the appropriate law enforcement authorities to take specific action.

The Recommendation also encourages research efforts at national and international levels to investigate on the use of the Internet in the prevention of sexual exploitation.

Finally, the Resolution 1307(2002) of the CoE Parliamentary Assembly on Sexual Exploitation of Children indicates how internet as a technology worsened the context of sexual abuse of children by allowing perpetrators to enjoy anonymity and easy access as well as unlimited contacts with potential victims. Furthermore, it calls for states to prioritize action to suppress sexual exploitation of children in any form as a national interest, and to enhance legislative and technical capacities of law enforcement institutions operating in the area of protection of children against sexual exploitation as a form of cybercrime. Last, it encourages all citizens to report sexual abuse of children, and it supports the free-of-charge nature of child protection hotlines and financial help to civil society organizations operating in this field, with a preference for those focusing their action on safer internet.
The international legal framework of the fight against exploitation of children via ICT is further completed by the protection standards contained the following acts, listed in order of adoption in the table below:

<table>
<thead>
<tr>
<th>Act (date of adoption) in Force in Country/Entity/Autonomous Province (signed, ratified)</th>
<th>APV</th>
<th>Montenegro</th>
<th>RS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universal Declaration of Human Rights (1948)</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
</tr>
<tr>
<td>Convention for the Protection of Human Rights and Fundamental Freedoms (1950)</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
<td>Signed and ratified (with reservations)</td>
</tr>
<tr>
<td>International Covenant on Civil and Political Rights (1966)</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
</tr>
<tr>
<td>Convention on the Elimination of All Forms of Discrimination Against Women (1979)</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
</tr>
<tr>
<td>CoE Committee Ministers Recommendation (91) 11 Concerning Sexual Exploitation, Pornography and Prostitution of, and Trafficking in, Children and Young Adults</td>
<td>N/a(^{a})</td>
<td>N/a(^{b})</td>
<td>N/a(^{c})</td>
</tr>
<tr>
<td>Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labor (1999)</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
</tr>
<tr>
<td>Convention on Action against Trafficking in Human Beings (2005)</td>
<td>Signed</td>
<td>Signed and ratified</td>
<td>Signed and ratified</td>
</tr>
</tbody>
</table>

Table 2: Overview of other international acts containing legal norms regulating the fight against exploitation of children via ICT, with ratification status in researched countries/entities/autonomous provinces.

---

\(^{a}\) Recommendations serve as non-binding guidelines on how to implement a specific convention; hence they do not require signature and ratification by participating parties.

\(^{b}\) See above.

\(^{c}\) See above.
I.b. National Legislation and Implementation, Existing Mechanisms and Procedures for Protection – Overview of Relevant Documents

Subject of the analysis of national legal frameworks developed by Ombudsman Institutions were the Constitutions of the Republic of Serbia, Montenegro, Republika Srpska and Bosnia and Herzegovina, as well as the following legal provisions in force:

### APV
- Constitution of the Republic of Serbia
- Family Law
- Criminal Code
- Criminal Procedure Code
- Law on the Fundamentals of the Education System
- Law on Organization and Competencies of State Authorities in Fight against High-tech Crime
- Law on Electronic Telecommunications
- Law on Protection and Treatment of Children and Juveniles in Criminal Proceedings
- Law on Police
- Law on Social Protection
- Law on Health Protection
- Labor Law
- Law on Public Information
- Law on Radio Diffusion
- Advertising Law
- Law on Electronic Trade
- Law on the Protection of Personal Data
- Law on the Protection of Consumers
- Serbia’s National Strategy for Information Society Development until 2020
- National Action Plan for Children until 2015
- General Protocol for the Prevention and Protection of Children from Abuse and Neglect
- Special Protocol for the Protection of Children and Pupils from Violence, Abuse and Neglect in Educational Institutions

### Montenegro
- Constitution of the Republic of Montenegro
- Family Law
- Criminal Code
- Criminal Procedure Code

### RS
- Constitution of Bosnia and Herzegovina
- Constitution of RS
- Family Law of RS
- Criminal Code of Bosnia and Herzegovina
- Criminal Code of RS
- Criminal Procedure Code of RS
- Law on Protection and Treatment of Children and Juveniles in Criminal Proceedings of RS
- Action Plan for Children 2011-2014 of Bosnia and Herzegovina
- Law on the Ombudsman for Children of RS
- Law on Communications of Bosnia and Herzegovina
- Law on the Protection of Personal Information of Bosnia and Herzegovina

| Table 3: Overview of legal provisions in force in APV, Montenegro and RS concerning internet child exploitation |

A comparative analysis of the definitions of specific criminal offences contained in the Criminal Codes of participating countries/entities/autonomous provinces was conducted based on information provided respectively by the Ombudsman Institutions of APV, Montenegro and RS. Results from such analysis, particularly highlighting similarities and gaps in legal solutions, are displayed in Table 3.

---

* Legal provisions for APV refer to those in force in the Republic of Serbia.
<table>
<thead>
<tr>
<th>Related Definitions</th>
<th>AP Vojvodina</th>
<th>Montenegro</th>
<th>Republika Srpska</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Child Exploitation, Cyber-bullying, Sexting</td>
<td>Display, acquisition and possession of pornographic material and exploitation of children for pornographic purposes</td>
<td>Display of pornographic material in presence of children and production and possession of child pornography</td>
<td>Production, display and possession of child pornography</td>
</tr>
<tr>
<td>Grooming, Cyber-bullying</td>
<td>Inducing a juvenile to witness sexual acts</td>
<td>Inducing a juvenile to witness the perpetration of criminal offences against sexual freedom</td>
<td>Sexual Intercourse by Abuse of Position</td>
</tr>
<tr>
<td>Grooming, Sexting, Cyber-bullying</td>
<td>Unauthorized publication and display of someone else’s writing, portrait and filmed image</td>
<td>Unauthorized publication and display of someone else’s writing, portrait and filmed image</td>
<td>Unauthorized photographing and display of someone else’s image</td>
</tr>
<tr>
<td>Grooming, Sexting, Cyber-bullying</td>
<td>Unauthorized collection of personal data</td>
<td>Unauthorized collection of personal data</td>
<td>Unauthorized use of personal data</td>
</tr>
<tr>
<td>Cyber-bullying, Grooming</td>
<td>Damaging computer data and programs; Creating and introducing computer viruses; Computer fraud; Computer sabotage; Unauthorized access to computer, computer network or electronic data processing</td>
<td>Damaging computer data and programs; Creating and introducing computer viruses; Computer fraud; Computer sabotage; Unauthorized access to computer, computer network or electronic data processing</td>
<td>Damaging computer data and programs; Creating and introducing computer viruses; Computer fraud; Computer sabotage; Unauthorized access to computer, computer network or electronic data processing</td>
</tr>
<tr>
<td>Internet Child Exploitation</td>
<td>Use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Child Exploitation</td>
<td>Mediation in prostitution</td>
<td>Pimping and procuring</td>
<td>International procuring in prostitution</td>
</tr>
<tr>
<td>Internet Child Exploitation</td>
<td></td>
<td></td>
<td>Exploiting children and juveniles for pornography</td>
</tr>
</tbody>
</table>

Table 4: Overview of criminal offences connected to exploitation of children via ICT as defined in the criminal codes of APV, Montenegro and RS and related to definitions

APV abides by Serbian Constitution, according to which “a child shall enjoy human rights suitable to their age and mental maturity” (art. 64). In the Constitution of RS and Bosnia and Herzegovina, the right to inviolability of human dignity, physical and mental integrity, privacy and personal and family life extends its action to all individuals including children. The Constitution of Montenegro guarantees to children special protection from psychological, physical, economic and other types of exploitation and abuse. Therefore the right to prevention and protection of children from exploitation using ICT is clearly set out in all constitutional charts in force in participating countries/entities/autonomous provinces.

Family laws of the Republic of Serbia, Montenegro, and Republika Srpska state the child’s best interest as the guideline for anybody in charge of managing activities dealing with children, as well as the state’s obligation to take all necessary measures aimed at respecting, protecting and advancing their rights and protecting them from neglect, physical and mental abuse, and any other form of exploitation.

Criminal Codes also present extended similarities as to provisions concerning the following criminal offences, as variously defined in APV, Montenegro and RS: production, display and possession of child pornography; inducing a minor to witness or participate in sexual acts; unauthorized publication and display of someone else’s writing, portrait and filmed image; unauthorized collection of personal data; criminal offences against the security of computer data; procuring for prostitution. If extensively interpreted, such criminal offence may be related to definitions as defined for the purposes of the present research. Interestingly, no criminal offences relate to the concepts
of sexting, grooming and cyber-bullying as such, but only in broader interpretations of regulations concerning child pornography or unauthorized use of personal data or images. Particularly relevant for the theme of this research are the criminal offences defined as:

- “use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile” (Republic of Serbia – APV), and
- “exploiting children and juveniles for pornography” (RS).

Such detailed definitions of criminal offences in APV and RS are currently countered in respective cases in other participating countries/entities/autonomous provinces by gaps or inadequate legal provisions which are not in line with the latest developments in ICT and related criminal behaviors. For this reason, it is fair to claim that such provisions represent the most advanced steps in protecting children from exploitation via ICT by legal provisions within the geographical span of the present research (see definition of “internet child exploitation”).

Special reports by Ombudsman Institutions from participating countries/entities/autonomous provinces provide more detailed information on individual legal frameworks and concrete activities implemented by relevant institutions in the area of the fight against exploitation of children via ICT, as well as on recommendations for advancement in the normative system as well as harmonization with international legal standards.

In conclusion, the national legal framework in participating countries/entities/autonomous provinces generally complies with international standards of protection of children from exploitation via ICT as contained in legally binding documents to which respective states are signatory. However, implementation of binding and relevant international regulations and requirements is limited due to incomplete reception into national law in the countries/entities/autonomous provinces in question. Legal gaps affecting adequate protection of children from exploitation via ICT have been highlighted in Table 3 (see above). This research helped identify specific gaps in implementation of regulations and requirements as stated in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. In particular, legislation in force in Montenegro and RS appears to be currently incompatible with article 23 as it lacks a comprehensive definition of criminal offences in the virtual world. To this extent, the Ombudsman Institution of Montenegro recommended the introduction of a dedicated regulation adequately criminalizing new forms of child exploitation via ICT, e.g. along the line of what prescribed by the Criminal Code of the Republic of Serbia: “Use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile”. For a more comprehensive list of recommendations at the legislation level, please refer to section 3.b. and individual reports from APV, Montenegro and RS.

I.c. Child Protection Regulations Adopted by ICT Companies

– Overview of Relevant Documents

The research included an overview of ethical standards of ICT companies operating in participating countries/entities/autonomous provinces as contained in ethical codes of conduct and relevant policies. Such overview specifically focused on major mobile phone operators. The rationale for this choice lies in the fact that minors nowadays largely access the internet from smart phones without adult supervision, thus being exposed to increased risks of exploitation. The underlying question in approaching relevant documents from the private sector was to what extent they mirror a concern for children’s safety and they were developed from a child rights perspective and in line with international protection standards.

The results of such analysis are all but comforting. The notion of corporate social responsibility is still relatively new in South East Europe, hence as such not mainstreamed in the routine practices of the private sector. Moreover, corporate social responsibility policies in the region mostly concern support to community cultural and social initiatives or in some cases charity initiatives for vulnerable groups such as individuals with disabilities. Images of happy, playful children are abundant on cover pages and within the text of analyzed reports while such detailed definitions of criminal offences in APV and RS are currently countered in respective cases in other participating countries/autonomous provinces by gaps or inadequate legal provisions which are not in line with the latest developments in ICT and related criminal behaviors. For this reason, it is fair to claim that such provisions represent the most advanced steps in protecting children from exploitation via ICT by legal provisions within the geographical span of the present research (see definition of “internet child exploitation”).

Special reports by Ombudsman Institutions from participating countries/entities/autonomous provinces provide more detailed information on individual legal frameworks and concrete activities implemented by relevant institutions in the area of the fight against exploitation of children via ICT, as well as on recommendations for advancement in the normative system as well as harmonization with international legal standards.

In conclusion, the national legal framework in participating countries/entities/autonomous provinces generally complies with international standards of protection of children from exploitation via ICT as contained in legally binding documents to which respective states are signatory. However, implementation of binding and relevant international regulations and requirements is limited due to incomplete reception into national law in the countries/entities/autonomous provinces in question. Legal gaps affecting adequate protection of children from exploitation via ICT have been highlighted in Table 3 (see above). This research helped identify specific gaps in implementation of regulations and requirements as stated in the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. In particular, legislation in force in Montenegro and RS appears to be currently incompatible with article 23 as it lacks a comprehensive definition of criminal offences in the virtual world. To this extent, the Ombudsman Institution of Montenegro recommended the introduction of a dedicated regulation adequately criminalizing new forms of child exploitation via ICT, e.g. along the line of what prescribed by the Criminal Code of the Republic of Serbia: “Use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile”. For a more comprehensive list of recommendations at the legislation level, please refer to section 3.b. and individual reports from APV, Montenegro and RS.

12 Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse).

13 In the lack of comprehensive regional data for the South East European region, a quick comparison in global trends helps provides insight in the relevance of children's access to the internet via mobile phones. A 2012 research on children's safety on the internet by the Ministry of Information Society and Telecommunications of Montenegro pointed out the following data: 26.5% of polled children access the internet from mobile phones, while 51.6% of them most often access the internet from their bedroom. The full report is available at: http://www.mid.gov.me/ResourceManager/ FileDownload.aspx?rid=110882&rType=2&file=Istrazivanje%20o%20bezbednosti%20djece%20na%20Internetu.pdf. Such data are in line with North American trends indicating that 27% of teens use their phone to get online (http://www.webwisekids.org/programs-facts-statistics-bescen.html).

14 See section 1.a.
a selling point than a concrete commitment to online child safety. In fact, the self-regulatory framework of the main ICT companies in APV, Montenegro and RS appears to respond to market, legal or at the most customer satisfaction and retention concerns rather than a commitment to protecting children from exploitation while using their services. No major divide was observed between mobile operators with state participation or state owned and private ones from a child rights perspective. Furthermore, elements of online child safety are not prescribed by legal regulations specifically targeting ICT companies in the countries/entities/autonomous provinces in question, so that any such related initiatives in the private sector are basically the result of good will and marketing strategy rather than compliance with legal obligations. Overall, data emerged from the present research indicate that:

- online child safety is not listed among the priorities of the corporate social responsibility policies and practices of the almost totality of mobile operators operating in APV, Montenegro and RS, as confirmed by the findings from related questionnaires (see section 2.b. Experiences and Perceptions of Parents, Professionals, ICT Companies, Media Concerning Exploitation of Children Via ICT: Roles and Responsibilities);

- practiced policies as listed in reports and ethical codes of conduct of ICT companies are not in line with what recommended in international acts (see in section 1.a. reference to the following international documents and related provisions: The CoE Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007) and Recommendation (2001)16 of the CoE Committee of Ministers on the Protection of Children against Sexual Exploitation).

**AP Vojvodina**

The ethical codes of conduct of mts Telekom Serbia and Vip Serbia are not satisfactory from a child rights perspective as they only contain brief regulations on customer legal protection in the phase of establishment of a subscription and over the course of its duration, as well as regulations on data protection. The only exception is represented by Telenor Serbia, which specifically operates in the area of children's online safety, understood as impeding the distribution of inappropriate content. As indicated in its 2011 Report on Sustainable Business Operations, the company's efforts in this area include the signature of an agreement with the Serbian Ministry of Interior in 2010 “on a strategic cooperation in order to introduce filters for blocking access to illegal websites with elements of child sexual abuse. Telenor users that attempt to access website of this type from their mobile telephone or computer are forwarded to our “Stop page”. There have been 116 such cases since the beginning of the realization of the project. At the same time, the Serbian Ministry of Interior Cyber Crime Department submits Telenor a list of sites that the Ministry of Interior and Interpol have determined to contain illegal material. Although commendable, blocking techniques along with the described practice of exchange of information with relevant national and international law enforcement institutions leave unresolved the issue of prosecution of perpetrators and proper action to combat child exploitation via ICT.

**Montenegro**

No elements of online child protection policies could be identified in the ethical codes of conducts and latest annual reports including information on corporate social responsibility activities of Crnogorski Telekom and m:tel Crna Gora. Interestingly, at the time of writing the local branch of Telenor Group was not disseminating on the internet reports on corporate social responsibility including information on child online safety and reported attempts of exploitation or other illegal activities. Telenor Montenegro website contains mention of filters for blocking access to illegal websites with elements of child sexual abuse; however no agreement with relevant local and international law enforcement institutions have been signed at the time of writing the present report.

**Republika Srpska**

The mobile operator scenario in the territory of Republika Srpska is dominated by: m:tel Bosna i Hercegovina, BA Telekom and HT Eronet. Concerns for child right to protection from exploitation via ICT appear to be absent from relevant documents of major mobile operators in RS, with the only exception of m:tel. As indicated in its 2011 Report on Corporate Social Responsibility, the company is collaborating with the Ombudsman for Children of RS and the Agency for Information Society of RS on their project on internet child safety. Concretely, m:tel organizes workshops for children, parents and teachers on risks on the internet and has published and distributed leaflets containing related information. Within the framework of the project the educational internet portal djecanainternetu.org was established.

---

15  http://www.telenor.rs/media/TelenorSrbija/fondacija/Fondacija_Izvestaj_2011-engleski.pdf
16  http://www.telenor.me/en/About-Telenor/Corporate-responsibility/Safety/
17  http://www.mtel.ba/images/content/DOP/IODO_2011.pdf
In order to adequately comprehend the phenomenon of ICT child exploitation in all of its social significance and implications, it is necessary to take into account the way in which different actors and stakeholders understand it. The following sections will give space to the experiences and perceptions of children, parents, professionals, ICT companies, media agencies concerning exploitation of children via ICT, as collected through field work as described in the methodological section of the present report. Results from field work will be particularly helpful to gain insight in direct experience, risk perceptions and overall knowledge about the virtual world, as well as to demystify misconceptions on the subject. As an introductory remark, it is worth mentioning how despite peculiarities in research samples in APV, Montenegro and RS, key findings converge on major common themes. Such overall commonality in themes suggests a fundamental socio-cultural similarity in needs and behavioral patterns as well as associated risks when it comes to the relationship between the virtual and real world, which has more to do with global trends in ICT use than with regional affinities.

2.a. Experiences and Perceptions of Children Concerning Exploitation Via ICT: Opportunities and Risks

In line with the outlined methodology, the outcome of the present research is a qualitatively significant yet necessarily partial snapshot of opportunities and risks as perceived and experienced by children in researched countries/entities/autonomous provinces. On the one hand, a focus on opportunities, meaning the core needs for information, social contact, entertainment, among others, which are enabled by ICT use provided insight in the reasons why children ultimately spend a sizeable portion of their time online engaging in different activities. Openly discussing with children about their online habits, on the other hand, was a privileged way to identify risks associated with ICT use. As a result of focus group discussions with children on this matter, high-risk behaviors have emerged, suggesting related areas for improvement of prevention and protection policies based on those. Furthermore, the value of focus group discussions, which are the preferred method of data collection in the present research, is their potential for raising children’s awareness on dangers they may face while online.
Experiences and Perceptions of Children Aged 10 to 13

Children aged 10 to 13 who participated in focus group discussions predominantly claimed they use the internet as a means of entertainment (online game playing, social contacts via social networks such as Facebook, Skype, music listening, information on sport happenings) rather than for educational purposes, e.g. to seek school-related information. When asked whether they would deem giving someone they met in a chat room their address or phone number to meet in person as an appropriate behavior, children gave very different responses in APV (100% Not appropriate), Montenegro (64% Not appropriate) and RS (96% Not appropriate).

Almost all respondents who answered negatively provided as an argument the possibility of misuse of personal information or of being contacted by individuals using false profiles. As far as sharing one’s pictures with someone met online is concerned, children in this sample predominantly expressed their security concerns and fear of misuse of those pictures for pornographic purposes, and for this reason declared they would refrain from this behavior. However, they admitted they have posted personal pictures on Facebook. Participation in online lotteries and prize contests requiring entry of personal information is mostly frowned upon by children in this age group, with the exception of situations in which they would feel they are in the position to “verify” their serious nature on their own. With the exceptions of children in Montenegro, the majority of respondents generally would not involve parents in this assessment. When polled about what they would do in case of a cyber-bullying incident in a chat room, respondents were divided in their answers, with two thirds of them determined not to react to it by informing responsible adults (in order of preference: parents, pedagogues, teachers, and police), the remaining third mostly unwilling to respond to the incident personally, and a minority in favor of it. When it comes to children's obedience to rules of ICT use agreed with parents, the most frequent standpoints include that such rules can be broken: if they have to do with time restrictions, while they should be respected if they have to do with access to certain contents (RS); or when accessing ICT outside the household, thus if parents do not find out (APV and Montenegro). Almost all respondents also claimed they would not give out passwords related to their email or social networking profiles fearing abuse. In the case of APV and RS, no unequivocal preference was given to either consenting or refusing to meet in person with someone children met online, with a slight majority choosing to refuse. In Montenegro, children predominantly claimed it would be dangerous to have such meeting, and in that case they would agree that they should inform their parents. Children who opted for consenting reported they would choose a public place or to be accompanied by someone they know when having the first meeting. Unpleasant situations related to exploitation via ICT were reported by individuals in this sample in APV and RS, while in Montenegro children did not report to have had any such experience and feel relatively safe since they believe they could easily “block” any attempts of exploitation.

Key Findings on Children Aged 10 to 13

In short, based on their largely naïve misconceptions they have about dangers, children in this age group demonstrated to be largely unaware of actual risks in the use of ICT. They do not see a clear connection between risks in the virtual and physical world, though they have a clear understanding of what is socially expected of them; they are also characterized by a natural curiosity dictated by their psychosocial development, encouraging them to have potentially dangerous behaviors which are not matched by adequate defense mechanisms.

Experiences and Perceptions of Adolescents Aged 14 to 18

Perceptions of adolescents aged 14 to 18 are somewhat similar to those of children aged 10 to 13. Significant differences emerged on the one hand due to different stages in their cognitive and behavioral development as compared with children aged 10 to 13, and on the other between researched countries/entities/autonomous provinces due to possible cultural specificities and social habits. The internet is for adolescents a lifestyle, and they access it for entertainment (music listening, Skype, Facebook and other social networks, YouTube videos and movie watching) as well as educational purposes, e.g. for school-related projects. The average time they spend online on a daily basis is up to 6 hours (Montenegro), with increased values during the weekend (up to the whole day in APV and Montenegro). Extended online activity clearly increases the possibility that instances of child exploitation take place.

Most of polled adolescents claimed they have never shared personal information with individuals they have met online for fear of misuse. In case they would, it would be only to people they “like” and with whom they had been entertaining online contacts for a long time (Montenegro). Those who admitted they have, though, also mentioned how such information was shared exclusively with people whom they met as part of common involvement in a recognizable social framework of some kind, such as community activities (RS). Adolescents claimed that pictures portraying them are available to all their contacts on Facebook, although almost all respondents claimed that they would never send them to someone they met online (APV and RS). Friend requests on Facebook from complete strangers are
never accepted, unless the contact seeker is a friend’s friend (APV and RS). Respondents who appeared to have a more outgoing personality were also the ones who claimed they accept more easily friend requests. Adolescents in RS mentioned the following as negative online experiences: insults and threats, exposure to explicit scenes, videos showing violence of some kind; unpleasant experiences they actually had included hijacking of their Facebook profile, publication of inappropriate pictures and messages and YouTube videos. As opposed to what emerged in the 2012 research on children’s safety on the internet by the Ministry of Information Society and Telecommunications of Montenegro, where 15.9% of respondents admitted they had unpleasant situations while using the internet, in the present research adolescents from APV and Montenegro denied such occurrence. However, they also reported the notion of fake profiles and peer violence on a social network was not unknown to them. According to adolescents, parents are overall informed about their children’s online activities, although their IT skills are very limited (RS); while trusting their good judgment completely (Montenegro), parents mostly warn adolescents about possible risks and discourage them from establishing contact with strangers (RS). However, parental control over access to ICT is considered low by focus group participants in this age group, especially those in APV, even when it only focuses on time restrictions, taking into account the diffusion of smart phones and the fact that they can be used virtually anywhere and anytime (e.g. in children’s rooms at night). All respondents expressed they would not be willing to share with alleged internet service providers passwords related to their email or social networking profiles fearing abuse. Although they are convinced to be adequately informed on this matter, prior research indicated that 90% of adolescent respondents in Montenegro would like to receive more information on safer internet use.18 In the present research, the research sample referred to dedicated media events, community based or extra-curricular in-school workshops, trainings, public debates, community based and seminars as effective ways to get more information on safer ICT use. The vast majority of respondents deny they have ever participated in first meetings with individuals they had met online, while in many cases this was reported as something that happened to a “friend.” Those who admitted they have met in person someone they had met online chose to be accompanied by a trusted peer as a protection strategy chosen, though they consented to such meetings only within a recognizable social framework such as participation in common community and social activities.

Key Findings on Adolescents Aged 14 to 18

Adolescents aged 14 to 18 demonstrated high self-confidence about their conduct on the internet, which they use for extended periods of time during weekdays and mostly in the weekend. In general, they have adequate awareness of possible risks connected to internet use and reasonably thorough defense mechanisms, though in some cases their self-confidence reaches a sense of exception and omnipotence when it comes to imagining themselves as a potential victim of exploitation. However, they are available for and interested in knowing more about safer internet use, mainly by participating in school activities on the issue. Adolescents also enjoy unjustified complete trust on the part of their parents, who largely have inadequate IT skills.

2.b. Experiences and Perceptions of Parents, Professionals from Institutions and Civil Society Organizations, ICT Companies, Media Concerning Exploitation of Children Via ICT: Roles and Responsibilities

The key indicator of focus group discussions with adults with a responsibility in children’s online safety was their level of understanding of their role, and awareness of their responsibilities. In particular:

- Focus group discussions with parents allowed us to easily verify the reliability of data collected from children and testing the truthfulness of key findings from focus group discussions with children of both age ranges;
- Polling representatives from public institutions, civil society sector, ICT companies, law enforcement agencies and ministries helped us identify gaps between legal norms of protection of children from exploitation via ICT and implementation;

18 Ministry of Information Society and Telecommunications of Montenegro
The press clipping on media treatment of news concerning online exploitation of children was insightful in outlining the background discourse in which all stakeholders are immersed, indirectly influencing their perceptions and decision making.

Experiences and Perceptions of Parents

Parents demonstrated a minimizing perception of the amount of time their children spend online (2 hours during weekdays; more than 2 hours during weekends; the older the children the longer they are allowed to spend time online). If compared with Chart 2 (Time spent online as reported by polled adolescents aged 14 to 18, above), Chart 3 (Time spent online by children and adolescents as reported by parents, below) shows how parents may have distorted perceptions as to the extent to which their children are exposed to risks connected to the use of ICT in terms of time spent on the internet.

Parents have agreed with children on time restrictions for internet use, though they recognize they are not in the position to supervise them due to their work and other daily obligations. Their opinion on ICT includes both a positive appreciation of easy access to information for educational and creative purposes, cheaper rates for communication than telephones, on the one hand, and a dislike of alienation, addiction, sedentary lifestyle, poor verbal skills, exposure to inappropriate content and contacts with strangers associated to their use on the other hand. Parents are correct at believing that using Facebook and other social networks represents their children’s main online activities, followed by Skype and YouTube. However, when it comes to the specific content of ICT interactions, parents are almost completely unaware and at a loss to understand their nature. When invited to reflect as to which world is more dangerous for their children, whether the virtual or real one, parents in most cases appeared concerned about both, though they seemed more preoccupied about not knowing enough about concrete dangers and in general about their own technological ignorance. For this reason, parents give their children only general warnings about online safety, with general statements along the line of “don’t talk with strangers” rather than with concrete guidelines for protection. When asked to be more specific about risks facing their children while online, the answers included pedophilia, false profiles, and exposure to inappropriate contents. In any event, parents were mostly unable to share with facilitators of focus group discussions more detailed descriptions of concrete instances or of real-life cases of exploitation via ICT which may have involved their children, as opposed to what established through focus group discussions with children and adolescents (see section 2.a.). Polled parents often stressed that an open communication with their children on Facebook use is a viable protection mechanism from exploitation, although in some cases parental advice appeared inadequate, naïve, or even counterproductive. For the most part, parents believe their children have not neither ever would give their consent to meet an online acquaintance in person, although they recognize their supervision is limited. Almost all parents are unfamiliar with the notions of “sexting,” “grooming” and “cyber-bullying” as such, although when explained what they mean they claimed to know about them with the exception of “grooming.” Due to its immediate counterpart in the real world and sizeable media exposure (see section Media Representation of the Phenomenon), the notion of “cyber-bullying” appeared to be the most widely known among parents.
Except for individuals who have professional knowledge of the matter, such as for example policemen working on anti-cybercrime projects and IT experts, parents are mostly unaware of the existence and/or do not make use of content filters and other protection software. As for rules agreed with children on internet use, parents are conscious that mere prohibition of ICT use would not work and that it would most probably produce a counter effect. Therefore parents mostly opt for content supervision. However, by exclusively focusing on dialogue and trust as protection measures, parents actually seem to mask their massive ignorance on the subject, as corroborated by comparing and counter checking information gathered during focus group discussions with children and adolescents. In conclusion, although very interested in having a debate on online child exploitation, parents recognize they are often not up to the task due to lack of basic IT skills, and that they need basic IT education so as to better protect their children from exploitation.

Key Findings on Parents

In general, parents demonstrate an overall understanding of the interconnection between the real and virtual world, and of the fact that a well-educated, resilient child will be more protected from online exploitation. However, due to their limited IT skills, parents are mostly unaware of their children’s experiences on the internet and appeared to fail to have a full grasp of concrete risks connected to some of their children’s behaviors and of means of protection, and for this reason they do not provide them with adequate support and supervision.

Experiences and Perceptions of Representatives from Relevant Public Institutions Working with Children

The sample of representatives from relevant public institutions working with children included psychologists, pedagogues, criminal police inspectors, prosecutors, judges, social workers, IT teachers and teachers of other disciplines. Their overall experience with instances of exploitation of children via ICT and their knowledge about means of protection are limited. For this reason, they expressed the need for further developing their skills to recognize victims of exploitation via ICT. The phenomenon is mostly understood as a form of child abuse, especially of sexual nature. Only a few of them specifically work on the subject, although they demonstrated an overall awareness that all information posted on the internet can be used for illegal purposes and become a means of abuse. When assessing the risks of exploitation in children's online presence, besides child pornography professionals see the use of Facebook and other social networks as particularly dangerous, as well as different kinds of financial fraud and identity theft. Many professionals participating in focus group discussions reported that the system of social protection is not comprehensively organized and does not allow for interventions outside what is prescribed by the law, which is sometimes perceived as insufficient to meet children's need of protection against exploitation via ICT. As for defining their role and responsibilities in combating online child exploitation, professionals are ultimately bound only by moral obligations in the lack of specific regulations to operationalize prescriptions as contained in national law. Other than in the area of organizing specialized trainings and publications for awareness raising purposes, professionals are generally mentioning they enjoy limited opportunities for concrete intervention to combat online exploitation. Specificities depending on the local legal frameworks in place need to be taken into account when analyzing this matter (see individual reports for APV, Montenegro and RS). Profession-related shortcomings such as lack of adequate technical capacities often end up hindering the work of professionals in the area of prevention and protection of children from online exploitation, as particularly expressed by police representatives when talking about cyber-crime interventions. Respondents’ perceptions vis-à-vis the definitions of “sexting,” “grooming” and “cyber-bullying” unanimously suggest that as such concepts are not understood. Rather, they require more descriptive labels that make them understandable in the local context and that therefore trigger the necessary action to combat the phenomenon. From the perspective of formal multi-sectorial coordination in the fight against online exploitation of children, professionals reported a basic vacuum and a lack of adequate platforms for exchange of information beside the only partially effective instrument of official memos. Meetings during seminars and other educational events represent an important opportunity for informal coordination among different sectors, although respondents stress that such exchange of information should be formalized in order to increase its effectiveness. Their understanding of the overall functioning of the system of protection is correct in terms of individual areas of competence; however, they stress the crucial role parents have in initiating contact with relevant authorities in case they suspect some form of abuse of exploitation. Professionals also lament shortcomings in the area of communication among relevant ministries, and the fact that there is no common monitoring system of cases of exploitation of children via ICT based on a shared understanding of key definitions and approaches.

Key Findings on Representatives from Relevant Public Institutions Working with Children

Shortly, professionals demonstrated sufficient specialized, sectorial knowledge of the phenomenon, though they would benefit from additional education outside their area of expertise and focusing on protection from exploitation of children via ICT. Overall, professionals rarely have the technical and human resources capacity to entertain multi-sectorial synergies. Furthermore, they reported a lack of necessary coordination, networking and information sharing mechanisms both internally within institutions and externally with parents with the purpose of preventing and combating children's exploitation via ICT.

Experiences and Perceptions of Representatives from Civil Society Organizations

Representatives from civil society organizations which are active in the field of the fight against internet child exploitation shared their perceptions on the subject through an in-depth interview. Key findings from field work with this sample specifically confirmed what emerged in focus group discussions with professionals from state institutions. Observations from this sample can be summarized as follows:
- **State-level institutions** hold a key responsibility in protecting children and combating exploitation effectively, although they lack adequate capacities and coordination mechanisms;

- **The role of civil society organizations** in the fight against internet child exploitation is mainly identified in the area of prevention (e.g. with the organization of awareness raising campaigns for children) and advocacy for change at the system level (e.g. to increase the effectiveness of protection mechanisms);

- The main challenges reported by civil society organizations which are active in this thematic area span from difficulties in defining the problem due to the extremely rapid advancement of ICT and related illegal activities to small-scale effect of their efforts, budget constraints and sustainability, isolation and lack of communication with other stakeholders, lack of transparency of state institutions, lack of multi-sectorial coordination among relevant institutions, low awareness of children and parents and understanding of institutions of the phenomenon, inadequate legal framework lacking key definitions of the phenomenon and specific regulations in the area of protection;

- The activities in which civil society organizations are most active include: educational workshops and counseling services for children and parents; research on social networks; media appearances; advocacy work to bring about improvements in the system of prevention;

- Key concerns in the area of awareness raising initiatives include: involving children form their earliest age so as to minimize risks of exploitation; providing hands-on, useful knowledge, e.g. how to protect personal information on social networks; fostering a climate of open dialogue between parents and children.

### Understanding of ICT Companies

Questionnaires sent to ICT companies (internet service providers and mobile carriers) were returned with very low participation,\(^\text{19}\) which represents by itself an interesting finding, confirming what observed during the analysis of ethical codes of conduct and other relevant sources of information on corporate social responsibility (see section 1.c.).

Respondents indicated exploitation of children via ICT as mostly related to pornography, exposure to harmful and inappropriate contents (e.g. web pages including information on hate groups, suicide techniques, kidnappings, drugs, peer violence, which perpetrators often use as a means of access to potential victims), and abuse aimed at achieving other results such as obtaining personal information, or committing violent acts that imply penal responsibility. **Respondents from ICT companies do not acknowledge any role or responsibilities in the prevention of acts of exploitation of children made possible by the use of their networks and services, other than in the case of removing illegal contents produced by the provider itself.** In terms of protection, their involvement is foreseen only in case of criminal investigations initiated by the police, in the form of submitting specific data from their records, which they duly store for this purpose. In this case, they also have the ability to prevent access to certain contents if they are so instructed by law enforcement agencies. Protection interventions of this kind were performed in a small number of cases. For the most part, respondents claim that **neither prevention nor protection of children from exploitation made possible by using their networks is listed among the priorities of ICT companies.** When asked about available means of prevention, respondents mainly stressed the importance of better parents’ IT and supervision skills and the use of antivirus programs and firewalls, as well as software recording all computer activity. As for protection methods, ICT companies mentioned removal of inappropriate content from their servers, and tracking, filtering or blocking access to pornographic materials from their networks, as well as next-generation technologies such as KAV, Palo Alto, Cisco, Fortinet, which they are not offering final users since their consent would be needed. In this respect, they admitted that they could, theoretically, have a more active role in educational projects and campaigns aimed at familiarizing parents with specific methods and techniques to increase their children’s safety while using ICT. Specific descriptions of the involvement of ICT companies in the fight against internet child exploitation are reported in section 1.e. However, they believe that such activities go beyond their duties as “neutral” service provider as agreed by contract with customers, and that the protection of children from all kinds of online exploitation falls under the responsibility of state institutions. Polled **ICT companies are unaware of specific regulations concerning the protection of children from online exploitation**, other than those referring to data recording for use in criminal investigation and court proceedings. **None of polled ICT companies has an ethical code of conduct including specific measures of protection of children from online exploitation,** though some have mentioned that they might consider their adoption in the future. In terms of established synergies with other stakeholders on the fight against exploitation of children via ICT, respondents reported limited coordination and communication channels with state institutions and none with civil society organizations.

---

\(^\text{19}\) 25% in APV, 60% in Montenegro, 26% in RS
Data from Law Enforcement Agencies and Ministries

Law enforcement agencies and ministries responded to a questionnaire in which they were asked to share information on registered cases of exploitation of children via ICT in 2011 and 2012 based on the definitions used in the present research. As envisaged in the methodology, organs within relevant institutions which were deemed relevant for the purposes of this research and contacted as sources of information included: Ministry of the Interior, Ministry of Labor and Social Policy and Ministry of Justice, with local adjustments based on the specifics of institutional organograms in each country/entity/autonomous province. Detailed information on sources, relevant legal regulations containing reference to the abovementioned definitions, and number of reported, dismissed and sentenced cases are available in individual reports by Ombudsman Institutions of APV, Montenegro and RS. Two issues are worth mentioning as preliminary remark. First, in some cases polled institutions returned questionnaires with the observation that national legislations contain no specific regulations referring to research definitions of “exploitation of children via ICT,” “sexting,” “grooming” and “cyber-bullying,” thus making it impossible to report cases accordingly. In Montenegro, for example, the Ministry of Internal Affairs commented that the criminalization of such concepts can be only based on an extensive interpretation of article 211 of the Criminal Code, concerning the display of pornographic material in presence of children and production and possession of child pornography. Second, some of polled institutions questioned their jurisdiction on the subject matter and/or referred us to other state organs, such as for example in the case of the Ministry of Information Society and Telecommunications of Montenegro and the Ministry of Justice of the Republic of Serbia, thus leading to the impossibility to collect comprehensive data.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>17</td>
<td>39</td>
<td>14</td>
<td>30</td>
<td>6</td>
<td>1</td>
<td>-</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>1</td>
<td>n/a</td>
<td>1</td>
<td>n/a</td>
<td>1</td>
<td>n/a</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>22</td>
<td>39</td>
<td>15</td>
<td>30</td>
<td>8</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Cases of exploitation of children via ICT, sexting, grooming and cyber-bullying as indicated by law enforcement agencies and relevant ministries

Data provided by the Special Unit for High-tech Crime of the District Attorney’s Office of the Republic of Serbia refer to the whole country. Individual data for APV was provided by its 7 Police Districts, indicating a total amount of 14 reported cases in the period 2011-2012.
Key findings from this analysis as well as from consultations with representatives from relevant institutions may be summarized as follows:

- In the period 2011-2012, a sizeable drop in the number of reported cases, indictments, sentences and convictions was registered;
- In the same period, the amount and harshness of convictions seems to be minimal as compared to the number and seriousness of reported cases, which may suggest extremely mild penal policies applying to crimes of exploitation of children via ICT;

Reflecting a legal vacuum in the definition of criminal offences in the area of exploitation of children via ICT in national legislations (see section 1.b.), polled state institutions were unable to provide comprehensive and unequivocal data on the subject.

Media Representation of the Phenomenon

Over a period of one year in APV, and one month in Montenegro and RS, a press clipping including an analysis of the treatment of news related to exploitation of children via ICT on behalf of printed media agencies was performed with a special focus on the following concepts:

1. Online exploitation of children and exploitation via mobile phones
2. Facebook
3. Cyber-bullying
4. Online harassment of children and harassment via mobile phones

Results from this analysis are clearly more relevant for APV in light of the extended research period. However, the geographical and cultural proximity of situations facing the region as well as its very similar socio-economic features and diffusion of ICT among children justify the drawing of tentative generalizations in all concerned countries/entities/autonomous provinces. In order to discuss the overarching media discourse in which all stakeholders are immersed in understanding the phenomenon, the following features stand out as particularly significant in the present research:

- News media demonstrate a deep interest in issues related to all forms of violence against children and violation of their rights, including exploitation via ICT; however, the reporting style is not in line with ethical principles as expressed in the codes of conduct regulating the work of journalists, and lacking basic knowledge of and concern for children's rights;
- In all articles, adults talk about issues facing minors and their protection, and represent the single source of information, thus de facto silencing children's voice and limiting their participation in the news making process;
- Marketing priorities and related tendencies to sensationalism in reporting instances of violence against minors shape the way in which news on internet child exploitation is treated; as a result, media contribute to spreading an atmosphere of helplessness and moral panic about the phenomenon rather than delivering a public information service with educational and awareness raising purposes aiming, for example, at explaining how to recognize, report and combat cases of exploitation of children via ICT;
- Distorted news representations mystify the true nature of the phenomenon, leading readers to gross misconceptions in suggesting profiling patterns and generalizations about perpetrators (adult men) and victims (young girls), except in the case of peer violence, as well as to confusion between means of exploitation (e.g. internet and Facebook) and criminal offences (pedophilia). In particular, children (mostly teenagers) are basically represented as passive victims who are not to be trusted or involved in protection measures rather than rights holders or potential offenders; parents facing cases of exploitation involving their children are helpless; suspects are immediately labeled as predators; state organs (mostly the police) appear in the story with the only function to arrest and interrogate suspects;
- The frequency of related news reports (once every three days in Serbia) intensifies in conjunction with specific events such as the presentation results from a specialized research on violence against children, rather than an informational or educational rationale which is relevant to the subject;
- Quality standards in analyzed news reports are unsatisfactory: articles are seldom signed by their authors and they contain serious breaches of privacy and anonymity regulations, especially affecting parents and children, based on which it is often possible to identify interested parties; the focus of analyzed news reports is generally placed on responding to the questions “when?” and “what?” rather than the more problematic “why?”; thus vastly failing to analyze the causes of the phenomenon; perpetuation of the criminal act and possible re-traumatization of victims may occur when media, as they often do, include graphic details in related news pieces, in a way unintentionally fulfilling perpetrators’ pleasure.

20 The website of the international project Pandora's Box provides further information on the dynamics shaping news treatment of the phenomenon http://pandorasbox.rs/sr/?lang=en
in seeing their offence as indirectly “glorified” (for this reason perpetrators often have the habit of filming their acts of exploitation), other than obviously jeopardizing the criterion of good taste; 21

- On a positive note, key concepts such as sexting, grooming and cyber-bullying are abundantly present and correctly used in analyzed texts as such or otherwise explained to inform the public about the different situations in which exploitation of children via ICT may occur, although such concepts are immediately equated to pedophilia;

Interestingly, the other child and adult respondents participating in the present research expressed views and perceptions suggesting that the current working practices of media operating in the region do not adequately meet their needs in terms of information, awareness raising and public service about online child exploitation.

2.c. Challenges and Obstacles in the Fight against Child Exploitation Via ICT

At the end of this overview of the phenomenon, a number of shortcomings have emerged in the fight against child exploitation via ICT in APV, Montenegro and RS. A roadmap of the areas in which action is particularly needed to advance the opportunities for prevention of online exploitation and the protection of children is outlined in this section. The following overview is organized by areas of action under which current shortcomings may fall, grouped as:

- Awareness raising, Capacity Building, Civil Society Participation
- Legislation, Policy Development, Instruments and Mechanisms
- System, Implementation, Operational

In a continuum from prevention to protection understood as processes which need to be strictly interconnected to ensure efficacy, areas of action for improvement of the present situation may specifically include the following groups of actors and related challenges and obstacles.

Awareness Raising, Capacity Building, Civil Society Participation

Relevant State Institutions

- lack of comprehensive, expert knowledge of the phenomenon among professionals, particularly concerning key concepts and definitions
- low motivation and responsibility in civil servants, with special reference to their role in child welfare

General Public

- parents’ limited IT skills
- parent’s distorted perceptions on the phenomenon and knowledge of key definitions and concepts
- poor parental skills in the real world have direct repercussions on children’s resilience to risks connected to ICT use and any other risks
- lack of commonly accepted and understood definitions of key terms in the area of exploitation of children via ICT in local languages, and of consistent cross references with terms used in relevant legal provisions
- low public awareness level of the phenomenon, especially in the area of key definitions and available means of protection
- scarcity of regional specific research focusing on the phenomenon in the countries/entities/autonomous provinces of concern
- passivity of consumers, in particular parents, in requesting more commitment to safe internet for their children on the part of ICT companies
- media provide a distorted, grotesque, partial and inaccurate representation of the phenomenon aiming at sensation rather than information

Children

- lack of knowledge of risks and means of protection

21 According to the Society of Professional Journalists Code of Ethics, in their work journalists should “show good taste. Avoid pandering to lurid curiosity” (http://www.spj.org/ethicscode.asp)
lack of awareness of the harmfulness and consequences of violent communication and peer violence (“netiquette”)

little trust in points of reference among adults in supporting them in case of sexting, grooming, cyber-bullying, unpleasant situations such as inappropriate requests on the part of other internet users, aggressive behaviors including peer violence using ICT, as well as all other forms of online exploitation

children spend a large amount of their free time using the internet and mobile phones as their primary and in many cases exclusive source of entertainment

Legislation, Policy Development, Instruments and Mechanisms

Relevant State Institutions

- legal gaps in the reception of international regulations at the national level
- legal vacuum in the definition of key concepts in the area of exploitation of children via ICT as criminal offences
- lack of binding legal obligations regulating ICT policies concerning online child safety
- discrepancies and factual gaps in recording criteria and lack of comprehensive, unequivocal data on cases of exploitation of minors via ICT in use by all relevant state institutions
- logistical disconnect between existing SOS lines/web pages to report cases of exploitation and relevant state institutions

General Public

- ICT companies in most cases do not hold online child safety and respect for children’s right to protection as one of their strategic priorities

System, Implementation, Operational

Relevant State Institutions

- low state budget allocations for activities and initiatives aimed at preventing exploitation of children via ICT
- gaps in the implementation of legal provisions
- limited opportunities for multi-sectorial coordination among state institutions to combat the phenomenon
- poor technical equipment of state institutions involved in the fight against exploitation of children via ICT
- mild penal policies and sentences for perpetrators
- lack of follow-up practices for victims and perpetrators outside an exclusively law-enforcement oriented paradigm
- relative isolation and insufficient two-way flow of information between local and all European/worldwide centers working on the issue
- only some ICT companies at the most operate in the area of blocking access to inappropriate contents, while attempts to access such contents are not investigated and prosecuted by law enforcement institutions

General Public

- no platforms for coordination between governmental and civil society sector to combat the phenomenon

---

22 In particular: use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile (Montenegro and RS)

For further information on gaps identified in the reception of international standards in national legal frameworks please refer to individual Ombudsman reports.
3. FINAL REMARKS

The scope of the present research does not allow for an exhaustive discussion of global trends in the fight against exploitation of children via ICT including state-of-the-art technologies for online child safety. However, a brief outline of existing opportunities for related advancements and necessary steps in APV, Montenegro and RS might be useful to indicate in which direction stakeholders should operate. The final part of this report will highlight prospects for improvement of the situation in the region vis-à-vis online prevention and protection of children, based on recommendations developed in conjunction with Ombudsman Institutions of APV, Montenegro and RS.


By investigating the exploitation of children via ICT starting from its legal framework and moving on to its understanding on the part of stakeholders, it was possible to identify a number of examples of best practices in the area of prevention and existing protection mechanisms, taking into account feedback from participating Ombudsman Institutions. Many of these best practices and protection mechanisms are implemented only at the local level, while other ones are already part of norms and regulations in force in the region. Before proceeding to developing recommendations for the advancement of the current system of prevention and protection, our purpose is to highlight policies and practices that are already in place or available for replication. While this list is not to be intended as exhaustive in any respect, it may provide insight in interesting developments in the fight against exploitation of children via ICT in the South Eastern European region. As previously done in section 2.c. while listing current shortcomings, the following overview is also organized by areas of action under which best practices and protection mechanisms may fall.

Awareness raising poster advocating safe use of internet by children produced by the Provincial Ombudsman of Autonomous Province of Vojvodina (Serbia)
Awareness Raising, Capacity Building, Civil Society Participation

- Primary School “Sečenj Ištevan” in Subotica (APV) has developed a research-based presentation on protection of children on the internet with tips for parents/guardians. Such presentation is highly informative and comprehensive in describing fact-based risks and mechanisms of protection of children from all forms of online exploitation, also including reference to the legal framework in force in Serbia.

- The civil society organization “Djeca prije svega” (Montenegro) and the Counseling Center to Help Parents and Children in Safe Internet Use of the civil society organization Target in Novi Sad (APV) are excellent examples of community-based support to parents and children. Anonymity, individually crafted approach and inclusion of both parents and children in the prevention of sexting, grooming, cyber-bullying and all other forms of online exploitation are among the strengths of such model of intervention. Both organizations have been involved in avoiding numerous potential cases of exploitation of children via ICT with educational, awareness raising and empowerment activities with clients, as well as child friendly publications on the theme (Djeca prije svega).

- Mobile operator m:tel (RS) has developed an awareness raising initiative in conjunction with the Ombudsman Institution of RS including the organization of educational activities for parents and children in schools and the publication of leaflets focusing on risks and protection tips concerning ICT use with a special focus on accessing the internet from smart phones (see section 1.c).

Legislation, Policy Development, Instruments and Mechanisms

- A number of legal provisions for the protection of children from exploitation via ICT are encompassed in relevant international documents (see section 1.a). Many of them may be listed as available protection legal mechanisms provided that they have been fully received by national law in APV, Montenegro and RS (see section 1.c). In particular:

  - The prescription that the following acts must be criminalized within national legal systems: producing, offering, distributing, procuring, possessing materials depicting child pornography; inducing a minor to witness sexual acts.

  - International cooperation in determining the jurisdiction of and prosecuting crimes committed with the purpose of online child victimization.

- The Child Online Protection (COP) global initiative is an important example of policy development support at the international level. Within the framework of the COP, an initiative by the International Telecommunication Union supported by a number of international non-governmental actors including Save the Children and private companies, a set of high-quality, research-based guidelines were developed in 2009. The development process was cooperative and welcomed feedback from all members of the initiative. As such, it is expected that COP might potentially benefit children and communities in all countries. The guidelines focus on safer ICT use and targeting, respectively, the stakeholder groups of: children; parents, guardians and educators; industry; policy makers. Summarized points from the guidelines are listed below.

Guidelines for Children

Guidelines for children include advice on potentially dangerous behaviors such as cyber-bullying, grooming and sexting, as well as online exploitation. The overall purpose consists in empowering children and youth through education and awareness raising initiatives. Guidelines are split by age group in recognition of the specific needs of each phase of psychosocial and physical development. Children aged 5-7 are mainly referred to parental supervision, children 8-12 are advised on “netiquette” and on how to react to online abuse, while tips for children over 13 particularly focus on independent and critical thinking while on the internet.

Guidelines for Parents, Guardians and Educators

These guidelines point out gaps between adult perceptions on children’s activities on the internet and what children actually do while online, calling for more alert on potential dangers. The overall purpose of this set of recommendations is to encourage...
responsible adults to make their child's internet experience a positive one by discussing and educating about online safety and setting reasonable rules. The guidelines also stress the importance of having basic IT skills so as to adequately support children and prevent risks.

**Guidelines for Industry**

By presenting relevant case studies on exploitation of children via ICT, these guidelines recommend that the industry adopt specific policies including provisions for coordination, cooperation, interoperability and codes of conduct by segment, common complaint rules, common standards and parental consent procedures. Besides, ICT companies are encouraged to organize awareness raising activities for parents and children, and to consider initiating (more) responsible work in related areas of operation.

**Guidelines for Policy Makers**

The added value of this set of guidelines consists in possible strategies that policy makers may adopt with the purpose of improving the system of prevention and protection at the state level, including establishing a thorough legal framework, enhancing law enforcement capabilities, setting out appropriate reporting mechanisms, and investing in education and awareness raising. The guidelines also include a national checklist as a tool to help policymakers better focus resource allocation with medium and longer term prioritization of planned activities.

**System, Implementation, Operational**

As discussed in section 1.c., Telenor mobile carrier in APV and in Montenegro is using a blocking filter to prevent access to inappropriate contents. If matched by comprehensive agreements with relevant law enforcement agencies and extended to all other mobile carriers, such technology may represent an important beginning in the fight against exploitation of children via ICT (see further discussion in the following section).

### 3.b. Recommendations for Advancement in the Prevention and Protection of Children from Exploitation Via ICT

Upon completion of field work and analysis of the legal framework related to the phenomenon, Ombudsman Institutions participating in the research developed a set of relevant recommendations for advancement in the prevention and protection of children from exploitation via ICT at the regional level. Although local specificities need to be taken into account when translating such recommendations into action, an overarching, transnational approach is beneficial to resolve a phenomenon by itself presenting international ramifications. Mirroring the presentation of shortcomings listed in table 5 (see section 2.c.), the report will now attempt to respond comprehensively to each identified challenge and obstacle turning them into operational suggestions. Information reported below is organized in a continuum from prevention to protection and in the analysis of the main areas of action in which action is recommended, specifically targeting groups of stakeholders.

**Awareness Raising, Capacity Building, Civil Society Participation**

**Relevant State Institutions**

- Strengthening comprehensive knowledge of professionals by organizing regular specialized capacity building activities and trainings on the subject, including educational initiatives aimed at furthering a sense of motivation and responsibility for child welfare in professionals and providing them with practical training on how to recognize and help a victim
- Distribution of the present research in all relevant state institutions and online

**General Public**

- Organize roundtables, public debates, trainings, workshops, and other interactive platforms for exchange of information in community-based and school-related contexts to help parents develop overall good parenting skills, with a specific focus on training them on children's rights, raising their awareness of the phenomenon, and developing basic IT skills to protect children from exploitation via ICT
- Develop and mainstream adequate terms in local languages by comprehensively interpreting key definitions (currently

---

30 For specific recommendations in APV, Montenegro and RS please refer to individual reports.
in English) in the field of internet child exploitation with the necessary cultural sensitivity so as to ensure that they are appropriately and predominantly used by all stakeholders including those operating in the judiciary sector

- Organize a public campaign with the purpose of raising awareness on the risks connected with the use of ICT and means of protection, specifically targeting parents and children with a particular emphasis on the concept of “grooming”
- Distribution of the present research in all relevant public venues and online
- Trigger a public debate on the role and responsibilities of the private sector in combating exploitation of children made possible by the use of their networks and services, ideally leading to grassroots civil society initiatives aimed at increased commitment to online child safety on the part of ICT companies
- Deliver to journalists a comprehensive training on children’s rights as well as on specific ethical principles and standards in treating news on exploitation via ICT, with the purpose of encouraging the production of related quality news pieces with a clear educational and prevention function

Children

- In conjunction with Ministries of Education, develop and implement a state-level educational program targeting children from their earliest age to raise their awareness, build their capacities, and enhance their participation and empowerment with a specific focus on the prevention of exploitation via ICT, sexting, grooming, and cyber-bullying. Such program should be based on existing best practices and unfold in the form of media events, public debates, workshops, trainings, seminars, including the following themes: key facts, dangers and safety tips connected to internet and cell phone use, non-violent communication, peer violence, “netiquette,”31 children’s rights and means of protection, different roles of responsible adults in ensuring that children are protected from violence, how to access locally available protection services in case of trouble
- In conjunction with Ministries of Education, empower teachers, pedagogues and psychologists to organize quality free-time activities and initiatives including sport, cultural and recreational events providing children and youth with forms of entertainment and organized free time that are alternative to the use of ICT, and promoting physical wellbeing, social interaction and verbal skills

Legislation, Policy Development, Instruments and Mechanisms

Relevant State Institutions

- Take the necessary political and administrative steps to ensure full reception of international legal standards into national legislations, in particular reception of art. 23 of Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, and introduction of criminal offences of “Inducing a juvenile to witness sexual acts” (RS) and “Use of computer network or communication through other technical means to commit criminal offences against sexual freedom involving a juvenile” (Montenegro and RS)
- Initiate and support the necessary legislative developments to encompass key concepts (or indicate how to include them in an interpretation of norms in force) in the area of exploitation of children via ICT in national legal provisions so as to fill the current legal vacuum with specific criminal offences
- Establish a common recording and prosecution system allowing for efficient exchange of information among all relevant state institutions including a consistent database
- Develop efficient networking mechanisms between existing SOS lines/web pages to report cases of exploitation and relevant institutions aimed at taking adequate protection measures

General Public

- Create an experts group including representatives from all stakeholders with the purpose of drafting legal regulations containing binding minimal standards in the area of online child safety for ICT companies, based on existing international protection standards, possibly requiring them to advertise web filtering services and child safety software as optional within internet and mobile phone plans

---

31 Netiquette is commonly defined as a set of unwritten norms concerning appropriate behaviors on the internet.
System, Implementation, Operational

Relevant State Institutions

- Increase public spending at the state level with the purpose of organizing prevention activities targeting professionals from relevant state institutions
- Establish a multidisciplinary, multi-sectorial system of protection including all relevant institutions and actors and encompassing all necessary bylaws and administrative norms and mechanisms to ensure smooth and efficient implementation of legal regulations, with a special focus on the development of clear protection policy guidelines in case of exploitation of minors via ICT
- Formalize existing platforms of multi-sectorial communication to advance opportunities for exchange of information on reported cases of exploitation of children via ICT, based on common monitoring practices
- Provide all relevant state institutions, in particular in the area of law enforcement and education, with state-of-the-art equipment to improve their technical capacities in the area of prevention and protection
- Improve the overall professionalism and efficacy of the judiciary system in dealing with cases of exploitation of children via ICT by organizing specialized capacity building activities and trainings for prosecutors focusing on a discussion of existing options for strengthening penal policies, resulting in harsher sentences for perpetrators
- Develop a nationwide follow-up system including psychosocial support services for victims and rehabilitation therapy for perpetrators based on existing best practices
- Establish more solid methods of networking and collaboration between local and all European and worldwide centers which are working on the issue
- Strengthen and systematize collaboration between all ICT companies and law enforcement institutions, creating mechanisms by which (blocked) attempts to access inappropriate contents are duly investigated and prosecuted

General Public

- Create regular opportunities for exchange of information, logistical and financial coordination of joint efforts between governmental and civil society sectors to combat the phenomenon (e.g. conferences, round tables, tenders for research projects, study groups, etc.)

Appendix

**LIST OF RELEVANT INTERNATIONAL ACTS FOR THE PURPOSES OF THIS RESEARCH** (in order of adoption)

- Universal Declaration of Human Rights (1948)
- Convention for the Protection of Human Rights and Fundamental Freedoms (1950)
- International Covenant on Civil and Political Rights (1966)
- International Covenant on Economic, Social and Cultural Rights (1966)
- Convention on the Elimination of All Forms of Discrimination Against Women (1979)
- CoE Committee Ministers Recommendation (91) 11 Concerning Sexual Exploitation, Pornography and Prostitution of, and Trafficking in, Children and Young Adults
- Resolution 1099(1996) of the CoE Parliamentary Assembly on the Sexual Exploitation of Children
- Convention concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labor (1999)
- Convention on Cybercrime of the Council of Europe (2001)
- Recommendation (2001)16 of the CoE Committee of Ministers on the Protection of Children against Sexual Exploitation
- Resolution 1307(2002) of the CoE Parliamentary Assembly on Sexual Exploitation of Children
- Convention on Action against Trafficking in Human Beings (2005)