World Vision®

A Study on Child Online Safety in Albania

Research Report

World Vision International is a Christian relief, development and advocacy organization founded in 1950, which is now working in 100 countries. The organization is dedicated to working with children, families and their communities worldwide to reach their full potential by tackling the causes of poverty and injustice.

World Vision started its programmes in Albania and Kosovo in 1999 and 1998, respectively, as an emergency response to support people and families displaced by the war in Kosovo. These emergency relief operations have gradually transitioned into sustainable development programming. Today, World Vision's goal in Albania and Kosovo is to empower communities to bring about social, physical and spiritual transformation.

World Vision Albania assists children, their families and communities through ten Area Development Programmes (ADPs) in Shkodra, Dibra, Kurbin, Lezha, Durres, Tirana, Elbasan, Korca, Librazhd and Vlora. In the years following the crisis in Albania, World Vision has mainly been focused on rural development; however, due to rapid urbanization, World Vision has also included several peri-urban areas in its programming. World Vision is working together with Albanian communities in education, child protection, youth and economic development.

More recently, World Vision in Albania has developed programmes with a special focus on child trafficking and child safety online within the Child Protection Sector, aiming to raise awareness, establish and reinforce referral and reporting mechanisms as well as encourage coordination and collaboration among governmental and nongovernmental stakeholders.

World Vision in Albania (WVA) is the host country for the Child Protection and Participation Learning Hub (CPPLH) for World Vision's Middle East and Eastern European egion since 2013. As a result, WVA in collaboration with CPPLH is undertaking several research and pilot projects in child protection and participation.

Table of Contents *(click the heading or subheading to go to the page)*

Acronyms / Terms Used

ALCIRT- Cyber Agency for Cyber Security

AMSD- Audiovisual Media Services Directive

CRCA- Children's Human Right Centre

EPRA- Electronic and Postal Communication Authority

EU – European Union

Europol- European Police Office

Interpol- International Criminal Police Organization

ISP – Internet Service Providers

IT- Information Technology

MES-Ministry of Education and Sciences

MIICT -Ministry of Innovation and Information Communication Technology

MS PiL- Microsoft and Partners in Learning

NAEC- National Authority for Electronic Certification

NAIS - National Agency for Information Society

PISS-Provider of the Information Society Services

SOCA- Serious Organized Crime Agency

1. Acknowledgements

This research has benefited from the support and collaboration of many. I acknowledge and thank World Vision's staff and peer educators, experts, peer reviewers, advisers, and consultants whose commitment and dedication have made the qualitative and quantitative part of the research possible. These include in particular Child Protection and Participation Learning Hub and Research Initiators B. Zogaj and M. Yamanis, R. Stana, J. Hajdaraj, E. Bowerman, A. Kallciu, M. Jaku, J. Dogani, E. Ikonomi as well as the WV Regional Advocacy Team that funded this research.

A number of representatives from other agencies also gave time and contributed their views and expertise through formal interviews. We gratefully acknowledge this support. These are, among others: Mrs. I. Malolli, National Agency for Information Society; Mr. R. Papa, Legal Advisor at the Electronic and Postal Communication Authority; Mr. E. Kerlukun, Director of the Cyber Crime Unit; Mr. Z. Hoxha, the Head of Cyber Security at Council of Ministers; Mr. S. Ymeri, and Mr. H. Kopani, Ministry of Social Welfare and Youth; Mr. S. Muca IT Expert at Microsoft, Representatives of ALBAtelecom & Eagle Mobile. We would also like to thank representatives of other NGOs active in similar projects such as Mr. A. Hazizaj, Head of CRCA and Mr. A. Goxhaj Head of the Office of the Consumer Protection.

Appreciation is extended to those who participated in the research survey - the field staff, peer educators and youth from Dibra, Shkodra, Tirana, Elbasan, Korca and Vlora.

Finally, special thanks and appreciation goes to Dr. Fabian Zhilla from the Canadian Institute of Technology for conducting the qualitative part of the research, the legal and policy review report, as well as to Mr. Albana Nelaj, the Director of EUNACAL Institute, for analyzing the surveys and producing the quantitative report.

2. Executive Summary

This report shows the extent to which Albanian children access the Internet compared to other European nations and the risks currently posed to children accessing the Internet. In addition, the report reviews the current steps taken by the Albanian authorities to regulate and provide adequate protection regarding children's safety online. The Albanian measures are then compared to those suggested by the EU and its recommendations on how to reduce the risks faced by children while online. World Vision has conducted qualitative and quantitative research involving children and young people, as well as parents and other sources at the community, national, and international levels.

A total of 821 field-tested and age-appropriate surveys were returned by youth between the ages of 13 and 18 out of the 1000 that had been distributed through World Vision's trained field staff or peer educators. Each survey was followed by focus group discussions to help improve the quality of the narrative. In order to reflect geographical variations across Albania, the sample was selected from both rural and urban areas in six different regions of the country including Tirana and Elbasan in the center, Dibra and Shkodra in the north, and Korce and Vlora in the southeast. Previous World Vision research indicated that the surveys would be best distributed in electronic or paper formats to schools and also to Internet cafes in order to reach youth who do or do not attend formal education.

The results demonstrated that improving online safety for Albanian children should receive the utmost priority. Within the country, 85% of the youth surveyed have a computer at home with 62% of those devices being located in their rooms while Internet cafes are also widely accessible in both rural and more urbanized areas. However, the most popular devices for Internet access are phones (65%), PCs (69%), and laptops (43%). Of those who responded, 44 percent state that they utilize the Internet to watch pornographic material daily while 62 percent confirm having friends who visit similar websites. Bullying, password theft, and unintentional porn viewings happen to 45 percent of responders every day. Further, 47 percent of the young respondents have been contacted online by a stranger within the last year who,

in 40 percent of the cases, was a foreigner. The rates of risk within the age range of 13 to 18 are cause for serious concern and are compounded by low rates of online safety information sharing. Only 44 percent of children receive information on online safety from parents or from various outlets for reporting online incidents. This suggests a significant 'IT generation gap' in Albania. Children view parents (48%), friends (37%), and siblings (36%) as the first persons to report an issue to, while teachers (32%) and police (27%) are the least likely people they would report to.

Counteracting the risks of online activity by youth is the responsibility of many actors, such as the Albanian government, parents, mobile service providers, Internet Service Providers (ISP), and schools. World Vision recommends that all stakeholders should promote awareness as a key to maximizing the protection of children. The government should also work in collaboration with other actors to provide better online safety for children. Mobile operators and ISPs should be obliged by legislation to provide parents with options to restrict Internet browsing to unsafe content. Similarly, public Internet access locations should collaborate with the government to create a safer Internet environment. This collaboration should involve the government issuing usernames and passwords assigned to every child that are required upon signing into public Internet cafés. In doing this, the content available would be limited to child-friendly material. Similarly, the Internet café can set up child friendly spaces in which children can access computers with their information while also being protected from visual material being viewed by adults in other sections of the establishment. Additionally, with levels of Internet usage so high, youth friendly reporting mechanisms should be set up through a government appointed agency to monitor and respond to risks. Other additional measures include increasing sources of awareness raising, such as school curriculums, anti-bullying initiatives, and educating parents to be better providers of online safety information for their children.

In order to identify gaps in the Albanian legislation regarding Internet child protection and addressing the above reported statistics, a mixed research methodology was applied. The study reviewed Albanian legislation in the context of EU policies. A number of semi-structured interviews were conducted with representatives of various stakeholders. These originated from the Ministry of Education and Sport (formerly the Ministry of Education and Science), the Ministry of Innovation and Public Administration (formerly the Ministry of Information and Communication Technology), the National Agency for Information Society, the cyber crime unit of the State Police, and the cyber security unit of the Council of Ministers, Civil Society, and ISPs. Other primary sources were also reviewed. These include records of parliamentary discussion related to relevant legislation. Based on these interviews and reviews, recommendations were formulated for policy making and improving current legislation.

Albania has a variety of relevant laws in place; the review, however, found that these are insufficient for adequately protecting all Albanian youths from online risks. One common concern within current legislation is a lack of clarity or language that specifically defines terms and roles in protecting children from harmful content. For example, Law no. 97/2013 and Law no. 9902, date 17.4.2008 do not provide sufficiently clear definitions on terms that are relevant to child safety online. Law no. 9918 lacks specific language for protecting children. Other laws such as Law no. 10128 need to define Protocols for appropriate action, especially regarding the situations in which Providers of Information Access Services are allowed to block possible illegal actions by subscribers. Some laws that have been created for guarding the rights of children, such as Law no. 10347 "On the Protection of Children Rights", should be expanded to include protecting children from online risks and their side effects. In general, laws must also be expanded to better define what constitutes child pornography and what acts are illegal in this context, e.g. abetting, attempting, or instigating the production of illegal materials.

World Vision's overarching recommendations for policy making involve raising the awareness and cooperation amongst all relevant stakeholders to create a more effective, protecting environment for youth online. The government should give priority to the interests of youth in all future legislation regarding online usage. Additionally, the government could legally require stakeholders to provide comprehensive protection mechanisms to be pre-installed on popular devices. The police could sign Memorandums of Understandings and create hotlines as well as cyber crime units that are trained and adequately staffed to respond to illegal online content such as child pornography. Additionally, the government is advised to

increase their efforts for awareness raising and training among Ministry of Justice staff who are responsible for addressing violations of relevant legislation including possessing or conspiring to produce and distribute child pornography. In addition, ISPs and mobile providers should monitor the content viewed by youth or provide protective software/filter options to parents that are able to prevent the viewing of inappropriate content. The government should also utilize the EPCA to monitor Internet usage in Internetcafes and public spaces as well as increase the ease of access to data directly from ISPS. Finally, the Ministry of Education is recommended to consider integrating online safety into curriculums, both for teacher training and schools.

Introduction

World Vision defines Child Protection as all measures taken to protect, prevent and respond to exploitation, neglect, abuse and all other forms of violence affecting children, especially the most vulnerable. Based on their past work in Albania, World Vision has identified the need for enhanced protection, prevention and effective response in the arena of child Internet safety. Through collaboration with its regional Child Protection and Participation Learning Hub whose mandate is to generate evidence and research regarding program impact on protection and referral mechanisms in the Middle East and Eastern European countries, World Vision has commissioned research on Child Online Safety in Albania. The aim and objectives of the research where informed by the internal development of Albania, as a country in a journey towards the EU accession process, but also by learning generated in other countries in the region that have implemented Keeping Children Safe Online projects.

During the last decade, almost every Albanian family has gained Internet access in their homes or through places such as schools, Internet cafes, bars, restaurants or other public spaces. By the end of 2012 the number of subscribers rose to 215,000, an increase of 24% from 2011.[1] Many children use smart phones and all Albanian mobile providers offer Internet for such devices. The numbers of persons which use this service (GPRS/EDGE) were around 1.4 Million in 2011, 15% more than in 2010.[2] Together with many benefits, the Internet also brings risks, especially when the users do not have the necessary knowledge to navigate safely and respond appropriately if an incident occurs online. This has become even more problematic for children in recent years. Incidents include the stealing of personal information, grooming, exposure to inappropriate content, bullying, and more. Although several positive steps have been taken by the Ministry of Education, the Ministry for Innovation and Public Administration, the National Agency for Information Society, Mobile Companies, and the Cyber Crime Unit, there is still a lack of awareness regarding children's online behaviors, the risks that they face online, and the functionality of response mechanisms that are intended to address cases of abuse.

This research consists of two parts: the quantitative part of the research includes survey findings, recommendations and analysis of child online safety in Albania. Throughout the report, the quantitative analysis compares these findings on Albanian children with the overall situation in the European Union (Barbosa et al. 2013). In the second, qualitative, part of the research, a legal and policy review presents findings and concrete recommendations to harmonize our situation with European standards. The study brings together the voice of children in the community and those of national decision makers,illuminating the steps that are needed to achieve safe internal access for children In Albania.

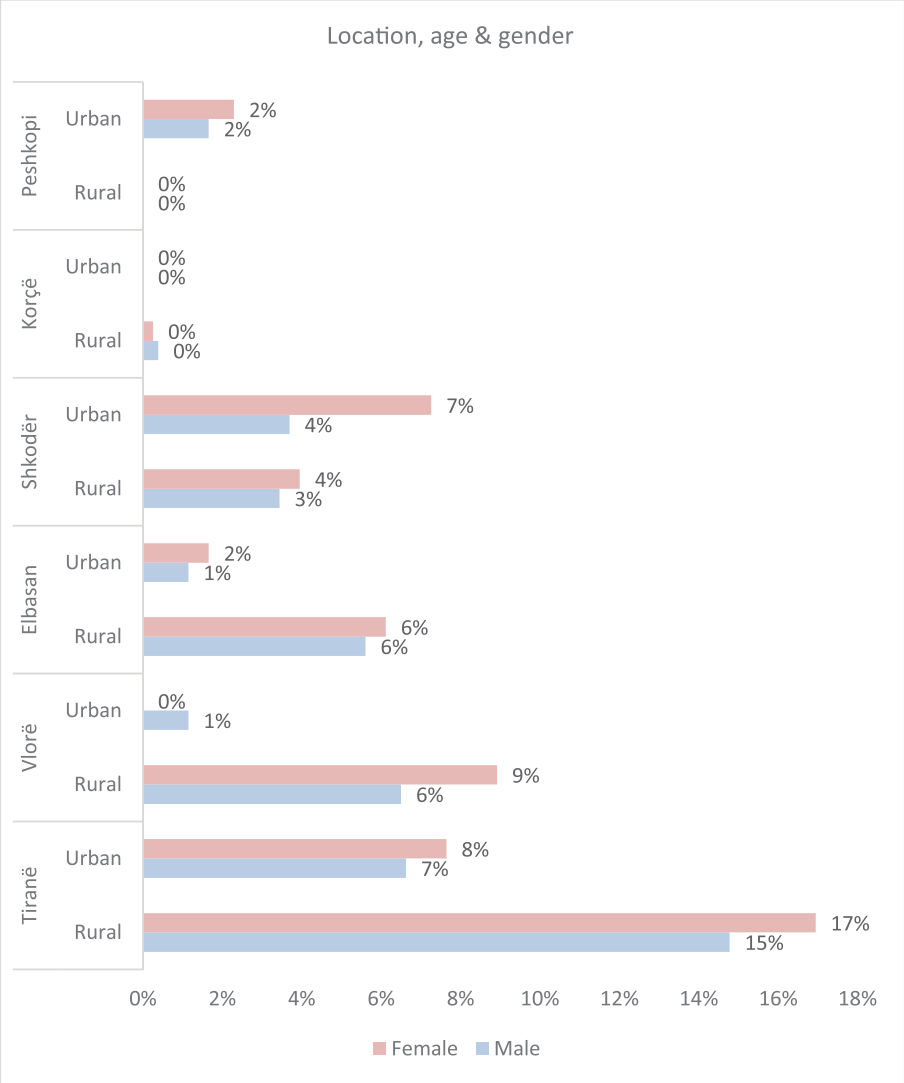
1 See the "Report on the Activity of the Authority of Electronic and Postal Communication for 2012", p.4, available at: http://www.akep.al/images/stories/AKEP/publikime/2013/RAPORTI-VJETOR-2012.pdf
2 See the "Report on the Activity of the Authority of Electronic and Postal Communication for 2012", p.4, available at: http://www.akep.al/images/stories/AKEP/publikime/2013/RAPORTI-VJETOR-2012.pdf

Part I

Survey findings

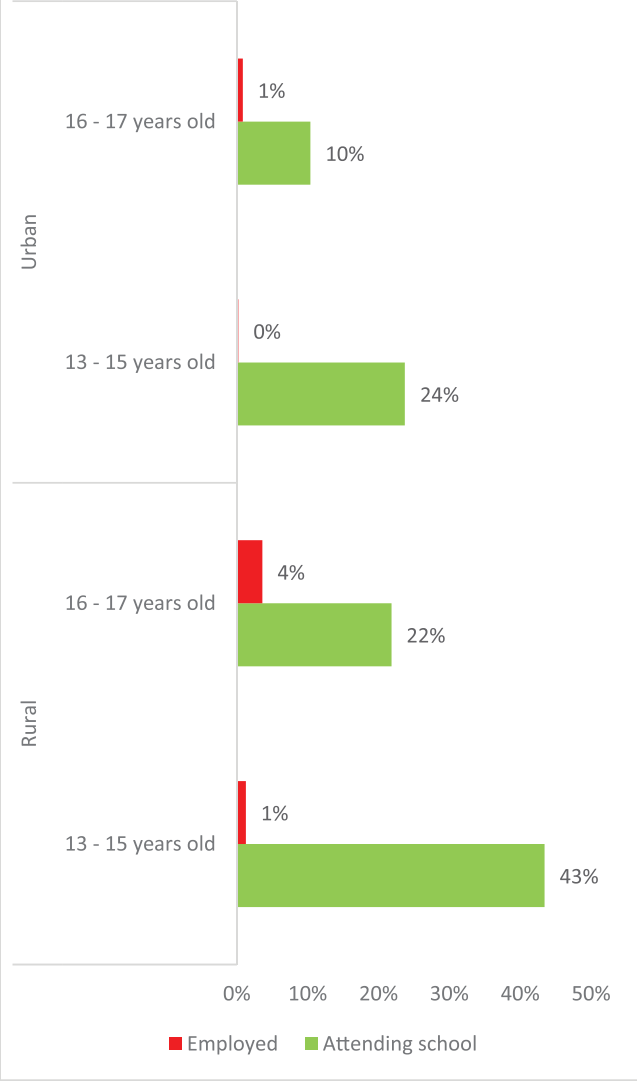
Demographics

Location, age and gender



The sample of this research is composed of children living in the districts of Tirana, Vlora, Elbasan, Shkodra, Korca, and Peshkopi. Responders were between the ages of 13 and 17 years old. Responders mainly resided in rural areas of Albania (67%). Females made up 55% of the respondents. Rural responders were mostly located in Tirana (32%), Vlora (15%) and Elbasan (12%). Urban responders were mostly located in Tirana (14%), Shkodra (11%), and Peshkopi (4%).

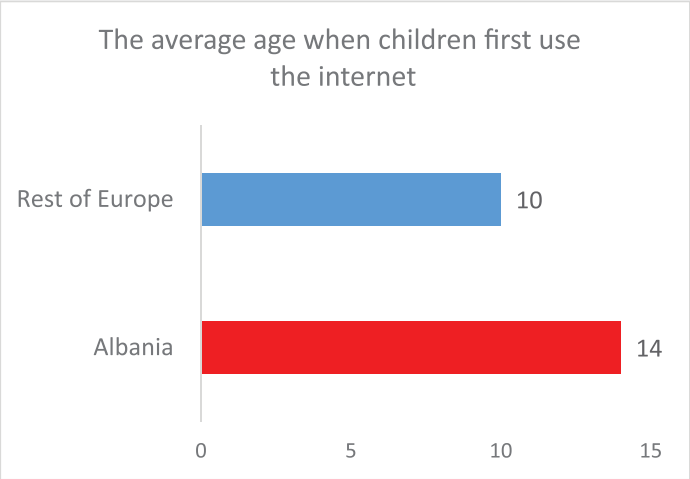
Location, occupation and age group



Sixty-seven percent of respondents were 13 – 15 years old, out of which 65% reside in rural areas. Thirty-three percent of respondents were 16 – 17 years old out of which 33% reside in urban areas.

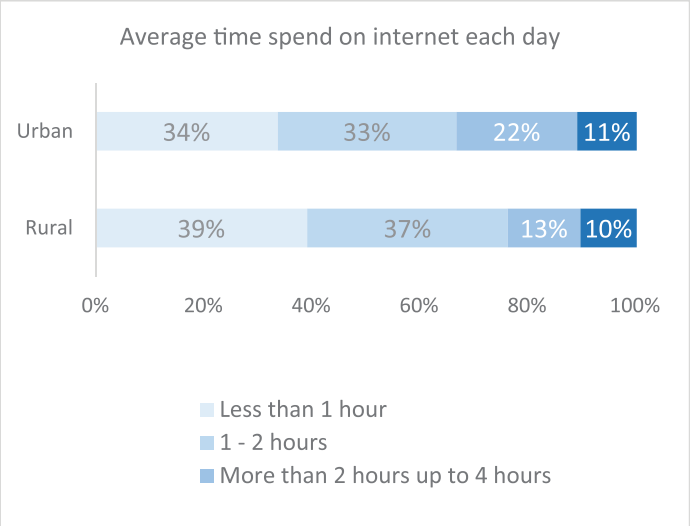
Age of use, times and forms of access

Age of first Internet access



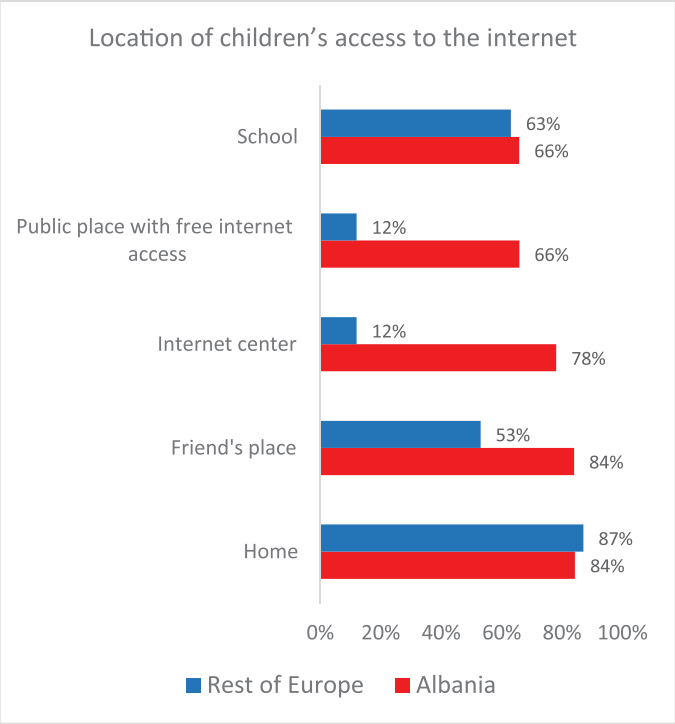
For Albanian children, the average age of using the Internet for the first time is four years higher than it is for children in the rest of Europe. A major reason for this gap may be a stronger presence of a digital divide in Albania. On the one hand, this situation brings to light the risk of underestimating the crucial role of online safety education in early stages of a child's life. On the other hand, a four year delay in access provides an opportunity for the government, businesses and civil society to better prepare for the future by taking immediate actions to adopt an education system that is able to cope with the future challenges to children's online safety.

Average time spent on the Internet each day



Sixty-three percent of children spend one or more hours each day on the Internet. For urban children, this figure is 5% higher than it is for rural children.

Locations of Internet access

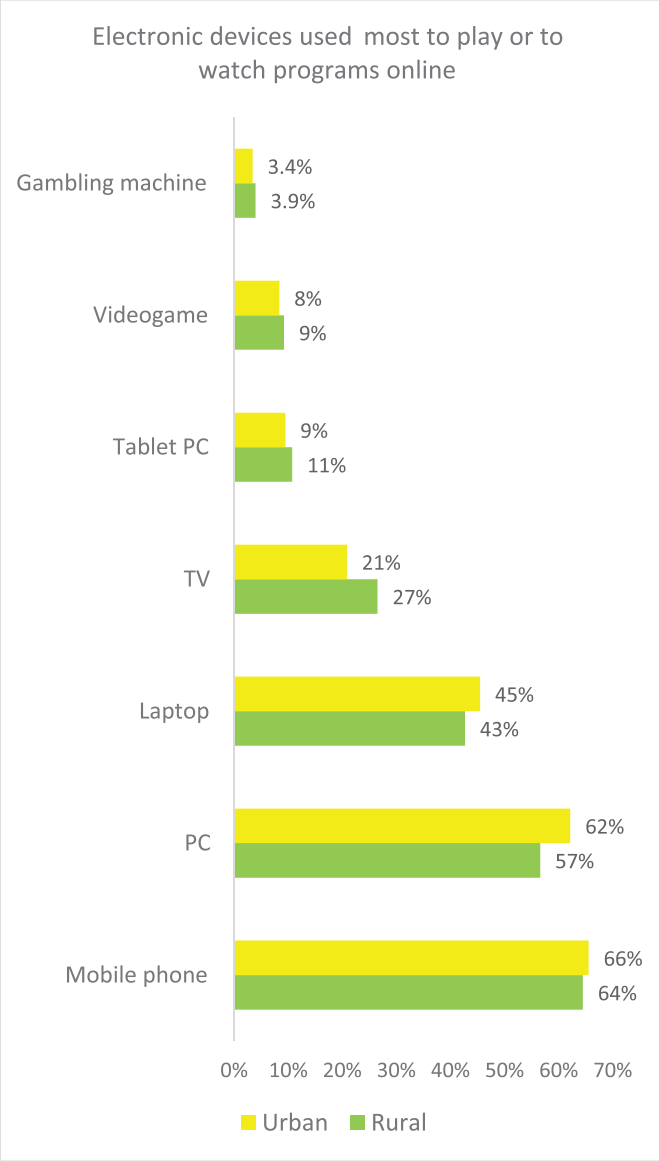


Compared to the rest of Europe, Albanian children have similar amounts of access to the Internet at home. Eighty-four percent of Albanian children and 87% of children in the remainder of Europe have Internet access within their house. The second most common location most used by Albanian children to access the Internet is a friend's home.

These figures are significantly higher among Albanian children (84%) compared to children in other countries of Europe (53%). Rates of Internet access from an Internet café or public location providing free Internet are also significantly higher for Albanian children. These high rates may be an indication of a significant digital divide in Albania. In other words, there is an inequality of access based on various factors such as socioeconomic class.

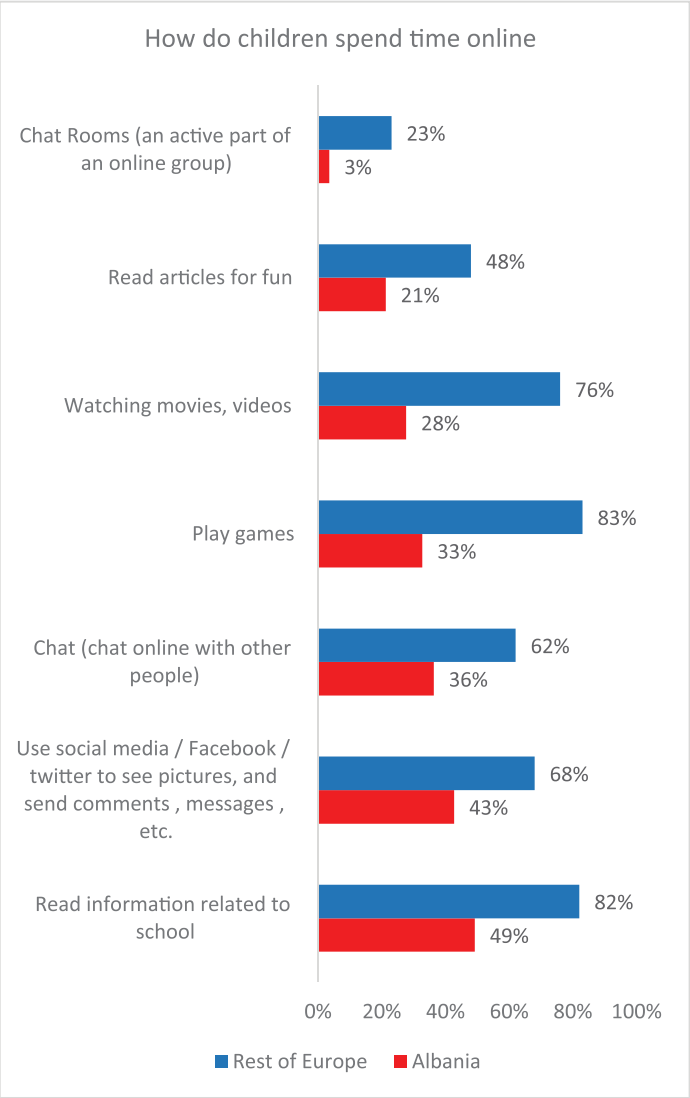
Internet access from schools is similar in both groups with Albanian children at the rate of 66% and children in the rest of Europe at the rate of 63%. This figure might confirm that projects implemented by the Albanian government, local businesses and international or local organizations are making Internet accessible at schools similar to other European nations.

Devices utilized for Internet access



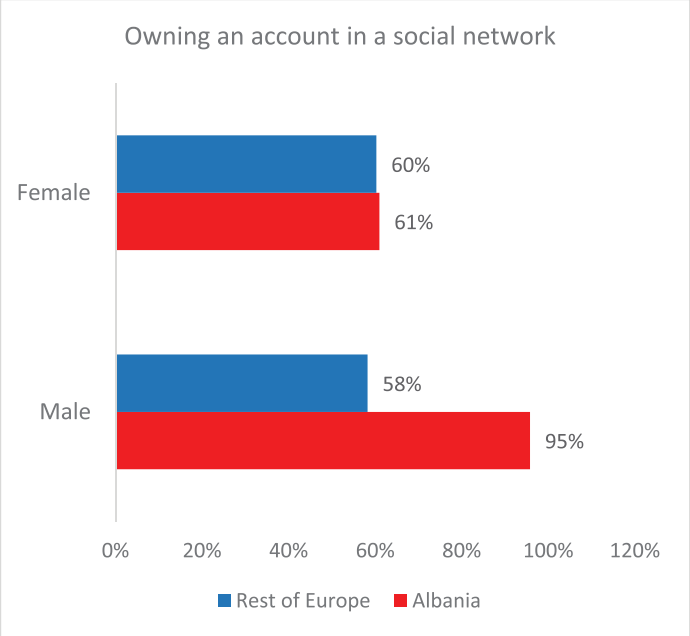
The top three devices Albanian children use to watch or play online are mobile phones (65%), PCs (59%), and laptops (43%). Reports from other European countries reveal that the numbers of children accessing the Internet via mobile phone differ based on their socio-economic classes. Children from higher socio-economic classes have a higher rate of Internet access via mobile phones. It is interesting to notice that for the case of Albania, children of lower socio-economic classes, which are assumed to be the residents of rural areas, have a similar rate of access when compared to children of higher socio-economic class, which we will assume to be the residents of urban areas.

How do children spend their time online?



Compared to other European children, Albanian youth spend less time playing games and watching movies online. Instead, they spend more time seeking information related to school as well as using social media. Low levels of game playing and video watching online are likely due to lower Internet speeds provided to Albanian children. It should be considered that Internet speeds provided by ISPs and mobile operators in Albania are rapidly growing. The government and civil society should be prepared for an increase in usage of these services by children as speeds improve. To prevent the harm and risk produced by an increase in usage of these services, coordinated measures should be put in place. Such services should restrict access to harmful online video content and online games that make children interact with unknown adults.

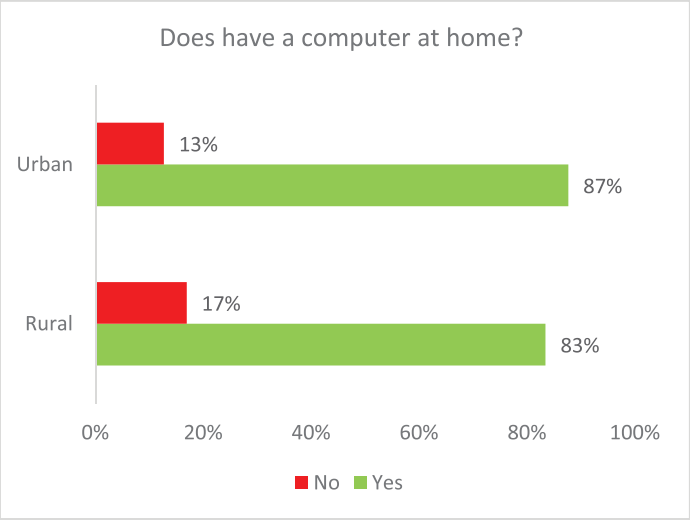
Social network account ownership rates



Compared to other children of Europe, a larger gap in social network account ownerships exists between male and female Albanian children. Female children from other European countries exceed social network account ownership of their male counterparts by 2% while Albanian male social network account ownership exceeds female counterparts by 34%. This large gap between Albanian children needs to be explored further by means of qualitative research focusing mainly on cultural context.

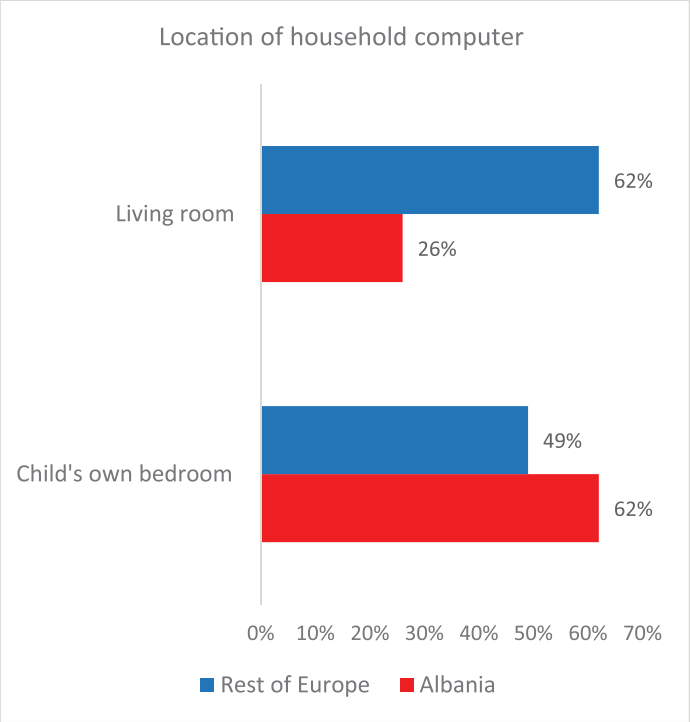
Internet Access at Home

Rate of computers at home



Eighty-five percent of Albanian children that access the Internet have a computer in their home. This figure is slightly higher (4%) for children residing in urban areas. Considering these rates, it is a parental duty to safeguard a child's usage at home. The task is of equal importance for parents of children living in rural and urban areas. Assuming that most parents of children living in rural areas belong to a lower socio-economic class and are less computer literate, their task to safeguard children activities online is more challenging.

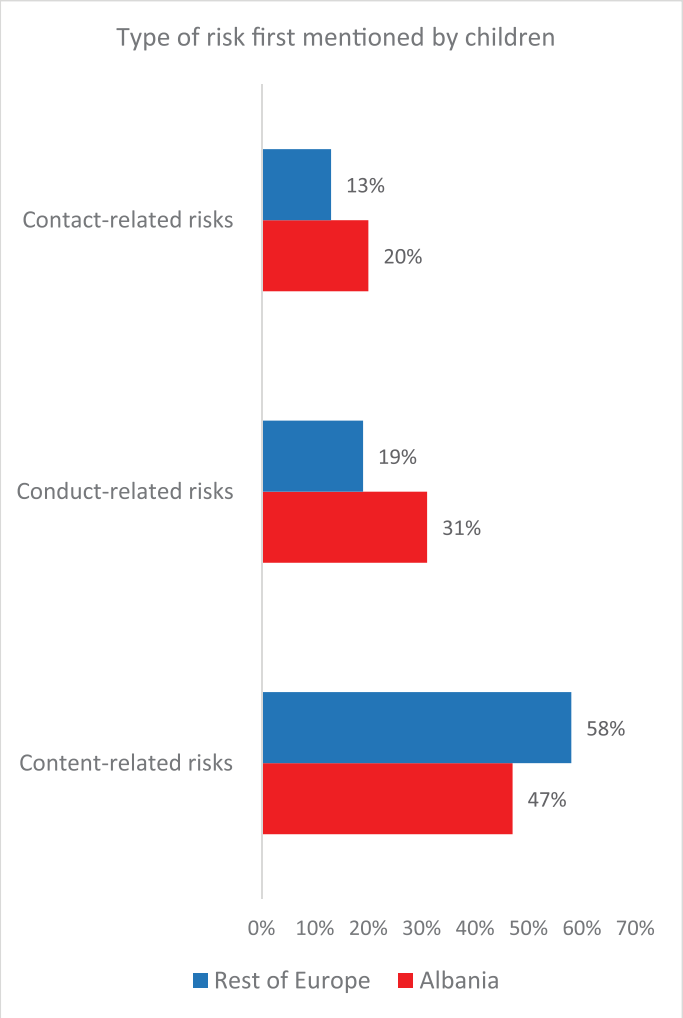
Locations of household computers



In other European countries, the trend among families is to keep computers out of children's bedrooms. Only 49% of children in other European countries have a computer in their bedroom. Conversely, Albanian families prefer to keep computers in the child's bedroom with 62% of children doing so. Having a child's computer in shared rooms of the house, such as the living room, makes it easier for parents to safeguard online activity, especially what content is being accessed (videos, picture, etc).

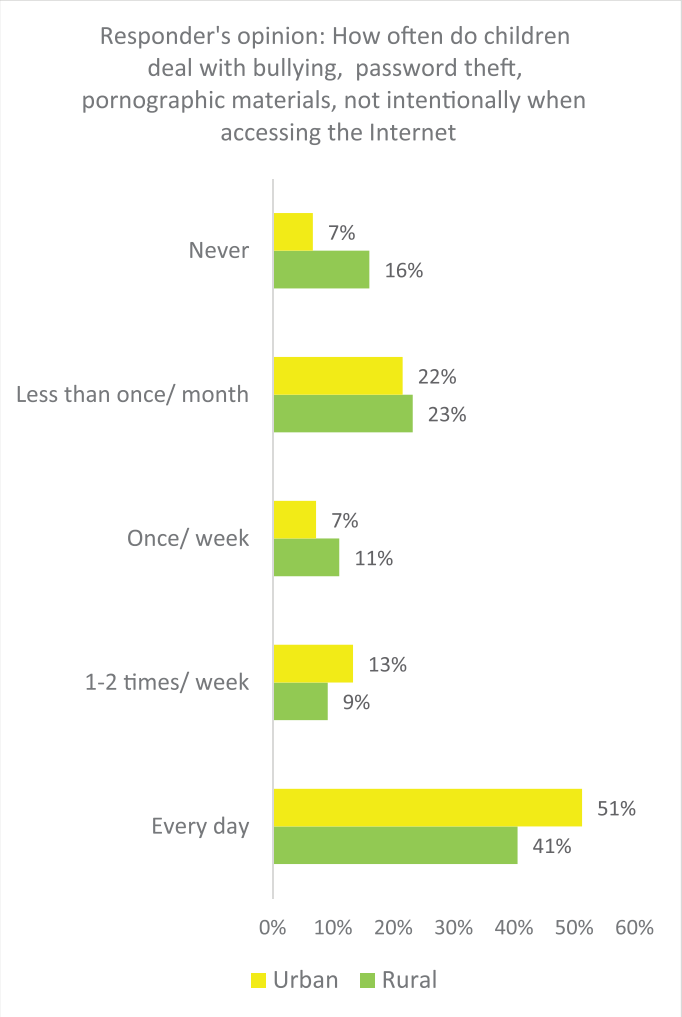
Potentials for Risk and Harm

Most commonly identified risks



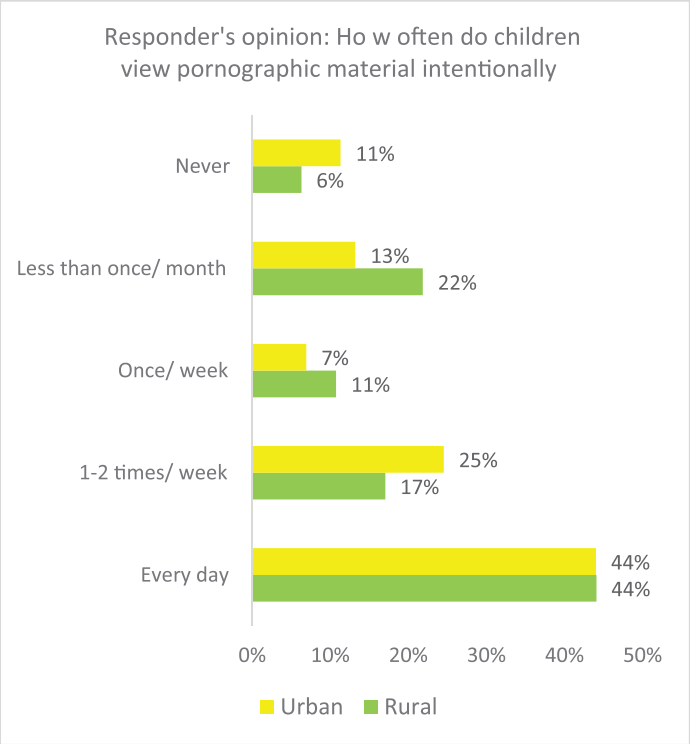
When it comes to perceiving online risks, Albanian children share a similar opinion with children of other European countries. Both groups place content-related risks as the most common issue, followed by conduct-related risks, and contact-related risks. Contrarily to children located in other parts of Europe, Albanian children perceive content-related risks be the most common (11% more). Again, these numbers exemplify the crucial role that parents should play in safeguarding content-related online activities of children at home. It is a task that is difficult to perform if home computers with Internet are accessed from a child's own room and parents lack basic Internet safety knowledge.

How often do children deal with issues such as bullying, password theft or pornographic materials?



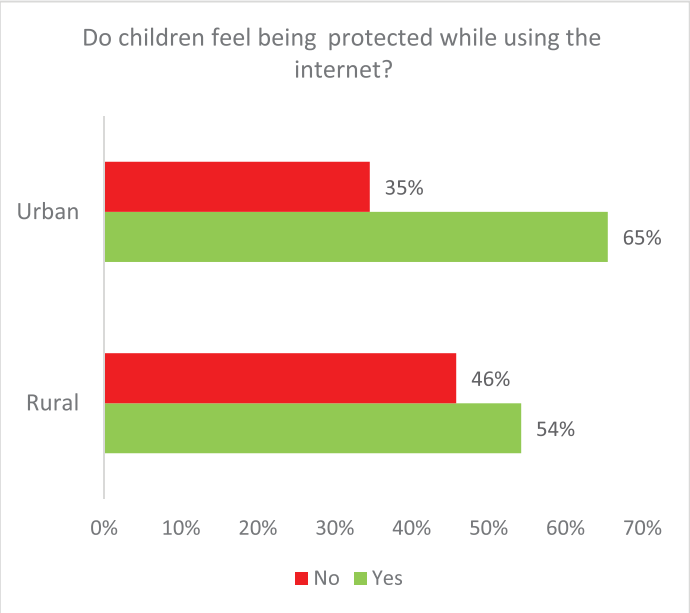
Data reveals that bullying, password thefts, and pornographic material viewing often occur unintentionally when accessing the Internet. These topics pose serious issues for children. Forty-five percent of respondents identified that children have to cope with these issues every day. When compared to children living in rural areas, urban based children seem to be 10% more affected by these issues.

How often do children view pornographic materials?



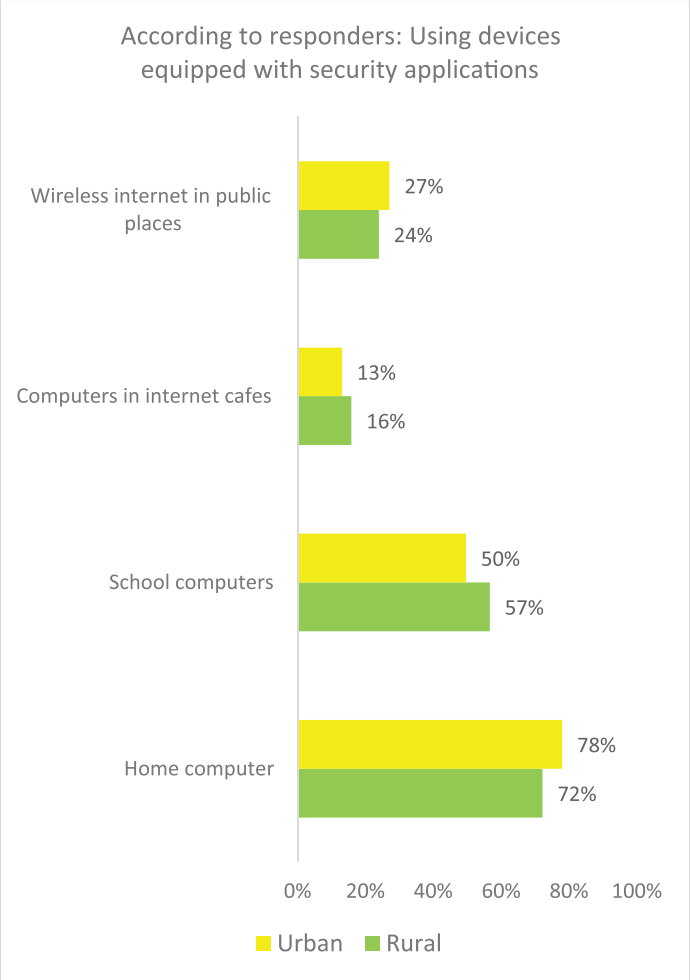
According to responder's opinions, in terms of watching pornographic materials on purpose, children of rural areas tend to have a similar attitude to children of urban areas. Of rural and urban children, 44% perceive that children watch pornographic materials every day.

Do children feel protected while using the Internet?



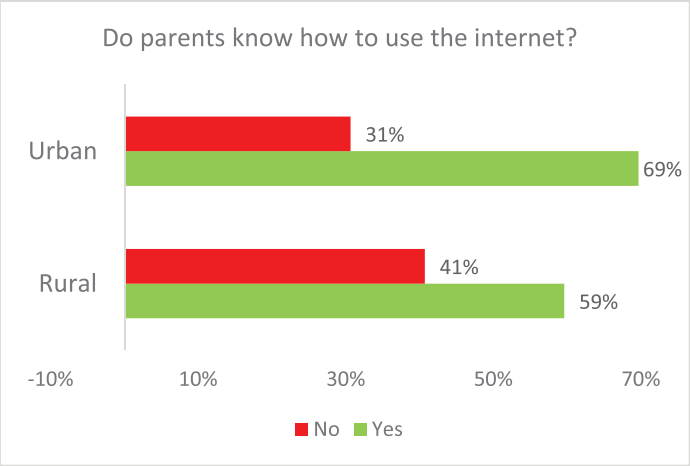
Fifty-eight percent of children interviewed feel protected while using the Internet. Compared to children from rural areas (46%), their urban counterparts feel more protected by 11%.

Are devices equipped with security applications?



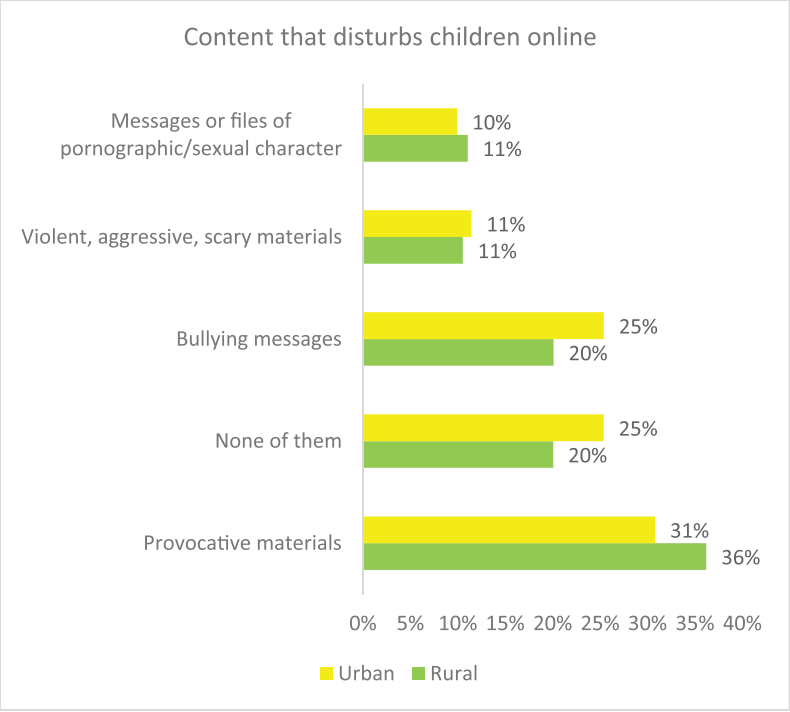
According to responders, 74% of home computers are equipped with security applications. This figure is 54% for school computers and 28% for wireless Internet in public places. The lowest figure is for computers in Internet cafes where only 16% are equipped with security applications. Considering that the online activities of children in Internet cafes are not safeguarded by adults, this figure reveals a crucial issue that needs to be addressed by the government, businesses and civic society.

Do parents know how to use the Internet?



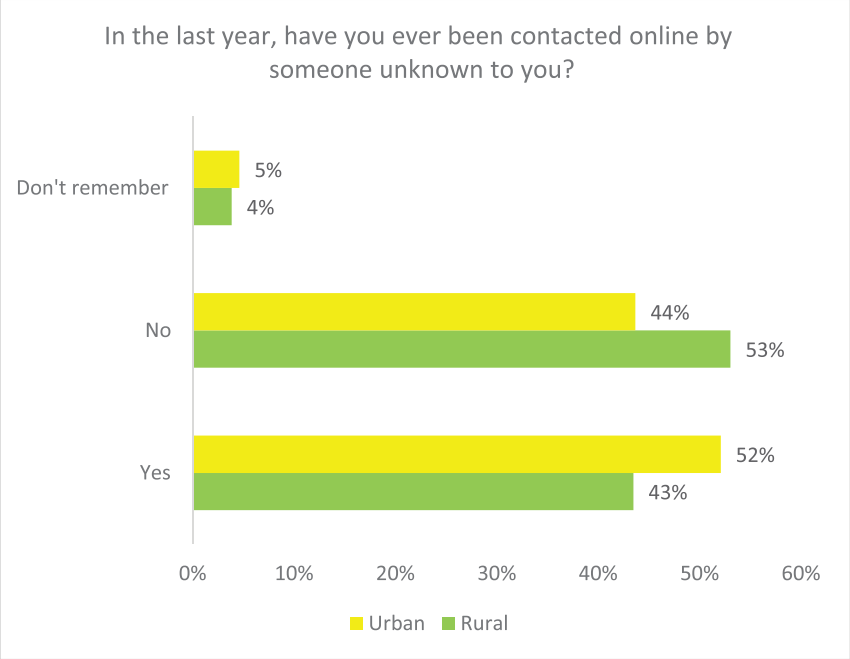
There are significant differences inthe digital dividebetween parents and children in urban areas and those in rural areas. Survey data shows that parents of children living in rural areas have 10% less ICT readiness compared to parents of children living in urban areas.A lower ICT readiness of parents in lower socio-economic classes (rural areas) leads to more online risks for their children.

Content that disturbs children online.



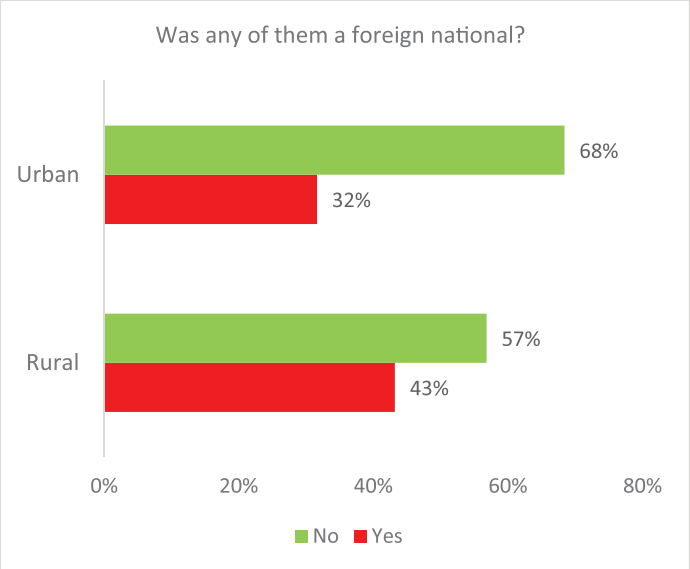
Children interviewed listed provocative materials (26%), bullying messages (22%), and violent/ aggressive materials (11%) as the top problematic messages they have received online.

In the last year, have you ever been contacted online by someone unknown to you?



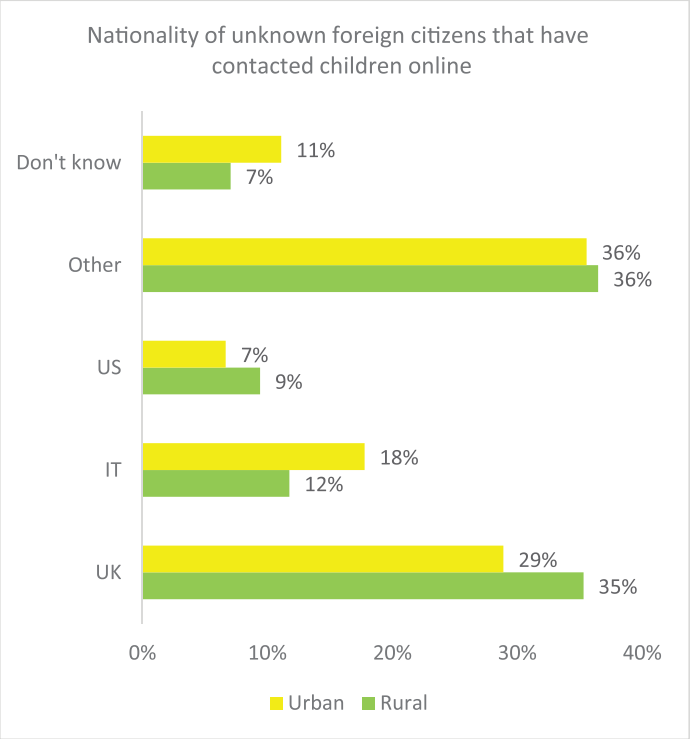
Forty-seven percent of interviewed children admit that, in the last year, they have been contacted online by an unknown individual. This figure is 9% higher for children living in urban areas compared to their rural counterparts.

Were any of the unknown individuals a foreign national?



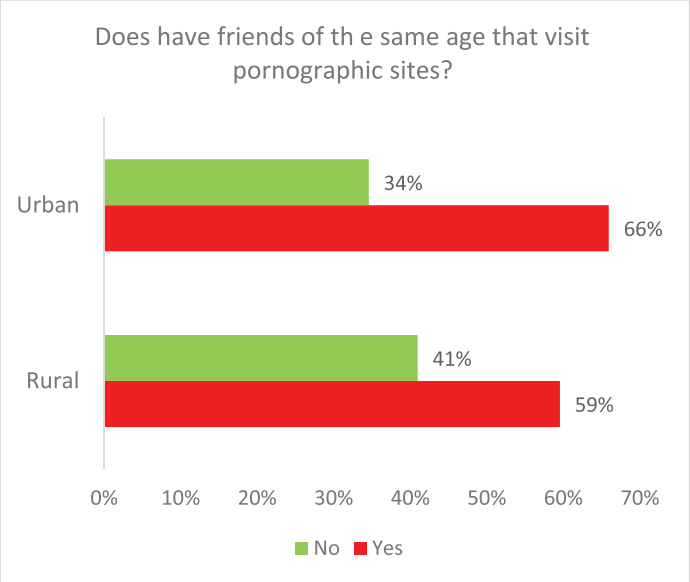
Out of the 47% of children that have been contacted online by an individual in the last year, 40% have been contacted by foreign nationals. This figure is 11% higher among children living in urban areas compared to children of rural areas.

Nationalities of unknown foreign citizens



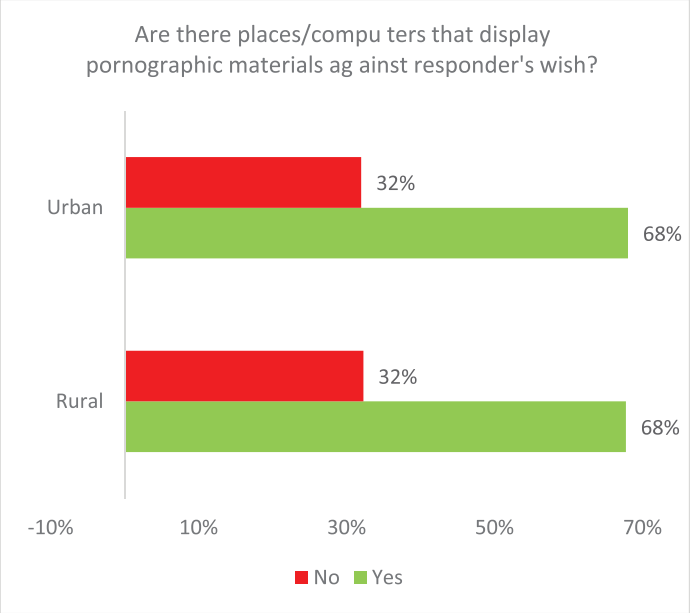
Most of unknown foreign citizens contacting online Albanian children are from the UK (33%), Italy (14%), and the US (8%).

Do you have friends of the same age that visit pornographic sites?



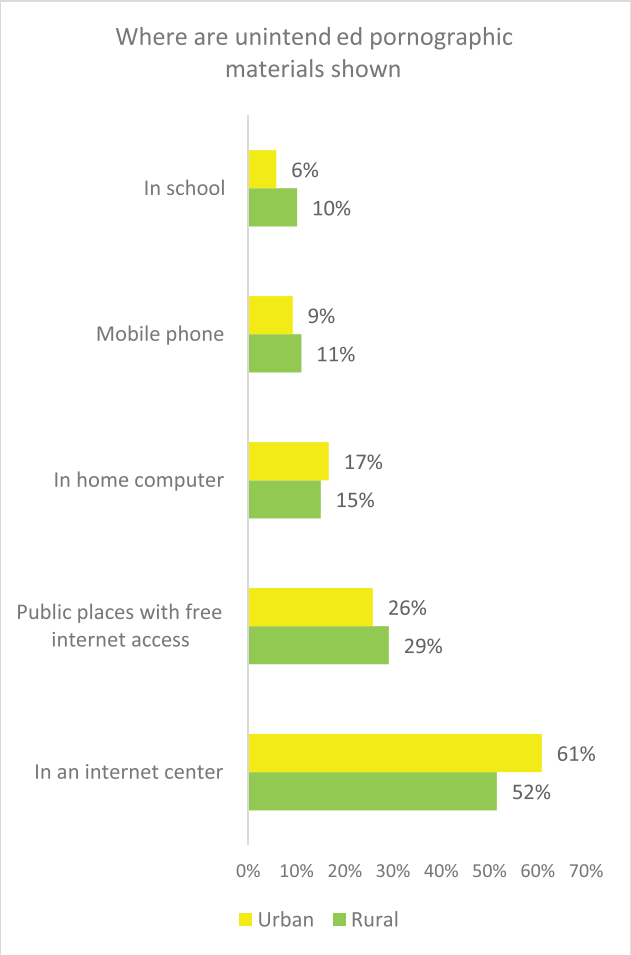
Sixty-two percent of children interviewed confirmed that they have friends that visit pornographic sites. The figure is 7% higher in urban areas compared to rural areas.

Are there places/computers that display pornographic materials against the responder's wishes?



68% of children in both rural and urban areas confirm the existence of places, computers or screens that display pornographic materials against their wishes.

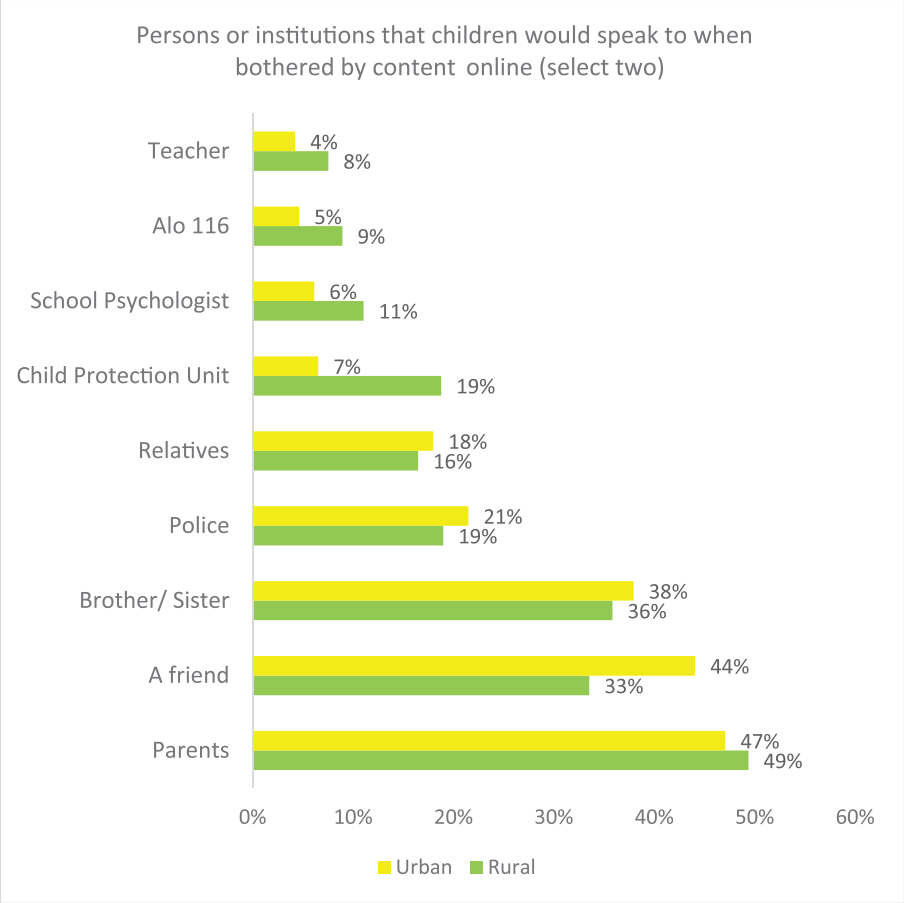
Where are unintended pornographic materials shown?



Most unintended pornographic material viewing takes place in Internet centers. This is noted by 52% of children in rural areas and 61% of children in urban areas. The second most reported location that displays pornographic materials against children's wishes are public locations with free Internet access. Public locations were pointed out by 29% of children in rural areas and 26% of children from urban areas. The critical situation produced by Internet centers needs to be addressed by designing and implementing access restriction policies that enable Internet cafes to become a safe online access environment.

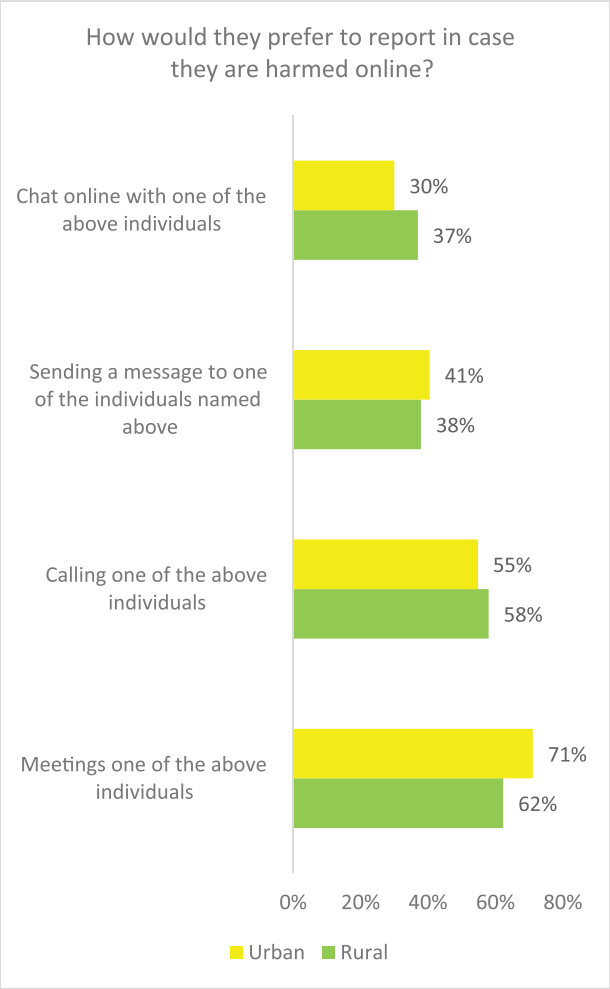
Reactions to Incidents

Persons or institutions that children would speak to when bothered by content online (select two)



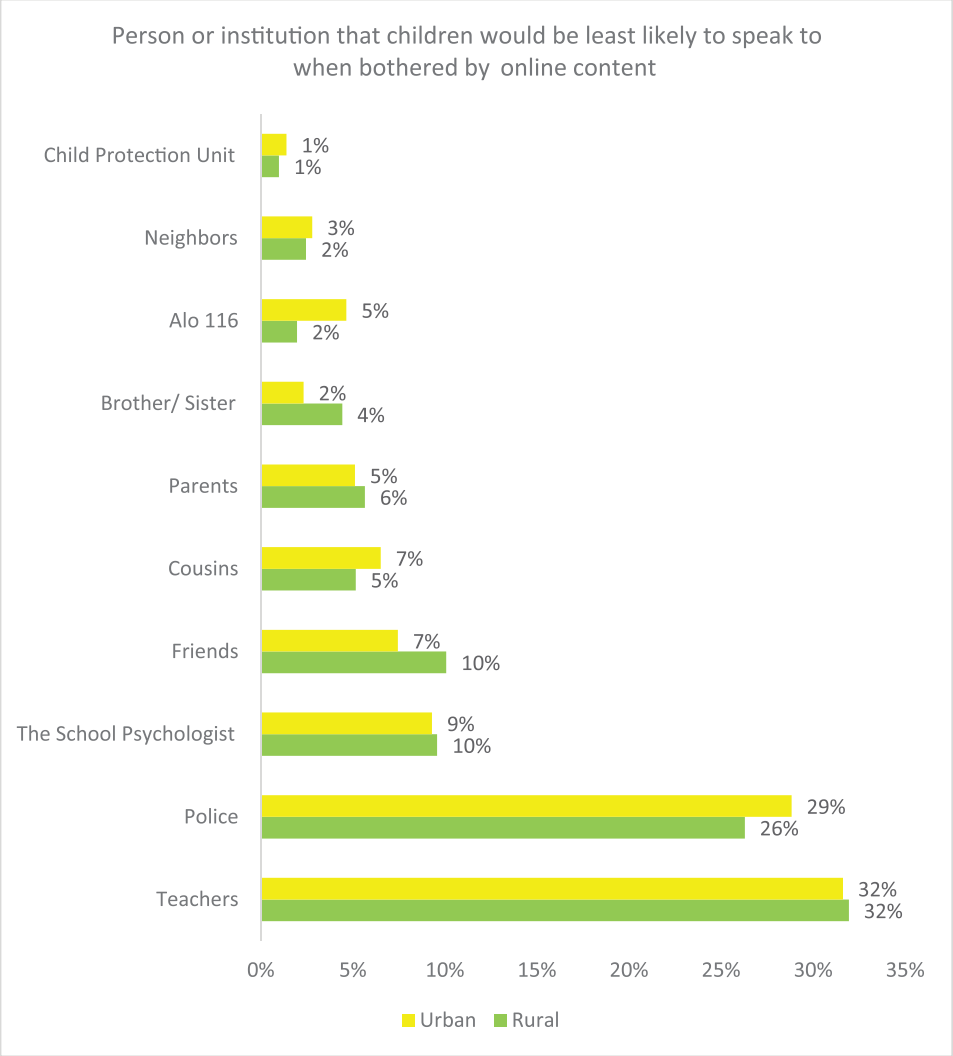
Children prefer to report online issues to their parents, friends, and brothers or sisters. Parents are seen as the first person to whom children should report an online issue based on 48% of interviews. Parents are followed by friends (37%) and brothers or sisters (36%). The individualsto whom children least prefer to report issues are teachers with only 6% of children feeling confident about reporting an online issue to them. It is noted that, compared to their rural counterparts, children of urban areas tend to feel more confident about their friends with a figure that is 11% higher. Both children of urban and rural areas show a high level of distrust towards institutions of the education system and the local government.

How would children prefer to report in the case of being harmed online?



The most preferred communication methods to use when reporting an online issue are meetings (66%), calls (57%), and messages (38%) to the individuals they feel comfortable talking to.

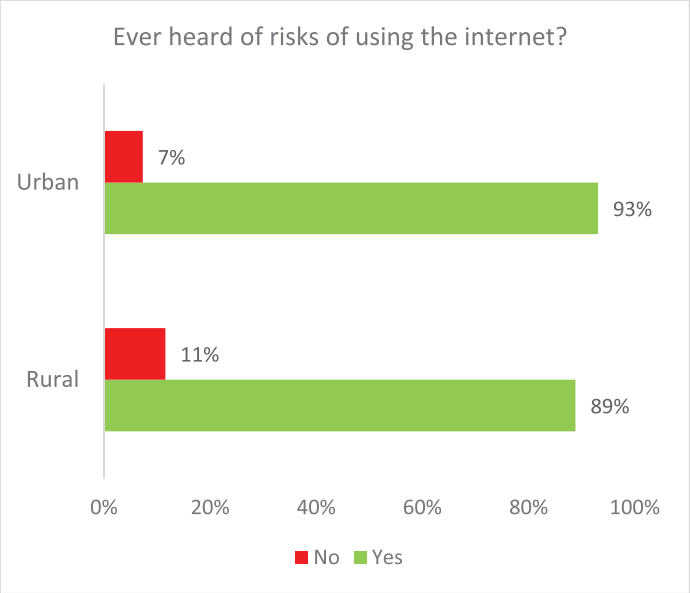
Person or institution that children would be least likely speak to when bothered by online content



In contrast to the previously graphthat depicts the most likely person for children to report to, this graph shows the least likely resource for child reporting. Respondents stated that teachers (32%) are the person they are least likely to report online issues to. Teachers are very closely followed by police (27%) as the least likely point of reporting. At first glance, these statistics seem contradictory in some aspects to the graph previously discussed. However, this question was carefully and strategically crafted to allow deeper insight into the minds of our respondents. What can be drawn from the results are two points: a) children may struggle to trust established structures such as teachers or police and b) that culture may also play a role in dictating who is a trustworthy source. Looking at categories such as friends (8.5%) and parents (5.5%), one can see that family remains a large component for children who experience online issues. These findings allow a cross examination of the children's perspectives to further enforce the notion that culture and trust may have relevant effects on children's responses. Their lack of faith in the system is concerning.

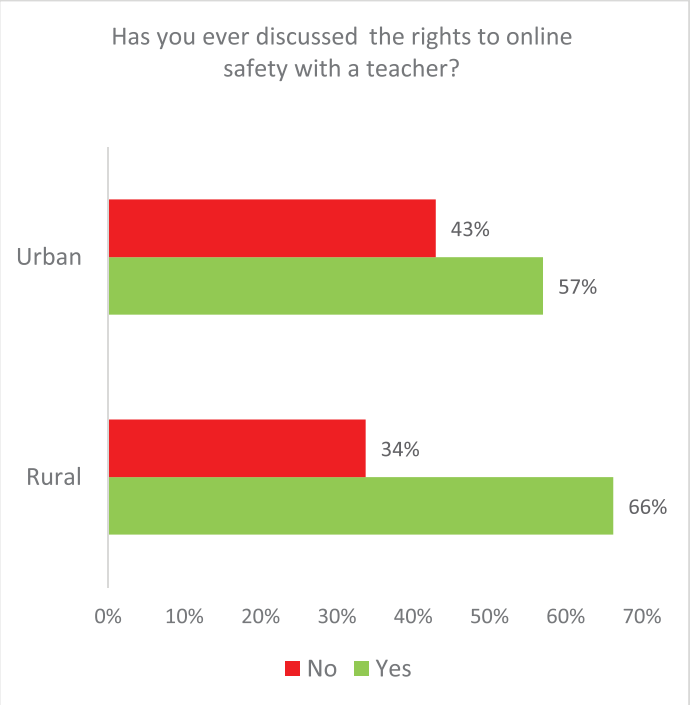
Education and Awareness

Have you ever heard of risks of using the Internet?



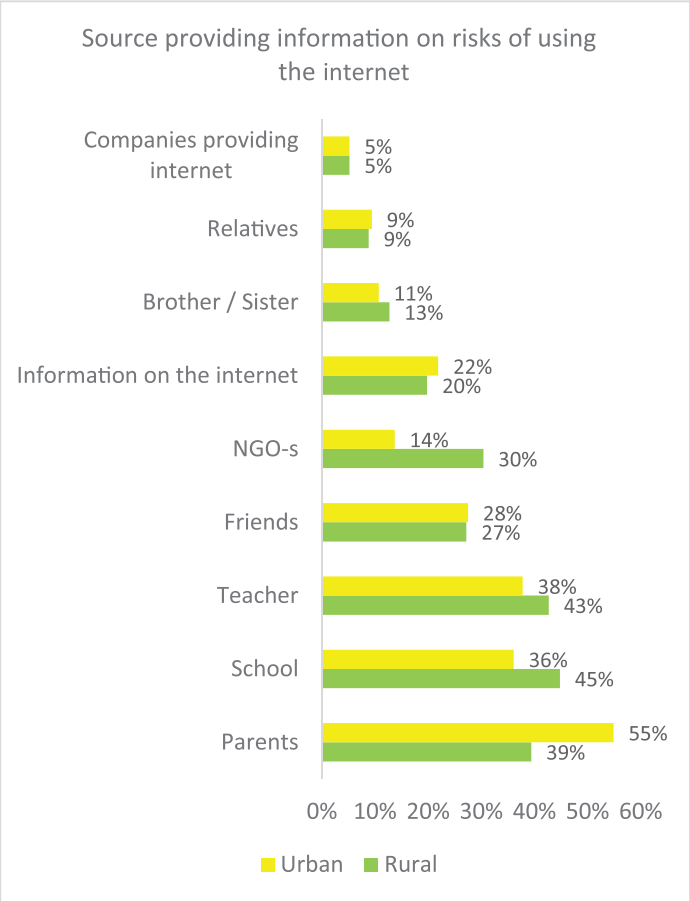
There is little difference among rural and urban children when recalling the concept of risks when using the Internet. Eighty-nine percent of rural children and 93% of urban children confirmed to have heard about Internet risks.

Have you ever discussed the rights to online safety with a teacher?



Often, teachers are seen as the least likely person to be considered for reporting online harm. Conversely, teachers are an important actor in discussing online safety with children. The survey results point out that 66% of rural children and 57% of urban children confirm to have been discussing their rights to online safety with teachers.

Sources providing information on risks of using the Internet



The key role in informing children about risks of using the Internet is played by their parents. Forty-four percent of the children surveyed confirm having received information about online safety from their parents, followed by school (42%), and teachers (41%). This data confirms that, in order to cope with the future challenges of children's online safety, special attention should be paid to appropriate training and education of parents, school staff, and teachers. In addition, mechanisms used for reporting of online abuse need to be reinvented providing children with reporting tools that are more efficient and child-friendly.

Key findings

•The top three devices utilized by Albanian children, ages 13-17, to consume media or play online are mobile phones (65%), PCs (59%) and laptops (43%).

•There is a discrepancy in social network membership between male and female Albanian children, especially when compared to similar groups in Europe. Among the children of Europe, social network account ownership for females exceeds male counterparts by 2%. Conversely, in Albania, social network account ownership for males exceeds female counterparts by 34%.

•85% of Albanian children that access the Internet have a computer at home.

•Contrary to other European countries, Albanian families prefer to keep computers in children's bedrooms. Data shows that 62% of children with access to the Internet have a computer in their bedroom.

•When asked about their perceptions of online risks, Albanian children shared similar opinions with children of other European countries. The top perceived risks were content-related, followed by conduct-related and contact-related risks.

•Bullying, password thefts and the unintentional viewing of pornographic materials when accessing the Internet are serious issues thatchildren face presently with 45% of respondents pointing out that children have to cope with these matters every day.

•According to 44% of respondents, children watch pornographic materials every day.

•47% of the children interviewed admit that, within the last year, they have been contacted online by an unknown individual.

•62% of the children interviewed confirmed having friends that visit pornographic sites.

•Out of the 47% of children that have been contacted online by an individual in the last year, 40% have been contacted by foreign nationals.

•Most of the unknown foreign citizens contacting Albanian children online are from the UK (33%), Italy (14%) and the US (8%).

•68% of children from both rural and urban areas confirm the existence of locations, computers or screens that display pornographic materials against their wishes.

•Most of the unintended pornographic material displayed takes place in Internet centers (Internet cafés).

•Parents are seen as the first person to report an online issue to by 48% of the children interviewed, followed by a friend (37%) and a brother or sister (36%).

•32% of the children interviewed confirmed teachers to be the least likely person they would turn to for help if they were harmed online. This was followed by the police with 27% of children not considering them an institution where they can seek assistance.

•44% of the children surveyed confirm to have received information about online safety from their parents.

Recommendations

1. Education institutions, civic society organizations and businesses should promote awareness raising and other safety practices for younger children as well as teenagers.

2. Legislation must guarantee that Internet centers or Internet cafes are equipped with a minor's only area that blocks visual access to adult content.

3. The government must trigger safer Internet browsing for children by assigning each minor a unique username and password. These assigned login details would be obligatory for accessing the Internet in public places. This method would restrict the access of minors to safe content only.

4. The government should set up a single agency in charge of collecting and managing reports of online abuse submitted by children. It should also be in charge of designing and pushing forward online safety strategies for children and supporting teenagers who face risks.

5. The government agency in charge should set up a reporting mechanism that is efficient, easy to access and child friendly by means of an online platform, SMS, Watsapp and Viber. In addition, the agency could develop peer mentoring schemes as a reporting/support mechanism.

6. In cooperation with private business such as ISPs, the government should trigger the creation and usage of a children security pack installed on home PCs/Laptops that is frequently updated with websites friendly to minors. Also, new safety tools are needed for new technologies such as mobiles, tablets, etc.

7. Mobile operators should provide parents with the option of requesting restricted online access for their children that allows safe content only.

8. Parents should be advised to talk to their child about the Internet or share an online activity with them.

9. In order to cope with the future challenges of children's online safety, special attention should be paid to appropriate training and knowledge educationof parents. Teachers also need to be trained and receive proper qualifications. Training should be extended to kindergarten levels too.

10. Curriculums in schools related to IT should be updated regularly and expanded to include Internet safety.

11. Anti-bullying initiatives should accompany efforts to promote Internet use.

12. The brand of Internet safety in Albania needs to be reinvented in a way that is less bland and more attractive to children.

Part II

Legislation and Policy Background Information

The global spread of Internet and its increasinglyuser-friendly approach allows huge opportunity for children to improve their education and develop their culture. The most prominent and effective tools are E-learning, online education programs, electronic libraries and social media. While the policy of the Albanian government (2005-2013) to extend access of Internet in each school has its positive side, little research has carried out to determine whether this policy has been effective as a legislative toolfor providing necessary safeguards on child Internetprotection. The Ministry of Education and Sciences (MES) launched a project called "Information and Communication Technologies in pre-University Education" in 2008. One of the main challenges of MES was the application of an effective computer science teacher training project in primary schools. By 2010 around1383 teachers were trained and 1334 tested.[3]

Today there are over200pre-universityinstitutions in Albania which have access to Internet all over the country (See table I).[4] The statics show a significant increase of the number of PCs per student in the last ten years.[5] This extensive presence of information technology (IT) increases the exposure of children to crimes such as cyber bullying.The current plan is to at leastdoublethe capacity ofInternetconnectionstoeducationalinstitutions. The use of Internet by households has also increased. By the end of 2012 the number of subscribers reached 215,000 with an increase of 24% from 2011.[6] Many children use smart phones and all Albanian mobile companies offer Internet. The number of people who use this service (GPRS/EDGE) was around 1.4 Million in 2011, 15% more than in 2010.[7]

The question this research aims to answer is, "how protected are Albanian children from the use of Internet?"This section will focus on the legal framework. This research is divided in to two main parts. In the first, we look at EU policies regarding child Internetprotection and analyze definitions and policies. This approach will help us to have a better understanding of the Albanian legislation on child Internetprotection. As part of its requirement to EU accession, Albania should approximate its legislation to EU law. Albania is also a member of the Council of Europe and has signed key conventions related to child Internetprotection. This aspect will also be considered in this section. In the second part of the research, we will focus on Albanian legislation from a broad prospective. We will look at policies and related legislation. Additionally, we will focus on cyber crime legislation and its enforcement.

Table I: Statistics of Internetusers in pre-university system 2010-2012[8]

Number of Internet users	2010	2011	2012
Primary School	196,000	188,000	183,000
High School	119,000	122,000	124,000

3 Interview with Hydajet Kopani, Directory of E-Education and Statistics, MES, August 20,2013.
4 Interview with Sokol Ymeri, Chief Sector of E-Education and Statistics, MES, September 10,2013.
5 Interview with Hydajet Kopani, Directory of E-Education and Statistics, MES, August 20,2013.
6 See the "Report on the Activity of the Authority of Electronic and Postal Communication for 2012", p.4, available at: http://www.akep.al/images/stories/AKEP/publikime/2013/RAPORTI-VJETOR-2012.pdf
7 Ibid.
8 Interview with Sokol Ymeri, Chief Sector of E-Education and Statistics, MES, September 10th ,2013.

3. EU Approach

In this section, we start by looking at the definitions which EU legislators have conceptualized in order to build an efficient legal environment in the EU zone for protecting children from the use of Internet. We then assess some of key relevant conventions and recommendations.

Definitions

We begin our research with a review of EU legislation and policies in order to have a better grasp of concepts that are often confused (i.e. illegal and harmful content). We also consider the problem with legislation enacted to confront the challenges of childInternetprotection. The widespread use of Internet among children in the EU is already evidenced. According to the research of Livingstone, Haddon, Görzig, and Ólafsson (2011: p.5) at least 93% of 9-16 year old users go online weekly and 59% have a social networking profile. It is important for our research to mention that child Internetsafety should not be limited only to illegal content, which often refers to pornography and cyber bullying. Children should also have safety from the content which is harmful to minors. There are two papers which served as the springboard of EU legislation on Internet child protection. Both papers were issued as a result of the concerns raised by an informal meeting of EU Council held in Bologna on 24 April 1996.[9]These studies where complimentary to each other and their scope was to stimulate short and long term policies within EU member states in respect of child Internet safety and protection of human dignity.[10] The first paper was on illegal and harmful content on the Internet (here and after the Content Paper) and the second on the protection of minors and human dignity (here and after the Green Paper).

The distinction between illegal content and harmful content was made initially by the Green Paper of 1996[11]. The Green Paper served as a spring board for the EU legislation as it was followed by the addition of the Council Recommendation 98/560/EC on the protection of minors and human dignity in audiovisual and information services (1998) to the EU "Guidelines for the Promotion and Protection of the Rights of the Child" (Council Conclusions 16457/07, 12 December 2007). While traditional modes of visual communication such as TVs and cinemas are more public in nature, current electronic devices (PC, laptops, mobile phones, iPod, etc.) have individualized communication and eased exposure to both illegal and harmful content. They have made it difficult to control and supervise children.[12]

The definition of illegal content is made clearer inthe Green Paper while the harmful content is summarized at the Content Paper. The Green Paper includes in the definition of illegal content *child pornography* (in the form of photos, photo-simulations and animated material); *violent pornography* (including material involving non-consenting adults), zoophilia pornography (cross-species material) as being widely prohibited; *incitement to racial hatred or violence (or both.)*.[13]We note that while both papers recognize the importance of the harmful content they do not provide a clear definition. However, the Green Paper hints ata fuller definition of harmful content when it highlights "the protection of minors against material which might harm their physical or mental development is an almost universal objective".[14]

9 See EU Commission Communication on " Illegal and Harmful Content on Internet", Brussels, 16,10,1996, (COM 96), 487, p. 4, available http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:1996:0487:FIN:EN:PDF

10 EU Commission Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, Brussels, 16,10,1996,(COM96) 483,p. 1,available at:http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=1996&nu_doc=483[accessed August 26, 2013].

11 Ibid

12 Ibid at p. 11 it notes that "It is unlikely that the new services carry more contentious material than the traditional media have to date. But the new services make this material more visible and relatively more accessible."

13 Ibid p. 13

14 Ibid p. 38

The argument brought fourth of not providing a definition of "harmful content" is that there is a diversity of cultural approachesand different countries have different views on the protection of minors and human dignity. For instance, in stark contrast with Latin states (e.g. Portugal or Spain), the Nordic (e.g. Norway or Denmark) countries are tougher on violent content and lenient in sexually explicit material.[15] In addition, even in terms of prohibition (general or special) and rules applying to media, EU member states differ. France applies a broad definition of illegal material (obscenity, indecency, etc.), whereasthe UK provides more specific examples of illegal material (i.e. child pornography, protection of children against abuse etc.).

The EU legislation provides a definition for "illegal content" but it leaves it to the member states to define "harmful content" contextualized in their culture. Albania therefore may take this approach and set its own criteria of what can constitute "harmful content".

Policies

It seems that the EU approach makes no difference in defining the offence in the context of technology. The Content Paperemphasizes that "what is illegal offline remains illegal online".[16] It also highlights the variety of actors and forms of access to the Internet, which makes online platforms vulnerable to the spread of illegal and harmful content. Therefore, an individual can access the Internet through Internet access providers (specialized in offering access to Internet), Internet service providers (ISPs) (who provide hosting content through their own company or third parties) and, online service providers (i.e. providers of propriety content and Internet for their subscribers on their closed system).[17] The ISPs offer access to Internet, which it leases from a telecommunication line, the "network operator" which in Albania is the Albanian Telecom.[18] In addition, "content publishers" are those who publish their content in "host" servers online, and are additional services provided by ISPs for a fee. Their content is accessible to everyone in the public, including minors via hyperlink.[19] Other forms such as emails, online chats, and social media allow individuals to share and disseminate illegal and harmful content. We see that since 1996 all actors involved in providing illegal content were subject to the law, including authors, content providers, host service providers who store and make them available, network providers and end users.[20] The Content Paper highlights several difficulties, which are worth summarizing as it may help this research to assess them in the Albanian context.

It is very difficult for law enforcement agencies to implement effective controls for discovering illegal content in time as this would need to bedone at "the entry and exit points to the Network (the server through which the user gains access or on the terminal used to read or download the information and the server on which the document is published)."[21] It is also hard to hold responsible ISP (access and host providers) for not directly controlling the content provider. However, the communication papers offers guidelines on possibilities for making the ISPs subject tocriminal law (child pornography), civil law (damages for the breach of copyright, libel) and administrative law (regulation by authority which supervise ISPs for technologies they offer to facilitate the access to illegal content by the users.[22] Some member states (i.e. Austria, Germany, France and UK) require that ISPs react immediately if it "becomes aware of the *prima facie* illegality of content hosted on its server and remove the content in question".[23]

15 Ibid p.3
16 The Communication, p.4
17 Ibid p.8
18 Ibid
19 Ibid p.9
20 Ibid p.10
21 Ibid p.12
22 Ibid
23 Ibid p.13

Network operators may also be asked to "to take steps in relation to their customers (access providers) if the latter use facilities to carry illegal content."[24] In addition, if the host server is in another country which applies different legislation from that of the EU, and illegal content cannot be removed, authorities may ask the ISP to block subscribers on that illegal content on a case by case basis.[25]AnonymousInternet users are also a concern. In the UK, the Safety Net "takes the view that use of truly anonymous accounts is a danger, while use of pseudonyms which are traceable is not". [26] As we will see in the Green Paper below, the protection of minors from harmful content should take into account the respect for freedom of expression. The Content Paper sets out two conclusions that "any regulatory action intended to protect minors should not take the form of an unconditional prohibition of using the Internet to distribute certain content that is available freely in other media…. [and] that existing rules on content regulation need to be examined to see whether they can be applied by analogy, and that the most restrictive rules should not be applied simply because of Internet's wide potential reach".[27]

Freedom of Expression v. Human Dignity

The Green Paper underlines several issues that need to be addressed. First, "illegal content" for adults should not be confused with "harmful content" for children such as access to pornographic materials, which are not illegal for adults. Second, the evolution of mass communication and the widespread use of the Internet has developed hybrid forms of content (i.e. legal +plus illegal content). For instance, games are come with advertisements, news, offers, etc. This hybrid form makes it technically very difficult to isolate, block and single out the illegal component of the mixed content.[28] In terms of enforcing of the law, the Green Paper recognizes the tension between freedoms of expression, which includes freedom to provide service, the right to privacy on the one handandon the other, the protection of minors and human dignity. Both freedoms (i.e. freedom of expression and right to privacy) are stipulated in the European Convention of Human Rights (ECHR), articles 10 and 8. These articles are incorporated in the EU Treaty and recognized by the Court of Justice. [29]Albania is bound by ECHR as it has integrated in its Constitution, article 17.

The case law of European Court of Human Rights has developed the test of proportionality, which has been followed by the EU. Thus, each Member State can restrict freedom of expression but the "measure must meet a real social need and be effective without being disproportionate in the restrictions it imposes".[30]However, concerns about the variety of moral standards, which had implication on the enforcement of law and policy-making, remain.[31] Albania, as almost all EU member states, considers both freedom of expression and protection of privacy constitutional rights.[32] The Green Paper highlights the difficulty of applying the restriction on decentralized services, which includes many actors from initial loaders to access by the end users.[33] In addition, the global aspect of the network has encouraged "shopping of Internet heavens" and limited the scope of national legislation. The service can be moved to another state with a more relaxed legislation.

24Ibid
25 Ibid p.15
26 Ibid p. 17
27 Ibid p. 18-19.
28 EU CommissionGreen Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, Brussels, 16,10,1996,(COM96) 483,p. 9,available at:http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=1996&nu_doc=483[accessed August 26, 2013].
29 See Case C-260/89 EllinikiRadiophonia Tileorassi [1991].
30 See Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, p.12, available at: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=1996&nu_doc=483 [accessed August 26, 2013].
31 Ibid p. 4
32 Albanian Constitution articles 22, 36 and 37.
33 Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, p.14, availableat:http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=1996&nu_doc=483 [accessed August 26, 2013].

There are two approaches shared in the EU area; several member statesuse a general application where they ban all forms of media that broadcast uncontrolled material that is illegal and harmful for the minors but lawful for adults. But there are other member states, which apply restrictions for specified media (i.e. TV).[34] As we will see in part II, Albania follows the general approach.

The restriction becomes very difficult with online services. Material is not scheduled in times so to allow parents to have control over their children. It can be watched round the clock. The access is very individual and unlimited. It can also be accidental. As mentioned above the material can be harmful for minors even though it is not illegal for adults. The Green Paper notes that the difficulty lies inprotecting minors while not limiting the freedom of expression of the adults. The main challenge rests with online services where both adult and a minor may access the material at the same time. This may have legal implications in terms of enforcement. In this context, the most viable solution proposed by the Commission is that "all services may be adapted to incorporate control devices, notably parental control".[35] It shifts the obligation to ISPs and end users.

The next issue is the labeling of "harmful material" and defining the age for adults. Different member states have different definitions for both.[36] For online services, the Commission proposes the filtering of information based on three types of filtering software (black listed, white listed and filter based on neutral labeling).[37] The Commission encourages the service providers and third-party content providers to filter and label the material, as this can be more effective.[38]The Commission suggests several policies[39], which may be adopted by Albanian authorities.

Due to the diversity of views and legislations in respect to childInternetprotection, the Commission proposed a "bottom-up" approach, which will avoid extensive censorship by the state and would increase effectiveness by encouraging self-regulation.[40] As this research will show later in part II, this is the approach followed by Albanian institutions.

From the judicial approach, the balance between freedom of expression and the protection of pubic moral remains a challenge for law enforcement agencies and courts. A strike balance should be maintained. And each Member State is free to define "public moral" according to its values and culture. In this context, there should be a consensus either by law or by a Constitutional Court decision on how "public moral" should be defined in Albania.

EU Legislation

There was an immediate reaction by the EU to the Commission's suggestions, which triggered a series of recommendations and conventions related the protections of minors and public moral.[41] Following the concerns and suggestions of the above mentioned papers (i.e. Content and Green Papers), the EU Council issued Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry. The recommendation promotes national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity. It was the first legal instrument, which asked members states to foster national frameworks for the protection of minors and human dignity.

34 Ibid p.15
35 Ibid p.18
36 Ibid
37 "Black list filtering aims to block access to sites identified as problematic in view of the material they distribute (nudity, violence, sex, etc.); black lists are difficult to update. White list filtering authorizes access only to pre-determined sites; access to material is heavily limited. Filtering based on neutral labelling gives users access to information on material loaded by suppliers or third parties on the basis of their own selection criteria."(Green Paper p. 19). See also the Content Paper. 20-21.
38 Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, p.20, availableat:http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=en&type_doc=COMfinal&an_doc=1996&nu_doc=483 [accessed August 26, 2013].
39 Ibid p. 24
40 Ibid p.4
41 See the list of EU legislation on the online child protection at Annex I.

Council Recommendations suggested member states to encourage the establishment of national frameworks for self-regulation by operators of on-line services. Industries and the parties concerned draw up codes of conduct for the protection of minors and human dignity, in order to create an environment favorable to the development of new services.

In order to assess the effects of these recommendations, the Commission prepared two assessment reports to the Council and EU parliament, the first in 2001 and the second in 2003. We see that the EU follows a bottom up approach encouraging self-regulation on the part of member states in terms of harmful content, which is difficult to define.[42] Also, it encourages member states to enact laws on prevention of illegal content. It is useful for this research to investigate how different EU states managed to deal with the fight against illegal content. Many members have specific legal requirements for operators hosting illegal content. Sweden, according to its Penal Code holds responsible for the content of their material anyone who operates on theInternetand obliges them to remove it. Lithuania and Poland require that judicial authorities and police be informed for the illegal content (without specifying individual, state or private agency).

In Luxembourg and Iceland, it is by practice and not by law that operators should remove illegal content if they discover it. Greece and France oblige ISPs to keep data (without specifying further) to assist law enforcement agencies. Other member states such as Hungary, Poland, Portugal, Iceland and Norway left it to the e-commerce Directive (Directive 2000/31) to set down rules to deal with this matter. [43] Albania has not yet transposed this Directive to its legislation and e-commerce law is still pending.[44]

In Germany ISPs are required to take all necessary measure to prevent minors from accessing harmful material. The authority is in charge of testing the technical capacity of the ISPs (i.e. possession and use of the right software) to make that possible. UK and Netherlandsdefer to a single association (Internet Content Rating Association) and Poland defers to three, which rate websites according to their content. Parents can then refer to this rating, which is based on content, and restrict access of their children therein. Norway sees education and the raising of awareness among children and parents as more effective tools.[45]

Another useful policy applicable in the EU is the use of hotlines. Everyone can complain about illegal content to the hotline which then asses the information and sends it to the agency in charge (i.e. police, regulatory agency, ISPs etc). Today there is a network of hotlines associated with the European Networks of Hotlines INHOPE.[46]

42 We draw this conclusion by looking at the rules that the Commission requiresin the code of conduct utilized by ISPs. The rules should cover issues (I) on the nature of the information to be made available to users, its timing and the form in which it is communicated, (ii) for the businesses providing the on-line services concerned and for users and suppliers of content, (iii) on the conditions under which, wherever possible, additional tools or services are supplied to users to facilitate parental control, (iv) on the handling of complaints, encouraging operators to provide the management tools and structures needed so that complaints can be sent and received without difficulty and introducing procedures for dealing with complaints and (v) on cooperation procedures between operators and the competent public authorities. See Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity p. 6.

43 Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, p.7.

44 See European Commission, Enlargement Strategies and Main Challenges 2012-2013 "Albania 2012 Progress Report", p. 39.

45 Second Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity, p.9.

46 Ibid p.8

Industries have also been active. In Germany, they have established a filtering system called "walled gardens" that "consist of special portals where the operators guarantee the quality of sites, which may be accessed through them"[47]. In other member states ISPs are obliged to inform subscribers for the filtering system and software.[48]Control of chatgroups is also a concern. Some states leave it to the chatgroup operators to control them not to the government. Other states consider it a constitutional right that should not be infringed upon. Greece has a special police unit which surfs and investigates cyber crime issues.[49] Another measure, which seems to be lacking in Albania, is the supervision of computer and video games. In 2002, the Council of Europe adopted Resolution (2002/C 65/02) on the protection of consumers, in particular young people, through the labeling of certain video games and computer games according to age group.[50] Some member states have specific legislation covering both online games and video games in protecting the minors.[51]

Following a 1998 recommendation, the Commission adopted more advance legislation, the Recommendation 2006/952/EC[52] on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry in 2006. The Commission here includes the role of minors and asks for opinion, which raises the awareness of the community of children in order to encourage more responsible use of audiovisual and on-line information services on their part. In the2006recommendations, we see that the Commission focuses on the fight against discrimination[53] (including discrimination based on age) and the fight against illegal activity on the Internet, which is harmful for minors. [54]

Another important EU legislation is the Audiovisual Media Services Directive (AVMSD) adopted in December 2007. The AVMSD specifies rules regarding the protection of minors in all audiovisual media services including the Internet {Article 1 (10(a)}.[55] However, while the Directive stipulates rules on protection of minors from on-demand service from adult content (article 12) and advertisement of harmful content for minors (i.e. "unhealthy" food and drinks in children's programmes, article 9(2)), there are no restrictions for "programmes which might simply be 'harmful'".[56]

47 Ibid p.10
48 Ibid
49 Ibid. p. 11
50 The initiative of Pan European Games Information (PEGI), which was launched in 2003, is interesting and can also be applied in Albania. PEGI is intended to protect minors from games that are not fit for their age. The PEGI age band is age bands are 3+, 7+, 12+, 16+ and 18+. This age range serves as icon, which is labelled on the back of the game box. The issue is not clear though about online video games and how this is regulated. As mentioned above there are member state such as Germany, Sweden and Norway, which have specific laws covering this issue. For more see Ibid, p. 15.
51 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a better Internet for Children,2.05.2012, p.3, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PD-Faccessed on September 3, 2013].
52 See the Summery of the Act at the Commission, Audiovisual and Media Policies, available at http://europa.eu/legislation_summaries/audiovisual_and_media/l24030a_en.htm, [accessed on September 3, 2013].
53 Member states were suggested to " to promote a responsible attitude on the part of professionals, intermediaries and users by:
-encouraging the audiovisual and on-line information services industry to avoid all discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation, and to combat any such discrimination;
-encouraging vigilance and the reporting of pages considered illegal;
-drawing up a code of conduct in cooperation with professionals and regulatory authorities at national and Community level." (ibid.)
54 Commission proposed the each member state takes "the following measures:
-awarding a quality label to service providers so that users can easily check whether or not a given provider subscribes to a code of conduct;
-establishing appropriate means for the reporting of illegal and/or suspicious activities on the Internet." (ibid.)
55 The Directive covers" all services with audiovisual content irrespective of the technology used to deliver the content: The rules apply whether you watch news or other audiovisual content on TV, on the Internet or on your mobile phone. However taking into account the degree of choice and user control over services, the AVMSD makes a distinction between linear (television broadcasts) and non-linear (on-demand) service." For more see a detailed explanation of the Directive at European Commission, Audiovisual and Media Policies available at http://ec.europa.eu/avpolicy/reg/tvwf/provisions/index_en.htm [accessed September 3, 2013].
56 See the Summery of the Act at the Commission, Audiovisual and Media Policies, available at http://ec.europa.eu/avpolicy/reg/tvwf/protection/index_en.htm, [accessed on September 3, 2013].

In line with AVMSD, the Commission adopted another Directive (2010/13/EU) on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services (Audiovisual Media Services Directive- AMS) in 2010. In terms of protecting children, the AMS improved the standard of protecting minors from programs that were harmful. It stipulated rules to "protect minors against the negative effects of pornographic or violent programmes, such programmes, when broadcast, must be preceded by an acoustic warning or identified by the presence of a visual symbol throughout the broadcast." In addition, commercial communication or advertisement should not contain, among other things, ads which can be interpreted as harmful content for children such as "messages relating to alcoholic beverages specifically aimed at minors" and content which "cause moral or physical detriment to minors". 57

Other relevant EU legislation is the Council Framework decision 2004/68/JHA on child pornography (2004). This Framework provided a broad definition of child pornography.[58]member states are required to include in this definition production, distribution, dissemination, transmission, making available as well acquisition and possession of child abuse material (article 3 (1a)). The sanction extends also to instigation, aiding, abetting and attempt, and requires Member States to make these offences punishable (Article 4). However, this Act did not cover "new forms of abuse and exploitation using information technology" and "outside national territory, does not meet all the specific needs of child victims, and does not contain adequate measures to prevent offences"[59]

On 25 March 2009 the Commission published the text of a proposal for a revised Council Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework2004/68/JHA. This act would broaden the definition of child pornography and approximate it with the Council of Europe Convention CETS No. 201 against child sexual exploitation and sexual abuse ("the COE Convention") and UN Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography 2000.

It broadened the range of offences such as "… knowingly obtaining access to child pornography, to cover cases where viewing child pornography from websites without downloading or storing the images does not amount to 'possession of' or 'procuring' child pornography." It also included a new offence "of 'grooming'[which] is incorporated closely following the wording agreed in the COE Convention."[60]An advantage of this Act was the approximation of substantive criminal law and procedure law to avoid "forum shopping" by offenders in moving in states with lax laws.[61]

Although there is a series of documents and studies on the national and EU level there are still concerns about the need to improve further policies about the protection of minors.[62] The most up to date 2012 Communication Act of the Commission highlights the important factthat market oriented policies such as self-regulation and use of code of conduct by the ISPs have not been enough to eradicate the risk.

57 For more see the summery of the Act available at http://europa.eu/legislation_summaries/audiovisual_and_media/am0005_en.htm [accessed on September 3, 2013].
58 Child pornography mean "pornographic material that visually depicts or represents:(I) a real child involved or engaged in sexually explicit conduct, including lascivious exhibition of the genitals or the pubic area of a child; or (ii) a real person appearing to be a child involved or engaged in the conduct mentioned in (i); or (iii) realistic images of a non-existent child involved or engaged in the conduct mentioned in (i)." See article 1 of the Council Framework decision 2004/68/JHA.
59 See Revised Council Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, March 25, 2009, p.3. available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0135:FIN:EN:PDF,
60 See Revised Council Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, March 25, 2009, p.6.
61 Ibid. p. 7
62 In 2011, the EU Council invites member states to "encourage providers of online media content, Internet service providers, social networking sites and online discussion fora to take full account of the protection of minors in the design of their services and to develop and adhere to relevant codes of conduct". See Council Conclusions on the Protection of Children in the Digital World of 28 November 2011, p.3, available at http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/educ/126399.pdf [accessed September 4, 2013].

[63] So, requirements put forth to ISPs to add parental control software, rank the content or offer free of charge counseling are seen as additional costs to the technology business. Therefore, "companies are all the more reluctant to develop and implement such tools if they are not confident that there will be a market of sufficient size to justify the investment".[64] In the Albanian context, borrowing from the EU experience, the bottom-up approach where companies are the main actors in protecting minors from Internet risksis unlikely to solve the problem. Some other problems raised by the 2012 Communication Act documents are that most of protective tools are those in English language. Though, there is an increasing number of apps used in Albanian language.

Furthermore "there are not many tools suitable for game consoles, tablets and mobile phones – the devices increasingly used by children to go online - and there are no solutions for users who access content on mobile phones or tablets using an application and not a browser."[65] The increasing modes of risk posed and lack of risk management is also evidenced in the EU. The most problematic risks are pornography, bullying and receiving sexual messages, contact with people not known face to- face, offline meetings with online contacts, potentially harmful user-generated content and personal data misuse.[66] Around23% of 9-16 year-old children have seen sexual or pornographic content, 6% have been victims of online bullying, 30% of children aged 9-16 have communicated in the past with someone they have not met face-to-face before. About 15% of 11-16 year-olds have received peer to peer sexual messages or images. Among the 11-16 year-olds surveyed there were some other kind of what the report called "potentially harmful user generated content" such as hate (12%), pro-anorexia (10%), self-harm (7%), drug-taking (7%) or suicide (5%). Nine percent of 11-16 year-olds have had their personal data misused – abuse of the child's password (7%) or their personal information(4%), or they have been cheated of their money online (1%).[67]

The Internet is creating a dangerous environment, which has facilitated the recruitment of trafficked children and distribution of child sexual abuse images.[68]In addition, studies have shown that often harm is referred or limited to the exposure or engagement with e-illegal activities such as "pornography or racism or the circulation of sexual messages" but little consideration has been paid by legislators to the side effects of excessive use of Internet or "the nature of the harm that may result and which, presumably, motivates the anxiety". [69].

63 Even after seventeen years where the first studies emerged (i.e. Green and Communication papers of 1996), it seems that limited progress has being made by member states in limiting the risk. Almost all memberstates rely on self-regulation of the ISP and code of conducts. Referring to 2012 Commission Communication Act "in the UK ISPs have adopted a code of practice that promotes an'active choice' whose implementation is left for each ISP to decide; in France, ISPs have to provide parental control software free of charge; in Germany a certified «youth protection software» can be used to prevent children from accessing websites providing harmful content. In other countries no such provisions exist. Germany also implements a self-regulatory framework that allows providers to rate different types of online content such as videos, websites or online games. In the UK, one of the recommendations of the Bailey report13 was to age-rate music videos. In other countries there are no provisions for classification of online content. In Finland and Belgium industry codes of conduct have also been brokered, for social media in the first case and addressing a wider range of providers in the second. In countries such as the UK, Spain, Italy or the Czech Republic different reporting mechanisms for harmful and illegal content and behavior are implemented with the support of different stakeholders such as the police, NGOs or industry." For more see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a better Internet for Children,2.05.2012, p.4, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDFaccessed on September 5, 2013].

64 Ibid p. 4

65 Ibid

66 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011).Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online, p.5.

67 Ibid. p.7

68 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions , European Strategy for a better Internet for Children,2.05.2012, p.5, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PDFaccessed on September 7, 2013].

69 Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011).Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.

In general EU policies and legislation have tried to protect children by focusing on regulating types of media and technology generally. It has encouraged self-regulation and code of conduct as they allow more flexibility among member states to adopt policies to their cultural context. This policy also gives more space to companies to respond to rapid technological changes. However, the diversity of strategies among member states may hamper the cooperation among law enforcement agencies. The 2012 Commission Communication Act noted this concern highlighting that the EU legislation so far "ha[s] not been combined in a coherent framework". In this context, the EU itself does not have a cohesive blue print strategy or legislation to draw on. Each EU Member State is free to devise and design its own policy within the framework of EU legislation under the "self-regulation" strategy and reliance on the "ISPs' code of conducts".

4. Albanian Policies and Legislation

After reviewing key EU and Council of Europe legislation about Internet child protection we move in Part II and focus on Albanian policies and legislation.

Albanian Policy Making

The Albanian government has taken considerable steps forward on child Internetprotection policies in the last five years. The key document is the Inter-sectoral Strategy of the Information Society(2008-2013), which was based on several regional and international policies.[71] In general the Strategy focuses on the information society and lays down the foundations to build a policy that involves all key institution in facilitating the development of a safe Internetuse in education, government and business. The approach taken follows similar key EU strategies in encouraging self-regulation and the implementation of the code of conduct by the ISPs (including tools and mechanisms such as parent control).[72] The information technology reform intensified in respect of child protection in 2010-2012.

In December 2010, the Ministry of Innovation and Information Communication Technology (MIICT), National Agency for Information Society (NAIS) and National Authority for Electronic Certification (NAEC), organized a conference for "a safer Internet". Its purpose was to raise awareness about online safety and in particular self-regulation practices. Among the most important ones were the approval of Law no. 10 347, date 4.11.2010 "For protection of children rights", the creation of the National Agency for the Children Protection Rights (NACPR) and an action plan specified for child protection.[73] The MIICT and NAEC were in charge to supervise and implement the action plan.

The 7th of February is "Internet safety day". This event takes place every year during the month of February (the first Tuesday of February). In 2012, MIICT launched "Internet safety week", and organized a round table called "all together for a safer Internet." Also, for the first time Albania became part of the international community celebrating this day by having his own space and webpage: www.saferInternet.org .

[74] Representatives from the business community, schoolsand international institutions were invited and the adoption of the code of conduct by ISPs and the possibility for ISP to offer parental control tools were discussed. It should be mentioned that the initiative concerning the preparation of codes of conduct and

70 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European Strategy for a better Internet for Children, 2.05.2012, p.6, available at http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0196:FIN:EN:PD-Faccessed on September 9, 2013].
71 For more see a brief of the Strategy at the official website of the National Agency of the Information Society, available at: http://akshi.gov.al/
72 See Intersectoral Strategy of the Information Society, 2008-2013, p.8, available at: http://akshi.gov.al/
73 Decision of the Council of Ministers (DCM) no. 182, March 2012.
74 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.

self-regulatory adaptation practices was welcomed by ISPs.[75] This activity also found wide coverage in the press. It is interesting to note that during the discussion that took place during these activities, ISPs highlight that parents are not interested in the guidance and measures offered by these ISPs on child protection.[76]

After the round table held on 7 February 2012, wireless companies and the main ISPs were seriously committed to the preparation of the code of conduct and also to providing guidance and tools on how to protect children from the risks of the Internet.[77] During 2012, in cooperation with the mobile companies, it was proposed that a code of conduct for the use of electronic communications safe from children and youthbe prepared by MIICT.

This code, which was mostly suggested by Vodafone, has been prepared in support of numerous national and international legislations. [78] The code was later distributed to the major companies which considered it as an effective tool.[79] As one representative of the ALBtelecom & Eagle Mobile noted "this Code aims to develop practical, self-regulated and entrepreneurialbehavior and practices in the electronic communications industry in relation to child protection, to provide a safe use of networks, services and devices to match with the existing legal and regulator."[80]

In February 7, 2013, a ceremony for the signing of the code of conduct was held under the auspices of MIICT and NAEC. Currently the code of conduct is signed by the biggest Internet access providers, which cover nearly 90%$ of the market such as ALBtelecom & Eagle Mobile, AMC, Vodafone, Plus, Abcom, Abissnest, Tring Communication as well as ICT associations AITA Albania.[81] As late as 2013, after signing the code of conduct, the companies begin to organize some activities. For instance, ABCOM during it marketing campaign promoted the offering of the parental control tool. Vodafone has a column on its website called "isigurt"where it provides extensive information regarding risk and measures of Internet usage. In form of pamphlets, the AMC provides information on how to safely use the Internet, specially on mobile phone. It also advisesparents on howto check on their children'sInternetaccess.[82] In addition ALBtelecom & Eagle Mobile is "in the process of providing a platform of 'Web filtering' which will allow parents to intervene and control/filter the content in the Internet for their children."[83]

Another key institution actively involved in policy issues of child Internetprotection is the Ministry of Education and Science (MES). In 2008 only 18 schools had access to the Internet. Since 2009, based on several documents and strategies[84], the MES undertook several projects to install Internet in every primary and high school. To improve the quality of training, MES has cooperated and singed memorandum of understanding with Microsoft and Partners in Learning (MS PiL). Within the MES there is a directory focused on E-learning which aims to supervise the implementation of ICT strategies in Albanian educational system. Teaching about child Internetprotection is included in the teaching of IT at the schools 'curricula on classes ofVII, VIII and IX'th grades. However, concern remains because the background of teachers who teach IT in most schools, especially in small cities and in rural areas, is not in IT but others sciences. Often the teacher of math takes over the teaching of the IT.[85]

75 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
76 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
77 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
78 The Code of Conduct was primarily based on the Law «On protection of children's rights», «Plan of Action for Children 2012 -2015 'adopted by the Council of Ministers Decision no. 182 dated 13.03.2012, "Social Safer Networking Principles for the EU" (2009)and European Framework for Safer Mobile Use by Younger Teenagers and Children" (207).
79 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
80 Interview with a representative of ALBtelecom & Eagle Mobile, September 21, 2013.
81 See the "Report on the Activity of the Authority of Electronic and Postal Communication for 2012", available at: http://www.akep.al/images/stories/AKEP/publikime/2013/RAPORTI-VJETOR-2012.pdfaccessed on September 12, 2013].
82 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
83 Interview with a representative of ALBtelecom & Eagle Mobile, September 21, 2013.
84 The Inter-sectorial Strategy of the Information Society, 2008-2013, National EducationStrategy2009 – 2013, National Education Strategy2004 -2015, Integrated Planof the Ministryin 2010, and Law no.9918, date 19/05/2008 "On the Electronic Communication".
85 Interview with a representative of the Cyber Agency for Cyber Security (ALCIRT), September 10,2013, Tirana

As one IT expert puts it, "There are no IT experts and trained teachers....most of them who teach IT are teachers of math. ...most of them do it for some extra money...this is a disaster...computers are installed without any monitoring system, the teacher simply behaves as guards just to make children aware that he is there.....inability of the teachers to monitor children with advanced IT knowledge makes the teacher and the school's system a vulnerable environment."[86]

Other institutions such as MIICT, NAEC and NACPR have somehow strived to provide polices on raising public awareness regarding the risk of Internet usage for children. However, concerns remain about effectiveness of both policy and law enforcement on keeping children safe from the harms of the Internet. As the Alternative Report on Albania for 2012 points out "The Government has focused efforts on combating trafficking, while other forms of commercial sexual exploitation of children remain largely unaddressed."[87] While the above institutions deal more with the policy making issues, the main agency which has a regulatory and enforcement power in terms of administrative law is Electronic and Postal Communication Authority (EPCA). Based on its 2012 report, EPCA has made progress in terms of improving its legislation by approximating with EU law. But it seems to not have been active in terms of Internet Child Protection policies and initiatives.

Generally governmental institutions have been active in developing strategies of integrating information technology in society generally and in the pre-university schools specifically. However, policies on child Internetprotection begin to intensify only in 2010 and onward. The involvement of industry came relatively late in 2012. A point to be noted is that while policy making institutions have been somewhat active, regulatory bodies such as EPCA seems more reluctant.

Legal Framework

In general Albania *de jure* has fulfilled its international obligation in approximating somewhat its legislation onchildInternetprotection with relevant treaties and conventions where it is a member. For example, Albanian has approximated its legislation with Law No. 8624 dated 15.06.2000 "On the Ratification of the Hague Convention on the Protection of Children and Cooperation on Adoptions abroad". Albania has also ratified the Optional UN Convention on the Rights of the Child on the sale of children, child prostitution and child pornography 2000 in February 5, 2008 without any reservation.[88] The UN Convention on the rights of the child was ratified by Albania in February 1992 and it came in force in March 1992.[89] The Convention on the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour (1999) was ratified in 2001, but it is still not in force. This Convention includes in its definition of the "worst forms of child labor" "the use, procuring or offering of a child for prostitution, for the production of pornography or for pornographic performances" (Article 3).

Albania was among the first members of Council of Europe to ratify the Convention on Cyber Crime 2001(here and after the Cyber Crime Convention).[90] Law no. 9262, dated 29.7.2004, has also ratified the additional protocol to the Convention on Cybercrime. Albania has integrated to its legislation the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature through computer systems. This came intoforce on 01.03.2006. It has also signed (in 2008) and ratified (in 2009) the Council of Europe's Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

86 Interview with an IT expert, September 25, 2013.
87 See the Alternative Report 2012 " Albania: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" prepared by Children's Human Right Centre (CRCA), Albanian Coalition against Child Trafficking and Sexual Exploitation of Children (ACTESEC) and ALO116-Albanian National Help Line, p. 9.
88 See United Nations Treaty Collections available at http://treaties.un.org/Pages/ViewDetails.aspx?mtdsg_no=IV-11-c&chapter=4&lang=en [accessed September 10, 2013].
89 Zaka, T., (2001) "UN Convention on the Rights of Child and Albanian Legislation", available at http://www.unicef.org/albania/conv-legis.pdf[accessed on September 20, 2013].
90 See Law no. 8888, date 25.4.2002 "On the Ratification of the Convention of Cyber Crime", available at:http://www.qbz.gov.al/doc.jsp?doc=docs/Ligj%20Nr%20 8888%20Dat%C3%AB%2025-04-2002.htm

Albania is bound by UN Convention of 1992, as Majlinda Bregu, then the Minister of Integration notes, to make sure that every policy and legislative step be taken on the best interest of the children (Article 3).[91] On the national level Albanian Constitution places a lot of emphasis on the protection of minors by requiring that "children [….] have the right to special protection by the state" (Article 54/1). In 2010, with a simple majority (opposition did not vote the law), Albania stipulated the Law on Child Protection Rights.[92] In 2013 amendments to the Penal Code an important sentence on the principles that drive this Code was added. Article 1/c now reads that the Penal Code in determining the guilt and the penalty is based among others "on the best interest of children".[93]

An important amendment was the improvement of article 117 of Penal Code (we will elaborate in depth in the section on criminal law). This article defines "illegal content" (i.e. child Internetpornography) but is silent on "harmful content" as the later is difficult to define. Regarding the interpretation of the "harmful content", Irena Malolli notes that the definition is:

"Verycontextualandrelated to socialandculturalaspects of a country(what one societydeemsharmfulthe other will not). Anacceptеddefinitionfor the harmful content can be "whatmakes me feelbad"...but even with this definition the meaning is also evasive so it is hard to determine a precise definition of harmful content in the law."[94]

While in child protection rights, Albanian law has largely drawn from international conventions, in terms of information technology, it has largely based on EU legislation. This is a requirement of the Stabilization and Association Agreement that Albania has signed (Articles 50, 57, 70, 71, 72).[95] In this context the following laws reflect the approximation with EU directives.

Law no. 97/2013 "On Audiovisual Media in the Republic of Albania"

This law is approximated with Directive 2010/13/EEC "On the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services". The law starts with a series of principles, including the protection of minors. It specifically considers minors' rights, interests, moral and legal protection (Article 4/b). The law regulates audiovisual programs over the Internet and it requires that programs of commercial and non-commercial nature should not include content which may risk the status of the children (Article 42/3, 5, 7 and 8).

This is the law which can be said to have defined somehow what does "harmful content" constitute. The legislator has defined as "harmful content" for minors the content which undermines their moral and physical status as well as their exposure of minors to dangerous and abusive situation. The law here is not clear on what is a "dangerous and abusive situation". This may include side effects of any visual film broadcasted via the Internetand may incur anxiety to children. On the other hand, the law is very specific on the harms deriving from food and it prohibits advertisement of food harmful for the health of children while it does not specifically provide a list of harmful content(Article 7/8). Law also requires the Audiovisual Media Service Provider (OSHMA) to not transmit pornographic programs without ensuring that it provides limited access and parental control for the subscribers (Article 33 / e).

It is the only law providing a definition of "harmful content" but the definition has not included promotion related to IT goods and services.

91 See the discussions of Majlinda Bregu, then Minister of Integration a the Minute of the the Member of Parliament regarding the 2013 amendments of cyber crime law at the Minute date April 03,2013, held by the Parliament Commissionon Legal Affairs, PublicAdministrationandHuman Rights, p. 05.
92 See the Alternative Report 2012 " Albania: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" prepared by Children's Human Right Centre (CRCA), Albanian Coalition against Child Trafficking and Sexual Exploitation of Children (ACTESEC) and ALO116-Albanian National Help Line, p. 7, available athttp://www.crca.al/sites/default/files/publications/OPSC%20Alternative%20Report%20Albania%202012.pdf[accessed September 10, 2013].
93Law no. 144/2013»On someamendments toLaw no. 7895, dated 27.1.1995»Criminal Code of the Republic ofAlbania», amended, article 1.
94 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
95 Albania has also ratified ITU with Law No. 8430, date 14.12.1998 "On ratification of Telecommunications Constitution and United Nation Convention, ITU (Geneva 1992)

Law no.10128, dated. 05/11/2009"On ElectronicCommerce"

This law is approximated with Directive 2000/31/EEC "On certain legal aspects of information society services, in particular electronic commerce, in theInternal Market". This law requires that the Provider of the Information Society Services[96] (PISS) ensure to protect the rights of minors in carrying out business (Article 5/c). The law is not specific in this aspectand it does not stipulate what actions and policies PISS should take to make sure that the rights of children are protected. The law holds PISS responsible for protecting its services from being exploited for criminal purposes (Article 5/ç).[97] On the other hand though, it offers two safeguards from this obligation; first, PISS is not accountableif its role is very technical, neutral, passive and intermediate for third parties (Articles 15 and 20).[98]Second, PISS will not be responsible if it has neither knowledge nor control over the information it catches (i.e. for those PISS which offer permanent store of the information Article 17) and hosts (i.e. for those PISS which offer hosting of information) on behalf of its clients (Article 18). PISS, however, is obliged to "terminateorpreventan infringement, if this is required by court or the authority in charge according to the law" (Article 19). Again the term "infringement" here is unclear as it does not specify the offences committed by the user. PISS is also required to inform EPCA immediatelyif it realizes that the user of its services conducts an illegal activity and provides illegal information (Article 20/2). It should be noted that the law does not encourage cooperation between PISS and the state police. Any information sought by the later should be asked through EPCA, and this may be time consuming and harming the investigation.

It does not mention what actions and policies PISS are required to take on child Internetprotection. It is unclear in what situations PISS will be required to intervene and disrupt their service to subscribers. PISSES are required to protect their services, but safeguards offered by the law makes very easy for them to escape to this obligation. Lack of direct of communication among state police and PISS is also a concern.

Law no. 9902, date 17.4.2008, "On the Protection of Consumers", amended with Law no.10444, date 14.2011.

This law is approximated with Directive 2008/48/EEC "On credit agreements for consumers and repealing Council Directive 87/102/EEC". However, the law has not considered the Council Resolution "On the protection of consumers, particularly young people, through the labeling of certain video games and computer games according to age group" 2002/C 65. The latter is not obligatory to EU members and those applying for membership, but it is a very good piece of legal guidance for member states to strengthen their legislation on issues related to the child Internetprotection for minors and parents consuming IT –related equipment and services.

The law has a general definition of what constitutes a consumer. According to article 3.6 a consumer is defined as "anyperson whobuysoruses goodsorservicesforpersonal needs, forpurposesunrelatedto thebusiness orexercise ofprofession". The definition does not categorize the consumer based on age, meaning that minors can also be subject of this law. In addition, consumer goods include the service. Even here the definition is also very broad and it can be interpreted as including online services and goods, such as video games and online games.[99]Other important definitions such as those of "trader", "promotion" and "publicity" are very broad and may be interpreted as including companies trading, offering and supplying online video games.

96 Information society services are " servicesprovided at a distance, against remuneration, , byelectronic means and upon the requestof the recipient of the services" (Article 3/a)

97 This can be interpreted to include grooming, child pornography and sexual harassment via Internet.

98 See also EU Directive 2000/31, Article 42.

99 See article 3.7»Good for consumers», below goods, including goods, used in the sense of providing a service, means anything movable or immovable, whether new, used or repaired, provided for use consumers or that can be used by them, even if it is not provided for them, in terms reasonably foreseeable that became available in the market in a commercial activity."

[100]The law stipulates the rights of consumers and includes "theright to protection ofhealth, environmentand safety of life" (Article 4). This may include cyber environments.

The law lays down requirements for the companies to inform the consumers about the risks and harms they may suffer from the product they offer. However, there is not a single article or section on either minors or the use of toys, video games and online games. It does not have articles or requirements on labeling the product according to the age (i.e. Article 8 on labeling is very general).

The law does not require that the language of advertisement avoid the incitement of hatred, discrimination, harm to children health, etc. The law is limited only to the requirement that the language of advertisement be in Albanian. There can be "exceptionslogansorparts thereof, which may beexpressedinanother language" (Article 22). The law is silent on promotions or apps which are in foreign languages.

While in the definition of "the consumer" the law does not specify minors, in article 48, the law indirectly makes a categorization of the consumers. Here "themostvulnerable groups of consumers, [are] children, the elderly, the poor, the disabled, the sickandpeople withmental and physical disabilities."[101] The institution in charge of hearing the claims of consumers is Consumer ProtectionCommission. It is composed of five individuals ofwhom four are from state institutions and only one is from civil society. [102]

In the discussion related to this law, the opinion of minors has not been sought. The law appears to not have been based on any previous research. The law also does not offer protection for children who use online games.[103] Today there are online games where children can easily enter in a virtual network with others and play with individuals with fake identity. In these games children are an easy target for pedophiles.[104]

Related definitions of law are broad (i.e. consumer, goods, trader, the right of protection of the environment) and are left to the interpretation of the courts and agencies in charge. There is lack of articles which oblige companies to inform minors about the risk of their electronic products and services. There is no article on labeling games according to age appropriateness. Children using online game services are not protected by this law. The opinion of minors (treated as most vulnerable group) has not been consideredin the preparation of the law.

Law no. 10347, date 4.11.2010 "On the Protection of Children Rights"

The law defines "child pornography" at article 3/j. The definition may be interpreted as including the offence of "Internet child pornography". This is evident in the terms ".....display, transmission of pictures, moviesoranyothervisualmaterialthatthe childisdoing...." This law, however, does not include any protection from other forms that may facilitate the violation of children rights generally and their protection from the use of Internet more specifically.

100"Publicity» isany form ofpresentationfortrade, business, craftorprofessionin order to promotethe supply ofgoodsorservices, includingrightsandobligations. (Article 3.11)
«Subject topromoteitsgoodsorservices» aremanufacturers, retailersor service providers, tomakepublicityfortheirgoodsandservices." (article 3.12)
Dealer»means anynatural or legal person, acting forpurposes relating toeconomic activity, trade, business, craftorprofessionandanyoneacting onbehalforin the interestof the trader." (article 3.14)
101 See article 48 in full "The competentstateinstitutionsarethe mainbodiesresponsiblefordevelopingandimplementing policies toprotect consumers, to protect-the basic rights ofconsumers, in particularthegroupsmostvulnerableconsumers, such aschildren, the elderly, the poor, the disabled ,the sickandpeople withmental disabilitiesand physical."
102 The composition of Consumer Protection Commission is of ; tworepresentatives of theMinistry responsible forthe fieldoftrade, one of whom isthe structureresponsibleforconsumer protection;
b) tworepresentativesfrom theMinistryofJustice;
c) representativesofcivilsocietywithexperienceinthe field of economicsandjurisprudence. (article 52)
103 Interview with Altin Goxhaj, Head of the Office on Citizen Protection (ZMK), September 5,2013, Tirana.
104Interview with Marius Gjoka, expert at computer examination unit, General Directorate of Police, Tirana, September 08,2013; Interview with Altin Goxhaj, Head of the Office of Citizen Protection (ZMK), September 5,2013.

For instance the law is silent about aiding, abetting, attempt and conspiracy of sex exploitation of children via Internet or other mediums. In addition, the law seems very difficult in terms of application because it lacks other legal mechanism such as bylaws and provides limited powers to enforcement institutionssuch as National Agency for Child Protection[105] (p. 8 and 11).

The law hasseveral articles thatprovide social safeguards (Article 20), protection from violence (Article 21), economical exploitation (Article 22), use of narcotics and psychotropic substances (Article 23), trafficking and sexual exploitation (Article 24), arm conflicts (Article 25) and torture (Article 26). However, the law neither recognizes the nature of harm that may derive from the excessive use of Internet (which often lead to anxiety and depression), nor does it offer any protection.[106]

The law does not offer protection from the potential harms ofInternetuse and of its side effects for minors. It also lacks protection against actions which facilitate (i.e. aiding, abetting, attempt and conspiracy) crimes against minors, including Internet child pornography.

Law no. 9918, date 19.05.2008 "On electronic communication in the Republic of Albania" amended with Law no.102/2012.

This law regulates the activity of whole networks and electronic communications services, but it does not cover the issues of "illegal" and "harmful". The law has been largely prepared based on similar version of both Czech lawand Macedonian laws.The 2012 amendments approximated the law with Directive 2009/140/ECC on electronic communication [107] and Directive 2002/58/EEC on privacy and electronic communications.

The Electronic and Postal Communication Authority (EPCA)supervises, controls and monitors the activities of ISPs in relation to electronic communications (Article 8). One of the main objectives of the EPCA is the protection of the interests of users of electronic communications services, (article 7 / b). As the term "users" (subscribers) is broad this may include minors too. There is nothing explicit about Internet child protection.[108] EPCA has noobligation to check if ISPs offerservicesto their subscribers regardingthe protectionof minorsonthe Internet(Article 2), butif acompetent authorityaddresses the concern to EPCA, based on a final decision that holds ISP guilty, then the EPCA will terminate the services thatcontain the content harmfulfor minors. Ingeneralterms, the so called "General Authorization" which is issued by EPCA to ISPs, stipulate conditions thatask ISPs to not transmit messages containing illegal content (Article 15of the Law). To date there is not a single case where EPCA has received a decision of the court thatasks them to interrupt the service of an ISP on the grounds of "illegal content for children".[109]

In addition EPCA has noobligationto design policies for Internet child protection. However, it does have the obligation to ask ISPsto take all necessary measures required by the law on the protection of subscribers(including children)from servicesthatmay have harmful andillegal content.For instance, some companies have seen article 122 very broadly, considering the protection of minors from the use of Internet in the interpretation of both "network security" and "potential risks".[110]

105 See the Alternative Report 2012 " Albania: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" prepared by Children's Human Right Centre (CRCA), Albanian Coalition against Child Trafficking and Sexual Exploitation of Children (ACTESEC) and ALO116-Albanian National Help Line, p. 8-11, available at: http://www.crca.al/sites/default/files/publications/OPSC%20Alternative%20Report%20Albania%202012.pdf [accessed September 15, 2013].
106 For more see Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011).Risks and safety on the Internet: The perspective of European children. Full Findings. LSE, London: EU Kids Online.
107 This Directive amended Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services.
108 Interview with Irena Malolli, Head of Postal and Electronic Communication, National Agency for Information Society, August 14, 2013.
109 Interview with Rudolf Papa, legal adviser at Electronic and Postal Communication Authority, September 2,2013.
110 Interview with a representative of ALBtelecom & Eagle Mobile, September 21, 2013.

In addition, according to the general conditions stipulated at the General Authorization issued by EPCA, the latter has the power to ask ISPs to deposit with EPCA an action plan which reflects the measures taken by the ISPs for protectionofsubscribers. These measures should be reflected in thegeneral terms and conditions of the contract between ISPs and their subscribers (Article 15/e, Articles99and122).

The law compels "the networks and electronic communications services to maintain and administerdata files of their subscribersfor a two-year term" (Article 101 / 1 `) and this information should be made available to the authorities upon their request in accordance with the procedures of the Code of Penal Procedures (Article 101/3). The law specifically defines which data the ISPs should store for two years. The list is extensive and includes almost everything related to the subscriber's identity (i.e. date and time of connection and disconnection (log on and log off), number of the phone where the communication is made and so forth (Article 101/3). However, the law does not required ISPs to check or select which content is illegal and harmful for minors and people generally. As mentioned in the first section, this would violate the freedom of expression. In this context, ISPs play a very neutral and passive role in relation to the control of illegal content. ISPs are bound by the law to ensure the confidentiality of communications and this includes content, traffic data and location (Article 123).

The law also obliges ISPs to offer a secured network and also inform the subscribers about risks and safeguards they provide (antivirus software) (Article 122). So, the law is restricted to protecting the network but not of the content, which is inside of the network. In this context, the ISPs are bound only by their-code of conduct, which is not binding, to somehow offer services to their customers in terms of "illegal content". Too much is left to the integrity of the ISPsand because of the high cost, especially for small ISPs, they invest little in training their staff to properlyadminister the data. As one IT expert highlighted, "ISPs do not have clear policies and technological capacities to prevent 'illegal content' and they do not invest because of the high cost of enabling filters. Irresponsibility is also an issue. Often during their internal audit, they may illegally access the data of their customers. Emails, sites visited by their customers and even VoIP are intercepted illegally simply to kill time during the night shift. This illegal access is called 'sniffing' and this and similar techniquesare simple and do not require high level expertise. It seems difficult for the ISPs in Albania to be able to control or prevent this phenomenon."[111]

In addition, there are two uncontrolled business activities where children are highly exposed to illegal content: first, Internetcafés and second, enterprises thatsell used computers.[112] The latter are totally off the radar of the regulators and they are only visited by tax revenue officers. The former can be subject of the EPCA only when they are registered according to the General Authorization. This means that they operate as ISPs or use frequencies authorized by the EPCA after receiving an Individual Authorization. If Internet-cafésoffer their services based on their contracts with ISPs, then they are not subject of EPCA.[113]ISPs often find that an individual applies to use the Internet for his home but in fact he intends to open an Internetcafé.[114]Internetcafésare the main place where children watch pornographic material,especially among a mixed community of minors and adults.[115]

This law does not address the issues of "illegal" and "harmful" content. There is nothing explicit about child Internetprotection. The role of EPCA is very neutral in checking ISPs service, which may contain illegal content. EPCA can only intervene after receiving a court order. This means that EPCA plays a very passive role in preventing cyber crime related issues. EPCA has limited powers to regulate and supervise one of the main hubs of Internet pornography, Internetcafés, andit has no control on the sale of used computers.

111 Interview with an IT expert, September 25, 2013.
112 Interview with Zamir Hoxha, Head of the Cyber Agency for Cyber Security (ALCIRT), September 10,2013.
113 Interview with Rudolf Papa, legal adviser at Electronic and Postal Communication Authority, September 2,2013.
114 Interview with Zamir Hoxha, Head of the Cyber Agency for Cyber Security (ALCIRT), September 10,2013.
115 Interview with Altin Goxhaj, Head of the Office of Citizen Protection (ZMK), September 5,2013.

Cyber crime legislation [116]

The Ministry of Justice issued a series of amendments to both material and procedural law regarding cyber crime related offences in the last five years. There have been two substantial changes; the first in 2008[117] and the second in 2013.[118] The first amendments of 2008 were not sufficient and did not include in the range of punishable offences the "possession of child pornography material". It was not until 2013 that Albania amended article 117s of the Penal Code to cover almost all actions related to child pornography through the use of computer and Internet, such as production, distribution, advertising, import, sale, offer, and possession and publication of pornographic materials.[119] Creating access to child pornography materials extends to ISPs and every form. The term used is very broad. It includes everyone who "creates access by any means" (Article 117).

While, the Cyber Crime Convention defines "child pornography" (article 2 a, b, and c), there is not such a definition in the Albanian Criminal Code. Albanian experts say that in this case the court refers to the definition provided by the conventions adhered to. This is why the legislator has likely not seen the need to have a special article despite the confusion it might generate.[120] During our interviews, we pointed out to Albanian experts that Albania has ratified various conventions (UN, Council of Europe, and EU) and each of them has a definition of "Internet child pornography". Their response was that all related conventions have very similar definitions for this offence.[121] It is important to mention that the title of article is "pornography" and the term child comes later in the text.[122] As mentioned above, the definition of "child pornography" appears at the Law no. 10347, date 4.11.2010 "On the Protection of Children Rights", article 3/j. It would have been more effective and it would have avoided confusion if a proper definition of "Internet child pornography" had been added to the Penal Code. The Law no. 10347 (mentioned above) sets out the rights of children who need to be protected, but offences are listed in the Penal Code. It is here where the definition of both "child pornography" and/or "Internet child pornography" should have been included. The lack of a definition for "child pornography" was also pointed out by civil society in 2012 and it is unclear why this concern was not addressed by the 2013 amendments to the Penal Code.[123] This anomaly of technical legislation may open opportunities to confuse the interpretation on the part of law enforcement agencies. Even in consolidated states the issue of defining "Internet child pornography" is still debated and poses a big challenge for prosecutors and judges.[124]

It is unclear why in the latest amendments to article 117 the law also does not consider "procuring child pornography through a computer system for oneself or for another person" despite the fact that this is a requirement of the Cyber Crime Convention (article 9.d). Albanian legislators seem to have been unclear about the translation of the term "procuring" from the Cyber Crime Convention because it is translated literally in the Albanian as "prokurimi". While there is not a definition of "prokurimi" in Albanian Civil Code, we have referred to the Law of Public Procurement no. 7971, date 26. 7. 1995, amended. Even here the definition of "prokurimi" is broad. It is defined as "buying, leasing or any other contracting of goods, construction and services" (Article 2).

---

116 Cyber crime legislation is not a special law but for reasons of practicality articles related to cyber offences have been gathered together and posted on the websites of the Ministry of Innovation, Information Technology and Communication. For more see its website on legislation available at: http://www.mitik.gov.al/index.php/legjislacioni [accessed September 20, 2013].

117 Law no. 10054/2008, "For some amendments to Law no. 7905/1995 "The Code of Penal Procedures of the Republic of Albania"", revised, which facilitates the procedures for the enforcement of new changes of Penal Code on cyber crime. For more refer to the " Council of Europe "Third Report Submitted by Albania Pursuant to Article 25, Paragraph 2, of the Framework Convention for the Protection of National Minorities" to Council of Europe, January 10,2011, p.30, available at: http://www.coe.int/t/dghl/monitoring/minorities/3_fcnmdocs/PDF_3rd_SR_Albania_en.pdf [accessed September 20, 2013].

118 Law no. 144/2013"On someamendments toLaw no. 7895, dated 27.1.1995"Criminal Code of the Republic ofAlbania", amended.

119 See the Alternative Report 2012 " Albania: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" prepared by Children's Human Right Centre (CRCA), Albanian Coalition against Child Trafficking and Sexual Exploitation of Children (ACTESEC) and ALO116-Albanian National Help Line, p. 7, available athttp://www.crca.al/sites/default/files/publications/OPSC%20Alternative%20Report%20Albania%202012.pdf[accessed September 20, 2013].

120 Interview with Elton Kercuku, Head of Cybercrime Unit, General Directory of Police, September 11,2013.

121 Interview with Elton Kercuku, Head of Cybercrime Unit, General Directory of Police, September 11,2013

122 Interview with Elton Kercuku, Head of Cybercrime Unit, General Directory of Police, September 11,2013

123 See the Alternative Report 2012 " Albania: Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography" prepared by Children's Human Right Centre (CRCA), Albanian Coalition against Child Trafficking and Sexual Exploitation of Children (ACTESEC) an ALO116-Albanian National Help Line, p.10.

124 Wells, M., Finkelhor, D., Wolak, J., & J. Mitchell, K., (2007) "Defining Child Pornography: Law Enforcement Dilemas in Investigations of Internet Child Pornography Possession", Police Practice and Research, Vol. 8, No. 3, p. 269–282, http://unh.edu/ccrc/pdf/CV96.pdf[accessed September 22, 2013].

Another offence which is not considered by both Albanian and the Cyber Crime Convention is "the acquiring" of child pornography materials. The term "acquiring" and "purchase" are distinct terms from "procuring". Procuring for instance includes different actions like "market research and vendor evaluation and negotiation of contracts "and it is not limited to purchase."[125] The term "procuring" is explained by the Explanatory Note of the Convention as "actively obtaining child pornography, e.g. by downloading it", but it does not mention "acquiring" as part of the process.[126]

There are also two offences that are missing in the Albanian cyber crime legislation, first, "knowingly obtaining access to child pornography" (i.e."kerkesa per blerje, perdorim personal, shfrytezim per qellime tregtare, etc." and secondly "grooming").[127] Albanian experts note that "acquiring and obtaining access" is integrated in paragraph 2 of article 117 in the sentence "consciously creatingaccessto, byany meansorform".[128] Again this term is ambiguous as it does not specify whether this is for those accessing illegal material for themselves or for those who facilitate it for others.

The approach taken by the actual Albanian cyber crime legislation appears to be individually centered, whereby it does not consider situations when offences can be committed in organized form or by organized crime. In this respect, Albanian cyber crime legislation lacks other actions and this may encourage offences such as instigation, aiding, abetting, attempt and conspiracy.[129] For instance, the Albanian Criminal Code is harsher when trafficking of women or drugsis conducted by an organized group or in an organized way.[130] Article 286/a considersit a separate offence to illegally use advanced technologies for the production, trade and facilitating of narcotics, psychotropic substances and other criminal activities (i.e. in articles 283-286/a of the Code), but it does not include child pornography material or use of advanced technology for the trade of child pornography materials. In the Criminal Code there are articles related to organized forms of committing a crime and they may be interpreted in the context of an organized child pornography activity on the Internet, but this is still a matter of interpretation.[131]

Furthermore, neither Albanian Law nor the Cyber Crime Convention has an article on those offenders who cooperate with law enforcements agencies to facilitate the investigation. Article 284/b of the Albanian Criminal Code only offers reduced prison time for offenders who help law enforcement agencies investigate crimes related to trafficking of drugs, weapons, illegal immigrants, or prostitution, and offenses committed by organized crime. Investigation of Internet child pornography is very complicated as it deals with environment of a rapid change in technology, multi-type computer uses and can be a cross border crime. While the investigation of other crimes may allow more time, investigation of child pornography through theInternet needs to be swift as the digital traces can be hidden or destroyed quickly and the offender can escape easily. So, the cooperation of a repented offender can be a very effective tool for prosecutors.[132]

In other Albanian legislation related to child protection, children are seen as a privileged category for protection by extending the range of actions that constitute an offence. It is difficult to understand why a similar approach has not been followed by the legislators in the context of Internet child pornography. For instance, article 117 does not penalize when the offence has serious consequences for the health of the minor, what is otherwise known as "aggravating circumstances". In this situation, the penalty, referring to EU legislation becomes harsher when the life of the child has been endangered and seriously harmed (Article 7 of 2009 Council Framework).

125 For more see Purchasing Insight available at: http://purchasinginsight.com/resources/what-is/definition-of-procurement-procurement-vs-purchasing/[accessed September 22, 2013].
126 See Explanatory Note of the Convention on Cyber Crime point 97, available athttp://conventions.coe.int/Treaty/EN/Reports/Html/185.htm[accessed September 25, 2013].
127 See Kambellari, E., "Mbrojta e te Mitureve ndaj Formave te Dhunes Seksuale Nepermjet Internetit", p.162, at "Konferenca Shkencore:Dhuna Kunder Femijeve ne Shqiperi, Tirana 21 November 2012, available at:http://www.unicef.org/albania/Dhuna_kunder_femijeve_ne_Shqiperi.pdf[accessed September 25, 2013].
128 Interview with Elton Kerluku, Head of Cybercrime Unit, General Directorate of Police,, September 11,2013.
129 Conspiracy to commit a crime is often included in criminal law of countries, which respond quickly to "modern" crimes such as cyber crime. See United States Code, Title 18, chapter 19, article 371 (conspiracy to commit an offence), available at: https://www.fas.org/irp/offdocs/laws/usc18.html[accessed September 24, 2013].
130 See article 114/b women trafficking is charged with both penalty and imprisonment from 7 to 15 years and if it is organized from 10-15 years. Drug trafficking is charged with 7 to 15 years of imprisonment. When it is organized is charged with 10 to 20 years of imprisonment (article 283/a).
131 Interview with Elton Kerluku, Head of Cybercrime Unit, General Directorate of Police, September 11,2013. See also articles 25-28 of Penal Code.
132 Wells, M., Finkelhor, D., Wolak, J., & J. Mitchell, K., (2007) "Defining Child Pornography: Law Enforcement Dilemas in Investigations of Internet Child Pornography Possession", Police Practice and Research, Vol. 8, No. 3, p. 272, http://unh.edu/ccrc/pdf/CV96.pdf[accessed September 23, 2013].

EU member states are required to include the following offences – "acquiring", "knowingly obtaining access", "grooming", "instigation", "aiding", "abetting" and "attempt" and "aggravating consequences" –into their national law according to the EU Council Framework decision 2004/68/JHA on child pornography, repealed by similar Council Framework decision of 2009.As this framework notes, these offences will cover other activities related to Internet child pornography because " cases where viewing child pornography from websites without downloading or storing the images does not amount to "possession of" or "procuring" child pornography."[133]Including these offences in the criminal law will bring Albanian legislation into compliance with the EU Law, which in fact is a perquisite of Albania joining the EU.[134] It should be noted that there is a growing concern by experts noting that today there are individuals in Albania who are soliciting and visiting child pornography sites. [135] As one of the interviewees noted, "While not on a large scale, we have Internet child pornography...we have more Albanians visiting these sites rather than foreigners targeting Albania..."[136]

The Cyber Crime Convention sets out the minimum standards that each member state should include in both its material and procedural law. Member states are free to stretch their national law to cover other offences that they may consider serious. The Convention itself considered offences related to Internet child pornography as "of the most dangerous *modi operandi* in recent times", hinting that member states can extend the range of offences above the threshold set out by the Council of Europe and criminalize more situations.[137] There areother offences included in the 2013 amendments of the Penal Code but which do not appear in the so-called "Cyber Crime legislation". The offence is sexual harassment and it includes "conduct of a sexual nature with every tool or form" (Article 108/a).[138] The term "every tool" can be interpreted as sexual harassment via the use of Internet. The legislation provides a harsher penalty if sexual harassment is committed against minors. In this context, Albanian cyber crime legislation should also include sexual harassment against minor through the use of Internet. There is no safeguard, however, provided by the Albanian law in cases where someone may deal with child pornography materials for non-criminal purposes (i.e. scientific and academic).[139]

It should be noted that there have been attempts by the executive branch and civil society to improve the criminal law on Internet child pornography, but significant proposals made by representatives of civil society and some members of government were not integrated into the law. For instance, representatives of CRCA proposed that Internet pornographic materials thatdo not constitute evidence for the investigation be destroyed. According to article 101/1 of the Law on Electronic Communication, the data stored by ISPs should be destroyed after the two-year deadline stipulated by the law terminates. Referring to the actual practice, in general online materials thatare accessed or examined for investigation of cyber crime related offences are not destroyed.140 Civil Society also proposed that all individuals charged for Internet child pornography be listed in a national register of sexual offenders.141 Another important proposal, which came from Majlinda Bregu, then the Minister of Integration, was about cyber stalking.142 This is an offence that is stipulated at the Council of Europe Convention on preventing and combating violence against women and domestic violence in general (2011).143 This convention was ratified by Albania. According to article 34, state parties are required to create a specific criminal offence of "stalking" with a non-exhaustive list of actions and subjects. The article is broad and it can be applicable when children are victim of cyber stalking.

133 Council Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography,2009, p.5.
134 According to article 70 of the Stabilization and Association Agreement with EU Albania is required to approximate its legislation with the EU. See National Plan for the Implementation of the Stabilisation and Association Agreement 2012-2015 of Council of Ministers, July 2012 at p.3.
135 Interview with Marius Gjoka, expert at computer examination unit, General Directorate of Police, September 08,2013.
136 Interview with Elton Kercuku, Head of Cybercrime Unit, General Directorate of Police, September 11,2013.
137 See Explanatory Note of the Convention on Cyber Crime, point 35available athttp://conventions.coe.int/Treaty/EN/Reports/Html/185.htm[accessed September 25, 2013].
138 This article is borrowed by Council of Europe Convention on preventing and combating violence against women and domestic violence (2011), article 40.
139 See Explanatory Note of the Convention on Cyber Crime for the term "without right" at article 9, point 103available athttp://conventions.coe.int/Treaty/EN/Reports/Html/185.htm[accessed September 20, 2013].
140 Interview with Marius Gjoka, expert at computer examination unit, General Directorate of Police, September 08,2013.
141 See the discussions of the Member of Parliament regarding the 2013 amendments of cyber crime law at the Minute date April 09,2013, held by the Parliament Commissionon Legal Affairs, PublicAdministrationandHuman Rights, p.12-13.
142 See the discussions of Majlinda Bregu, then Minister of Integration a the Minute of the the Member of Parliament regarding the 2013 amendments of cyber crime law at the Minute date April 03,2013, held by the Parliament Commissionon Legal Affairs, PublicAdministrationandHuman Rights, p. 06.
143 See the Report of Ms. Gisela Wurm, before the Committee on Equality and Non-Discrimination, Parliamentary, Assembly, Counsel of Europe, available at: http://www.assembly.coe.int/Communication/24062013_Stalking_E.pdf[accessed September 27, 2013].

Cyber crime legislation does not include a definition on "Internet child pornography". The law does not cover other important criminal activities related to the main offence such as "knowingly obtaining access", "grooming", "instigation", "aiding", "abetting" and "attempt" and "aggravating consequences". The law is also missing a safeguard for when access to illegal content is made for non-criminal purposes.

Enforcement and cooperation

A good law is only as good as its enforcement. Lack of enforcement remains a problem regarding the fight against crime generally and especially sophisticated crimes such as cyber crime. There are several agencies that deal with investigation of cyber crime such as, the prosecutor, state police (i.e. special cyber crime units and a unit on computer examination) and the secret service (ShiSh). It should be mentioned that the above units of the General Directorate of Police are not separate entities but are part of key directorates (i.e. cyber crime unit is under Financial Crime Directorate and the unit on computer examination is under Directorate of Forensic Police).[144] There are also other units dealing with cyber security such as Cyber Agency for Cyber Security (ALCIRT) attached to the Council of Ministers and another unit thatthe Ministry of Defense plans to open.[145] This segregation of units hampers cooperation and decreases efficacy.[146]

The main unit in charge of fighting cyber crime generally and Internet child pornography more specifically are units attached to the state police. There is one at the General Directorate of Police composed of four people. There are also special units within the state police of each region. The largest one is that of Tirana with 3 people and all others have only one person in charge of cyber crime offences. The unit in the General Directory of Police coordinates, designs policies and serves as an operative unit in the fight against cyber crime. The people working in these units have qualified from the academy of police and also been trained in fighting cyber crime. The unit of computer examination serves examines all evidence related to crimes involving information technology. In addition, state police units have a very good cooperation with international state police such as Interpol and Europol and also with powerful national agencies such as SOCA, the main UK law enforcement agency dealing with serious organized crime.[147] All members of the Cyber Crime Convention (2001) have an open channel 24/7 to communicate and share information in order to facilitate investigation and prevent harm in time.

Cyber crime units of the state police seem to cooperate well with the prosecutor and ShiSh.[148]The General Directorate of Police has a memorandum of cooperation with the latter. Collaborationwith ALCIRT is not permanent and is made via project. The later is more focused on the protection of national security and people working there are highly specialized in IT. They are IT engineers. ALCIRT, however, has taken a role in coordinating public and ISPs in combating Internet child pornography. In the Code of Conduct of the ISPs there is an email account where children and everyone who wants to report a crime, such as those of child pornography, and this is managed by ALCIRT, which later sends the message and liaise to the respective institution. This is not clear how it works as the process has just started. ALCIRT has opened a year ago and is still notpresent on the website of the Council of Ministers. There are problems with the investigation of Internet child pornography. In general the investigation techniques used by cyber crime unit of state police are classic (i.e. used for every crime). Information comes from two sources, open sources (claims from the victim, parents or any citizen, anonymous, and the media) and second by closed sources (informants).

144 See unites (seksione) in charge of cyber crime at the structure of the General Directory of Police available at: http://www.asp.gov.al/images/pdf/struktura_dhj2010_DPP1.pdf [accessed September 25, 2013].
145 Interview with Zamir Hoxha, Head of the Cyber Agency for Cyber Security (ALCIRT), September 10,2013, Tirana.
146 Interview with Elton Kerluku, Head of Cybercrime Unit, General Directorate of Police, September 11,2013
147 See the visit of Hudley GILL, the Regional Director of SOCA to General Directorate of Police in November 2012. For more see at: http://www.asp.gov.al/index.php?option=com_content&view=article&id=2837%3Adrejtori-i-pergjithshem-i-policise-se-shtetit-z-hysni-burgaj-sot-priti-ne-nje-takim-z-hudley-gill-drejtori-rajonal-i-agjensise-britanike-soca-s&catid=41%3Ainformation-for-press&lang=sq [accessed September 20, 2013].
148 There has been a serious of actions where offenders have been caught in flagrance, thanks to the efficient cooperation between cyber crime units and prosecutors. For more see the description of coordinated actions at the operation coded "Illegal Internet" in 2011, available at: http://www.asp.gov.al/index.php?option=com_content&view=article&id=1726%3Aprocedohen-penalisht-dy-shtetas-per-mashtrime-kompiuterike-arrestohen-dy-te-tjere-per-vjedhje&catid=41%3Ainformation-for-press&lang=sq [accessed September 20, 2013].

It should be pointed out that Albanian Code of Procedure stipulates that everyone is obliged to report to the law enforcement agencies if he has knowledge about a legal activity (Article 283). This includes the employees of the ISPs. However, in general experts of the cyber crime unit are not satisfied with the level of cooperation provided by ISPs. While ISPs are required by the law (article 101 on Electronic Communication) to keep the data, including the Internet Protocol (IP), in practice this seems to have not been followed by all.[149] In addition, state police cannot ask ISPs for the information directly according to the Electronic Communication Law, but it should go through the Electronic and Postal Communication Authority (EPCA), which delays the procedure and hampers cooperation.

The Explanatory Note of Council Framework decision of 2009 also suggests an interesting point which may be consideredfor use as an explicit article to be included in the Albanian legislation: to hold ISPs liable if they have knowledge and control of the illegal content they host. The law may be amended to hold ISPs liable for being passive and neutral in cases where they may discover that their user possesses child pornography materials.[150] While this is difficult for ISPs to control, Kambellari (2012:p.164) suggests that "ISPs [may be required by the law] to develop the technical methods necessary to secure the traffic control communications content they transmit and the signaling mechanisms for cases of distribution or publication of materials with illegal content through their networks."

There is a growing debate today even in the EU legal community about the difficulties that arise in interpreting the liability of ISPs in terms of managing and preventing the flow of illegal content offered by their networks or services.[151] Another issue regarding the investigation of Internet child pornography is on the ambiguity and the difficulty that law enforcers confront when interpreting legal provisions of Code of Criminal Procedures related to articles 299/a and 299/b (i.e. expedited preservationandmaintenanceof thecomputer data). As Mrs. Kerluku notes " these articles, although copy pasted from the Cyber Crime Convention, are ambiguous and leaves room for interpretation... and this is something that we discussed among us. Even representatives of Council of Europe have suggested to us that we should improve cyber crime legislation and procedures and adapt to the Albanian context". [152]

There is lack of a cooperation strategy between law enforcement agencies. Their architecture is more focused on cyber security. The Penal Code of Procedures should be amended as the related articles on collection of evidence are vague. As mentioned above, the regulatory law makes it difficult for state police to access ISPs directly for information. The law is not very clear about the role and obligation of ISPs in preventing Internet child pornography.

149 Interview with an expert at computer examination unit, General Directorate of Police, September 08, 2013.
150 Kambellari (2012: p.164) interpreting article 3 of Law no.9754, 2007, "On the Criminal Liability of Legal Persons", highlights that ISPs and every other legal persons (i.e. those who offer service, products, and advertise) can be held responsible if the ISP has knowledge about the existence of child pornography material consumed by its client.
151 The debate is about the interpretation of Article 14/1 of e EU E-commerce Directive (2000/31/EC) which specifies condition of ISPs liabilities' exemptions. For more see the analysis of JF Bretonniere (2011) "Europe: Liability for Internet host providers in the European Union: time for a reform?" Baker & McKenzie Europe, available at: http://www.iam-magazine.com/issues/Article.ashx?g=f8e060f5-378c-4979-a1d5-0ef3a42f0c9c[accessed September 27, 2013].
152 Interview with Elton Kerluku, Head of Cybercrime Unit, General Directorate of Police, Tirana, September 11,2013

Policy Making Recommendations

1. Raise public awareness among parents, children, teachers, ISPs, public institutions and media.

2. Government policies should also consider the interest of minors and self-awareness among minors should be encouraged.

3. Offer an interactive "hotlines" by the State Police (cyber crime unit) with respect to the reporting of abuse of minors online.

4. More cooperation between different interest groups is needed along with legal regulation.

5. ISPs should be required by the law to install special devices which can indicate that transmitted content is illegal and harmful for minors in the network services they offer. There is software on the market that can monitor the content using key words.

6. ISPs should be asked by the law to offer protective services (parental control tools, filters), either free or based on small fees.

7. Mobile companies should provide filters for minors ordering mobile phones and Internet service within.

8. There are not many tools suitable for game consoles, tablets and mobile phones – the devices increasingly used by children to go online - and there are no solutions for users who access content on mobile phones or tablets using an application and not a browser.

9. School personnel who teach IT should have proper qualifications and be trained annually by MES. Training should be extended to kindergarten personnel as well about the risk of child pornography generally and Internet child pornography specifically.

10. School IT curriculumshould be updated regularly and expanded to includechildInternetprotection.

11. Awareness campaigns should not be only on "Internet day" and on pilot schools but they should be organized in permanent and long-term programs.

12. Cyber crime units should include more IT expert and have their own IT forensic specialist.

13. The General Prosecution should have a special section on cyber crime and prosecutors trained with issues of Internet child pornography.

14. Courts should have special judges dealing with cyber crime offences.

15. A memorandum of cooperation should be arranged among all law enforcement agencies.

16. Penal Code and Procedural Code should be improved to include a definition of "Internet child pornography" and other facilitating actions such as "abiding", "conspiracy", etc.

17. The law should be improved to allow state police and other law enforcement agencies to ask for data from ISPs directly and not through EPCA.

18. Powers of EPCA should be extended to monitor and supervise Internetcafés. An article in the contract between ISPs and Internetcafés may be added to stipulate this power, when the later are not registered within EPCA.

19. Powers of EPCA may include monitoring the sale of used computerseven if they are certified from abroad as not containing illegal content. In addition, custom should not allow used computers, which do not bear a clearing certificate, to be traded in Albania.

Legislation Recommendations

1. Law no. 97/2013 "On Audiovisual Media in the Republic of Albania" should be revised, especially the definition of "harmful content". The definitionshould include content promoted via or related to IT goods and services that may harm children.

2. Law no. 10128, dated. 05/11/2009 "On Electronic Commerce" needs to be revised and indicate what actions and policies the Provider of the Information Society Services (PISS) should take on Internet child protection. The law should also be clear aboutsituations in which PISS will be required to intervene and disrupt their services to subscribers.

3. Law no. 9902, date 17.4.2008, "On the Protection of Consumers", amended with Law no.10444, date 14.2011 needs to be revised. The law should provide clear definitions for consumer, goods, trader and the right of protection of the environment. Companies should be obliged to inform minors about the risk of their electronic products and services. It should contain an article on labeling games for age appropriateness. The law should also require that the language of advertisement avoid the incitement of hatred, discrimination, harm to children's health, etc. Specific articles should be added to offer protection for children using the services of online games. This is aserious issue considering the significant business incentive for the continual development of smart phones, laptops and PCs. It is estimated that there were more than 5 billion mobile subscriptions worldwide and sales of video gameswere predicted to reach around 62 billion euro in 2012.In the new amendments of the law the opinion of minors (a most vulnerable group) should be sought.

4. Law no. 10347, date 4.11.2010 "On the Protection of Children Rights" should be revised and offer protection from the potential harmful effects of Internet use for minors.

5. Law no. 9918, date 19.05.2008 "On electronic communication in the Republic of Albania" amended with Law no.102/2012 should be revised. It should explicitly address the issues of "illegal" and "harmful" content. It should be more explicit about Internet child protection. The role of The Electronic and Postal Communication Authority (EPCA) should be more proactive in supervising the ISPs service which may contain illegal content. More power should be given to EPCA to regulate and supervise Internetcafés and the sale ofused computers. This law should allow for direct communication among state police and PISS in terms of cyber crime issues. The law should be more clear about the about the role and obligation of ISPs in preventing Internet child pornography.

6. Cyber crime legislation should also be amended. It should provide a definition of "Internet child pornography". The law should add other offences related to the main offence such as "knowingly obtaining access", "grooming", "instigation", "aiding", "abetting" and "attempt" and "aggravating consequences". The law should also consider as offences actions which facilitate Internet child pornography (i.e. aiding, abetting, attempt and conspiracy). EU member statesare also required toinclude these offences into their national law according to EU Council Framework decision 2004/68/JHA on child pornography, repealed by similar Council Framework decision of 2009.

7. Cyber crime law should offer safeguards for those accessing"illegal" and "harmful" content via Internet for non-criminal purposes (i.e. scientific and academic).Albanian cyber crime legislation should also include sexual harassment against minors through the use of theInternet. The Penal Code of Procedures should be amended as the relevant articles on the collection of evidence are vague.

8. The European Commission encourages the service providers and third party content providers to filter and label the material, as this can be more effective. European Commission suggests several policies that may be adopted by Albanian authorities.

9. Other member states such as Hungary, Poland, Portugal, Iceland and Norway left it to the e-commerce Directive (Directive 2000/31) to set down rules to deal with this matter. Albania has not yet transposed this Directive to its legislation and e-commerce law is still pending.