LLM Thesis for the Research Master in Law


Thesis Supervisor  Dr. E.J. Koops
Department          TILT
Author              L. Jasmontaitė
Date                April 10
Abstract

This thesis presents an exhaustive overview of the state of the art concerning children’s online safety in the European Union in relation to self-regulation. Recently, this complex topic has been frequently addressed by policy makers and diverse stakeholders in a lively public debate, which unfortunately have not led to substantial outcomes as parties involved tend to get overemotional or present one-sided opinions. Furthermore, it appears that arguments provided in the debate are not based on a coherent legal analysis of the current regulatory approach. Therefore, the thesis aims at capturing underlying legal and regulatory aspects related to self-regulation of children’s online safety. In order to provide a full picture of issues at stake, first, the thesis defines the problem of children’s online safety, and then it provides origins and the state of the art regarding the European regulatory approach and its latest developments in relation to this problem. Subsequently this thesis introduces empirical data proving the seriousness of the existing situation and problematic regulatory aspects surrounding the problem. Secondly, the thesis presents a firsthand experience on the debate over the children’s online safety, which was observed by the Digital Agenda Assembly. This is followed by a normative analysis of the self-regulatory initiative titled “The European Union Safer Social Networking Principles”. The analysis is based on the test of good regulation, proposed by Baldwin and Cave. The thesis is concluded by remarks recapitalizing the main findings.
Contents

Abstract.................................................................................................................................................. 2

Introduction............................................................................................................................................ 5

Chapter I................................................................................................................................................ 7

The state of the art of the regulatory framework protecting children’s online safety in the EU ............ 7

1. Chapter overview.................................................................................................................................. 7

2. Why is children’s engagement online problematic? ........................................................................... 7

3. Children’s engagement online in Europe: empirical data.................................................................... 8

4. The best practices for minimizing online risks in the European region ............................................. 9

5. Is it possible to apply the best practices originating outside the European borders? ................. 13

6. The perception of responsibility for the Internet’s safety: development in the EU .................. 14

7. What is the most appropriate level for adopting regulation of children’s online safety in the European region? .................................................................................................................. 15

8. Heading towards regulatory action enhancing online safety in the EU ........................................ 17

   a. The primacy of self-regulation ensuring children’s online safety............................................... 18

9. Troublesome aspects of children’s online safety regulation............................................................ 19

   a. Risk and its perception .................................................................................................................... 19

   b. Definition of children’s online safety .......................................................................................... 20

10. Conclusion.......................................................................................................................................... 20

Chapter II............................................................................................................................................... 22

Insights to the debate on children’s online safety ................................................................................ 22

1. Chapter overview.................................................................................................................................. 22

2. The Communication on the Digital Agenda: the way forwards ....................................................... 22

   a. The Core of Action 37..................................................................................................................... 23

   b. Politicians shape the regulatory approach towards children’s online safety ............................. 23

3. Reflections on the workshops of the Digital Agenda Assembly ..................................................... 24

   a. The Digital Agenda Assembly ..................................................................................................... 24

   b. Observations of the workshop on cyberspace security ............................................................ 24

   c. Observations of the workshop on children’s online safety .................................................... 25

4. Concluding remarks............................................................................................................................. 26

Chapter III.............................................................................................................................................. 27

The Normative Analysis of the Safer Social Networking Principles for the EU ................................. 27

1. Chapter overview.................................................................................................................................. 27

2. Diverse perception of the notion ‘good regulation’ ........................................................................... 27

3. Introduction to the Safer Social Networking Principles ................................................................. 28

4. The rationale behind the development of the Principles .................................................................. 29
5. Can the Principles on the Safer Social Networking be regarded as a good regulation? ........ 30
   Question no. 1 ......................................................................................................................... 30
   Question no. 2 ......................................................................................................................... 31
   Question no. 3 ......................................................................................................................... 32
   Question no. 4 ......................................................................................................................... 33
   Question no. 5 ......................................................................................................................... 33
   Concluding remarks of the good regulation test .................................................................... 34
6. Other peculiarities of the Principles .................................................................................... 34
7. Concluding remarks ............................................................................................................. 35

Conclusion .................................................................................................................................... 36
Bibliography .................................................................................................................................. 38
Annex I .......................................................................................................................................... 40
   a. Summary .......................................................................................................................... 40
   b. Questionnaire .................................................................................................................... 41
   c. Interview transcript ........................................................................................................... 42
Introduction

It is acknowledged that enhancing trust and security of the Internet is the most important step that has to be taken in order to enjoy opportunities that are provided by the digital world[1]. Following this, ensuring the safety of the Internet services for all users is a primarily goal which will also foster a confidence of the Internet services. In particular, the attention should be drawn to the children as they are considered to be the most vulnerable group in the terms of risks that they are exposed while engaging in the online activities. However, the current situation regarding children’s safety online in the European context is somewhat awkward as the possibility to develop regulation measures is entrusted in the hands of private actors without having measured the possible impact of this regulatory approach in the long run. Therefore, it is worth analyzing the context in which self-regulation is developing.

The main objective of this thesis is to provide an elaborate analysis of the current situation regarding children’s online safety in the European Union (EU) in relation to self-regulation from a legal perspective and to discuss points of improvement in the existing regulatory approach. The sociological implications of children’s engagement in the online activities have been discussed at large by social scholars in a vast number of empirical studies, pointing out the risks and harm that children might experience while being online. However, legal scholars seem to lag behind in this debate as it is mostly seen through the lens of criminal law. The possibility to approach this topic by means of regulatory theories, in particular by self-regulatory modes, is to a large extent ignored, although legal scholars by applying the regulatory theory as a multidisciplinary subject could contribute to the issue at stake by combining sociological and legal aspects and presenting an in-depth analysis of the topic. Thus, this thesis goes one step further than the traditional approach towards the problem of children’s online safety and it addresses the issue in a broader regulatory context.

This thesis presents a qualitative research, which to a large extent is based on the technique of desk research which results in a systematic literature review. The systematic literature review is enriched by information obtained through a semi-structured interview and a firsthand experience at the conference, which focused on the issues related to children online safety. The significance of the thesis lays in the application of a good regulation test, which conceptualizes a theoretical framework and specifies the underlying aspects regarding self-regulation. Based on the application of different methods and topics covered, the thesis is divided into three chapters, which eventually answer the central thesis question: What is the state of the art regarding the regulatory approach towards children’s online safety in the EU?

The first chapter introduces the origins and state of the art of the regulatory approach to children’s online safety. The chapter briefly introduces recent empirical data concerning children’s engagement in the Internet and it also provides a brief overview of the existing best practices aiming to fight the problem on the European level. Although the chapter primarily focuses on the EU level, subsequently it touches upon the international law and compares the positions on the issue of children’s online safety of two main actors in the European region, namely the European Union and the Council of Europe. The final part of
the chapter points out the aspects that complicate regulatory process; it emphasizes the lack of clear definitions and the peculiarities related to the perception of risk.

The second chapter provides insights to the ongoing debate on children’s online safety. The chapter is organized in the following structure. First, the chapter places the debate in the context of the goals provided in European Commission’s (EC) Communication on the Digital Agenda for Europe. Second, the chapter presents personal reflections on practical aspects and the discussion on the regulation of children’s online safety, which took place at the Digital Agenda Assembly, June 16-17, 2011. This chapter is unique because of the methodology applied; it is based on the empirical experience gathered by participating in the Digital Agenda Assembly. The firsthand experience provides the thesis with insights regarding the regulatory aspects of children’s online safety that otherwise would not be possible. In addition to author’s personal observations, the chapter, where relevant, includes Dr. V. Donoso’s opinion on the workshop. Although both opinions are subjective, Dr. Donoso opinion, which is distracted from the interview, is regarded as a valuable source of information as she was actively engaged in the debate. Currently, Dr. Donoso works as project Manager e-Safety at Child Focus (Belgian Safer Internet Centre) and is a network member of the EU Kids Online Network. At the time of the observatory interview she worked directly with stakeholders involved in the debate; this was among her duties while performing and coordinating the evaluation of the Safer Social Networking Principles in 2010-2012. Finally, one has to acknowledge a value of personal observations because they contribute to the better understanding of the state of the art.

The third chapter is of a decisive importance as it presents the core problems of the current regulatory approach towards the issue of children’s online safety. In particular, the chapter provides a normative analysis of the self-regulatory initiative on the Safer Social Networking Principles of the EU. In order to evaluate and analyze the initiative in the context of a good regulation, the test of good regulation, proposed by Baldwin and Cave, is applied. The decision to apply this particular test is based on the world wide scholarly recognition and expertise in the field of regulation of both authors[2, 3]. In addition to the normative analysis, the chapter briefly discusses the notion of good regulation.

The Annex provides an interview report on the interview with Dr. V. Donoso, which includes a summary, a questionnaire, and a full transcript of the interview. The interview was used as a source of information throughout the thesis.

---

1 Dr. V. Donoso at the time of the interview was working as a research coordinator appointed by the European Commission for the Safer Social Networking Principles for the EU.
Chapter I

The state of the art of the regulatory framework protecting children’s online safety in the EU

1. Chapter overview

The main challenge of this chapter is to present the state of the art of the regulatory framework protecting children’s online safety in the EU. The section proceeds in the following structure. First, it introduces the historical developments that led to the rapid growth of children’s engagement in the online world and the issues that it raised. Second, the empirical data, which is of a great interest to policymakers and other stakeholders, is presented. Third, the paper provides a brief introduction to the best regulatory practices safeguarding children online from the United Kingdom, Belgium, Norway and the Netherlands. All five provide regulatory approaches which can be regarded as examples to be followed by the other Member States (MS) of the EU. Then, the paper examines the regulatory actors that are involved while approaching this topic. Subsequently, the paper examines the regulatory framework concerning children’s safety, which is in a constantly developing. The policy documents on the EU level are introduced in a chronological order. Eventually, the chapter discusses the ways in which the issue of children’s safety online is addressed by two major regulatory players in the European region, namely the EU and the Council of Europe. The final part of the chapter focuses on the reasons that are claimed to impede the adoption of any binding measures ensuring children’s safety on the Internet.

2. Why is children’s engagement online problematic?

According to Robert Madelin, the current Director-General for the Information Society and Media of the EC, the Internet is the petrol of XXI century.² Indeed, it is; it ‘is becoming ubiquitous covering all the events of our everyday life’[4 p. 8] For this reason, children’s engagement into information and communications technology (ICT) is perceived as a given fact in the contemporary world. Statistics show that children constitute 20% out of the overall number of the Internet users, children constitute[5]. Most of the children and their parents warmly welcome the Internet to their homes and lives as a domain for development and entertainment. However, the problem arises because initially, the Internet was not designed for the children’s use. Its primary goal was to enable academic and governmental networks to share knowledge. The 90s destined the Internet to a somewhat different path; with a rapid growth of users, the Internet has evolved to a widely used and accessible network. As a direct consequence of this expansion in regular internet users and services

² The idea was expressed in the plenary speech given at the 1st Digital Agenda Assembly, June 17, 2011.
available online, children were becoming acquainted with new technologies at an early stage of their development since it was a part of their home environment[6 p. 4-8 , 7]. Furthermore, children have indisputable curiosity, which contributes to the fact that the average age of children getting involved in various online services has been decreasing ever since. According to the latest research, children are starting exploring cyberspace at the age of 6 or even younger[8 p.7].

This does not raise concerns for most of the society members as the Internet’s impact on the children is taken for granted. Generally, it is perceived as a positive phenomenon, which provides children with access to all human knowledge, and which is conceptualized as “the new home of Mind”[9 p. 3]. The Internet is deemed to be beneficial for children as it provides the endless space of knowledge. It offers to children a vast number of opportunities to develop and educate themselves by playing games, applying teaching resources, viewing broadcasts, TV programs, listening to music, etc. However, the Internet has the Janus face, meaning that opportunities are accompanied by potential risks, which subsequently, can harm a child. The level and kind of a potential risk differ throughout the developmental stages[10 p. 6-8]. By now, it is clear that technology affects the way youth’s mindsets operate. There is a reliable scientific evidence proving that ‘the actual dynamics of looking at a computer screen, with its multiple sensory inputs and its fast changing images impacts teens’ ability to think, making them more prone to taking risks’[11 p. 537 ]. In addition to this, the research proves that children born in the XXI century do not differentiate between a real life and the one online, which means that everything what happens in the online world is a part of a real life and vice versa, and thus, the generation called ‘born digital’ regard the Internet as an integral part of their environment[12 p. 1-16]. Given this, ignorance to the need for a regulation ensuring online safety of the ‘digital natives’ opposes a de facto hazardous situation.

3. Children’s engagement online in Europe: empirical data

As it is mentioned above, it is roughly estimated that children constitute one fifth of the overall Internet users. Following this in the EU context, children must constitute a significant 50 million as the overall number of regular internet users reaches 250 million[1]. Given a more precise statistics provided by the Internet World State there are 35930110, it might be claimed that almost 72 million of children are using the net[13]. In order to specify these estimations and learn more about children’s use of the Internet, the London School of Economics department of Media and Communication in cooperation with a research network, including representatives in other 24 European countries, conducted a study covering a random stratified sample of 25,142 children aged 9-16 who use the Internet. The study claims that 93% of those children are weekly Internet users and 60% of children are daily or almost daily Internet users[10 p. 5-6]. These conspicuous numbers do not surprise anyone, as XXI century children possess a lot of electronic devices via which they can access cyberspace, such as mobile phones (smart phones), personal computers, book readers (e-readers), play stations,
etc. Although this comparatively easy and diversified access to the Internet provides children with many development opportunities, a reference to a potential risk, which awaits a child while exploring cyberspace has to be considered as well. According to the aforementioned study, 12% of European children, within the taken sample, have experienced a negative impact of the Internet; they ‘have been bothered or upset by something on the internet’[10 p. 6]. The study also reveals that children’s capacity to recognize risks differentiates, and it increases with age[10 p. 6]. Another interesting finding, which refers to the impact of recent communications technologies, is that 21% of 11-16-year-olds within the sample have been exposed to various types of potentially harmful user-generated content, such as websites containing information about hate, pro-anorexia, self-harm, drug taking or suicide[10 pp. 5-6]. Moreover, this report emphasizes that children’s online engagement, risks and harm differentiates from one Member State to the other, and can be directly correlated with the ‘range of online activities’ that are available in a particular country[8 p. 33].

However, these findings of the EU Kids Online survey are not novel as they support findings of individual country studies, which also point out an obvious need for a coherent and thorough action, including all stakeholders, to tackle the problem of children’s online safety. Due to the limitations of this thesis only three examples will be discussed. The Belgian Center for Consumer Group Information, conducted a survey within a random sample of 2336 children in 2008, in which it was found out that 60 % of children on frequent basis communicate with ‘strangers’ and that adolescences are keen on sharing their personal data as well as engaging in ‘experimental’ relationships[8 p. 33]. Aligning the results of these findings, the recent independent research conducted in the UK shows that 48 % of adolescences (11-16-year-olds), within the random sample 1718, who had undergone instructions on the Internet safety, are still willing to communicate or get in contact with strangers[8 p. 31]. However, the most striking findings were published in the Polish report of 2006 summing up the results of two surveys. It appeared that 68% of children aged 12-17 were invited to meetings with Internet acquaintances, within the random sample of 1799, and that 80% of children from the random sample of 2559 have been confronted with information containing illegal content such as pornography, violence or racism [14 p. 23].

Obviously, with the rapid development of technology and change in various technological applications, the situation of children’s safety online is constantly changing. The scrutiny of surveys and studies differs and depends on both the sample, which was taken into consideration, and a country’s financial and human resources to fund such surveys. Therefore, one has to be caution while deducting any conclusions from any empirical findings and data related to children’s online safety.

4. The best practices for minimizing online risks in the European region

The importance of the best practices (interchangeably referred to as good practices) in a particular policy field increased remarkably with the introduction of Open Method of Coordination in the Lisbon Agenda, in 2000[15 pp.150-152]. Within a decade the method became a core element in developing European policy documents. Following this method, the
Member States of the EU are supposed to share their experience, regulatory approach or policy on a national level in the areas of common concern[16]. This method strives at enhancing efficacy and efficiency, and ‘achieving greater coherence towards the main EU goals’[15 p.151]. This method has been warmly greeted on the EU level as it does not require additional investment into research, and subsequently, it enables the MSs to set individual and common benchmarks, or even initiatives while comparing good practices.

Hence, following this explanation, the existing best practices should be considered in order to determine the European policy and approach towards the issue of children’s online safety. Given the development of coherent legal or policy frameworks four countries stand out as good examples to be followed, namely the United Kingdom (UK), Norway, Belgium, and the Netherlands. Three of them (the UK, Norway and the Netherlands) lead in minimizing the risk of children’s online engagement by establishing legal constrains. All four countries provide outstanding examples of research efforts and methods ensuring children’s online safety. While referring to the four countries as the best practices it must be noted that most of the regulatory frameworks are or used to be limited to harmful content. Thus, meaning that they remain ignorant to other considerable risks, such as stalking, cyber bullying, providing personal information to strangers or meeting them. This is due to a reason that only lately, some forms of harmful conduct by minors or adults have received legislator’s attention. The following paragraphs will briefly introduce country specific policy and regulatory approach to children’s online safety.

The UK has been a pioneer in this field. However, the role of its national government should not be overestimated; it was the private sector of the internet industry that initiated the establishment of the first European hotline centre in 1996.3 The center was titled the Internet Watch Foundation (IWF) and it has been successfully running for the last 15 years. Despite being a quasi-legal measure and not having any binding enforcement powers, it has gained respect of public actors, meaning law enforcement bodies and the government[17]. Given that in 2009 the IWF identified and shared information about 450 criminals selling and distributing visual information containing sexual abuse of children, its decisive role cannot be questioned. In order to achieve its aims, the IWF has developed a number of content monitoring systems (e.g. Cleanfeed), dealing with tracing images of child sexual abuse, criminal, obscene and racial hatred content containing data hosted in the UK and abroad[18 p. 2]. Interestingly, though self-regulation, which was the founding method of the organization, received a lot of criticism in the beginning, eventually it was deemed to be the core of the organization’s success. Self-regulation was a key, because it ensured involvement of stakeholders, namely industry and civic groups, and laid foundations for other private and public initiatives and projects, raising awareness of the online world, such as Childline or the Byron Review on children and technology funded by the National Children’s Bureau. In addition to this, the British government played an important role in fighting the problem; it actively supported the development of self-regulatory approach for solving the issue of children’s online safety, and it established several agencies to tackle the issue such as the

3 It should be noted other authors have a different position, e.g. David S. Wall in Cybercrime: The Transformation of Crime in the Information Age (Polity Press 2007) argues that the establishment of the IWF was based on the police initiative.
Child Exploitation and Online Protection Centre and the Serious Organized Crime Agency. Furthermore, the UK was the first European country to criminalize child grooming, which encapsulates a behavior of an adult seeking to establish a trust-based relationship with a child in order to sexually abuse a child in the online or offline environment [8, 19 p. 7]. In 2003, an act with an intention of committing a sexual offence with a child was made illegal by passing the statute of the Sexual Offences Act for England and Wales, and in 2005, this statute was reiterated in the Protection of Children and Prevention of Sexual Offences Act for Scotland[8 pp. 19-20].

Regarding the legislation protecting children online, Norway to a large extent has been following the UK’s approach; Norway criminalized grooming in 2007. The rationale behind criminalizing this activity under the provisions of Norwegian criminal law was to provide legal security for a child at the early stages of sexual exploitation[8 p. 21]. In addition to the substantive law provisions attempting to minimize online risks, the Norwegian legislator sought for ‘more’ and it developed a red-button policy, which enables children to report unwanted or abusive content while browsing the net to the hotline center. In a way this reporting method is similar to a system developed by the IWF, yet this button is found on the internet browser itself. The reporting system has been warmly greeted as a merit by stakeholders, especially parents and teachers. However, currently, this application receives a lot of criticism regarding its effectiveness and added value to children’s online safety. The rise for criticism was provided by the internal research of the Norwegian hotline center that revealed that only a modest amount of the reports submitted to the 24/7 hotline center, contain illegal materials or are of an illegal content. As the credibility of the red-button has faltered, Norway now focuses on awareness raising campaigns[20 pp. 11-17].

Another country that could be regarded as an example of good practices is Belgium. Although this country does not have specific substantive law provisions safeguarding children’s rights online, recently, it actively seeks for alternative ways to ensure children’s online safety. The Belgian government has funded the development of the Safer Internet Center called Child Focus, which developed the following initiatives, stopchildrenporno.be and click-safe[8 p. 34]. In 2011 under the initiative of the NGO Child Focus, the E-safety Charter was signed with six leading content and access providers[21]. This initiative consists of seven commitments. Following the most essential commitment of the leading players all internet service providers are obliged to ensure children security online[21]. Noteworthy, this document is a soft-law instrument, and thus, is not legally binding upon the parties. Nonetheless, it might become a powerful tool, as the provisions of this self-regulatory initiative have a wide scope; it includes techno-preventive measures, such as optimization of default-settings and easy to use privacy settings, and it aims at raising awareness, or enhancing collaboration among the market players and law enforcement agencies[21]. In addition to running a stakeholder’s platform, Child Focus also encourages voluntary individual contributions of people giving information sessions for pupils. Nevertheless, the most significant achievement of Belgium in the field of internet safety is the development of

---

4 This argument is based on the information observed during the Digital Agenda Assembly in a workshop on children’s online safety.

5 It is a Belgian Safer Internet Center; it is funded by the EC and Belgian government.
a scheme for electronic identity cards, known as Kids ID, for children under the age of 12[22]. The Kids ID is an authentication certificate and serves as a protection measure, which aims at protecting children in the online and offline worlds. The Kids ID can enhance children online safety as ‘a built-in PIN code enables to automatically authenticate the child and to grant him access to web services he is allowed to use’[22]. Furthermore, Belgium recognizes children’s online safety as a problem, which is in a constant developing mode, and therefore, it seeks to observe important and relevant aspects for shaping policy fighting the problem by means of empirical studies. The most recent study was conducted in 2008 by the Belgian Centre for Consumer Group Information. The study encountered a high level risk for information containing youth’s private data, which so far has not been tackled by any measures[8 p. 33]. Finally, it is possible to conclude, that although Belgium does not have legal measures fighting the problem of children’s online safety yet, it represents an example of a country playing a ‘constructive supporter’ which seeks to achieve the ultimate goal of internet safety by indirect measures.

The Netherlands is the last country to be discussed in this section, and as the aforementioned countries it also actively attempts to enhance security in the cyberspace. It has instituted a helpline center called “Netherlands Internet hotline Meldpunt” and it has criminalized grooming in the substantive law provisions in 2010[23 p. 14]. The country’s approach towards the Internet regulation used to align the British approach, given the fact that it used to support filtering Internet traffic for child pornography. Following examples of other countries (the UK and Norway) content filtering was introduced in the Netherlands in 2007[24 p. 251]. However, this practice by governmental bodies did not last long as Dutch law enforcement agencies were acting without any legal basis[24]. Despite that filtering was regarded as a breach of rights to information declared in the European Convention on Human Rights and Fundamental Freedoms, filtering activities have continued under the supervision of the Dutch hotline center. Finally, the Dutch government has gone one step ahead of the British one as it seeks not only to support self-regulation, but it aims at providing and creating incentives for private parties to take action and ensure online security. For example, recently the Dutch government inquired the Institute for Information Law to conduct a study into duties of care on the Internet of the Internet Service Providers (ISPs). The study was published in December 2010 and it proved that, indeed, the ISPs could greatly affect online safety and while doing so they would benefit all Internet users[25].

Obviously, the description of each country can be expanded and cover not only current state of the art but also include policy documents and public debate on the issue of children online safety. However, the aim of the section is to point out European countries which can be regarded as examples of good practices and which could be followed by others. While approaching the problem of children’s safety in the online environment every country has developed its own strategy, reflecting its own needs and coping with the problem in question. This situation is clear proof of equivalence functionalism stating that ‘different elements can respond to the same problem’[26 p.356]. Furthermore, the analysis shows that the scope of regulatory initiatives related to children’s online safety is limited and is mostly concerned with the illicit content. The recent trend in criminalizing grooming in national substantive law might be regarded as a direct consequence the ratification processes of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and
Sexual Abuse (Lanzarote Convention), which in Article 23 criminalizes grooming activities. Finally, the section points out the fragmentation of regulation and the existing variety of approaches to tackle the problem, the lack of coherent policy among the countries; this all makes it difficult to fight the problem of children’s online safety in an effective way.

5. Is it possible to apply the best practices originating outside the European borders?

The aforementioned four European countries are not the only countries which seek to ensure children’s online safety. The problem of children’s online safety is regarded as a common concern of developed countries, which have means to develop innovative solutions combining all regulatory efforts and including as many stakeholders as possible. The United States of America (USA), Canada, Australia and New Zealand have developed profound and elaborated frameworks dealing with children’s online security, and therefore, they could be considered as examples to draw one’s inspiration[8 p.5]. Due to the limitations of the thesis only the example of the USA will be briefly introduced.

The USA has started developing the regulatory framework securing children online with the rapid increase of the Internet users in the mid 90’s. In 1998 the Children's Online Privacy Protection Act and the Child Online Protection Act (COPPA) were enacted; the latter did not come into force as it was challenged under the First Amendment to the US Constitution declaring the freedom of speech. On the same basis the Communications Decency Act of 1996, which also included safety provisions, was struck down by the USA Supreme Court’s decision in Reno v. ACLU, in which Internet communications were awarded the same level of First Amendment protection the printed media sources[27]. Given the decisive importance of the civil right to free speech in the USA, regulating online content directly seemed to be impossible till 2010, when The Federal Trade Commission announced the extensive review of COPPA. This initiative was supported by the President’s administration, which published several reports urging to secure children and adult data online[28].

In the USA an obligation is set on the operator to disclose and secure personal information that is gathered about children[29]. ‘The operator’ means ‘any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce’[29]. Another remarkable finding is that the USA approach to the problem of children’s online safety opposes the European practice as the legal framework securing children online protects children till the age of 13. Only until 13 does a child fall under the vulnerable category as

---

6 For example, Canada’s government recognized that the growing access to the net service can endanger children safety and therefore it seeks to raise public awareness about the threats that await on the Internet, and thus, it supports establishment of agencies(http://www.cybertip.ca/app/en/about), non-profit seeking organizations(http://www.protectchildren.ca/app/en/whoweare) and various websites, such as http://www.wsd1.org/internetsafety/ or http://www.webawareness.org/english/index.cfm.
regards the information it provides online. Noteworthy, this age limitation does not match the civil maturity, which is recognized at the age of 21. Consequently, children from the age of 13 till civil maturity are left without legal protection which opposes the practice of the European approach.

Although the American (or other countries’) regulatory approach might appear tempting for the European legislatures to follow, they can only consider them as the source of inspiration. The European region has developed its own specific characteristics and values, and thus, it has to find regulatory solutions aligning those values.

6. The perception of responsibility for the Internet’s safety: development in the EU

As the risks arising from children engagement online and country specific individual regulatory approaches have been discussed at this point it is relevant to discuss the issue of Internet regulation on the European level, where it seems that the question and division of responsibility for the safety online has never been crystal clear.

Influential stakeholders have been trying to avoid this question and national legislators were incapable of regulating the borderless Internet. Furthermore, as the aforementioned examples of good practices identify, countries address the issue of the online safety in different manner. There is a trend among the European countries to fight the problem of online safety by means of filtering content and establishing hotline centers, which fight illicit materials online. Whereas the American approach sets an obligation for private parties to ensure appropriateness of their behavior and information which is put online. Despite huge differences among the countries, in most of them self-regulation concerning online safety is praised and is regarded as the optimal solution.

In order to understand the question of responsibility for safety online, one has to approach the matter in a chronological order. It appears that Internet safety primary was considered as state’s internal security issue, and thus, states sought for individual ways to secure the online environment. However, due to Internet’s specificity, meaning that its reach does not recognize any frontiers, attempts of individual countries were not sufficient to fight the problems occurring on the Internet[7 p. 3]. This ‘incapacity’ gave rise to the ideas of developing a coherent action plan or policy among countries[7 p.3].

The European Union as a regional cooperation between the MSs provided a platform for a common action concerning online safety. Despite the fact that in the mid 90’s the Internet was still an issue, which is “hard to define”,[7] the idea of fighting the Internet problems, meaning various forms of cybercrime, such as identity or information thefts, on the European level was born. The topic was included under the third pillar, constituting intergovernmental decision making process. Placing the issue under the pillar of Police and Judicial cooperation in Criminal Matters seemed to be an adequate solution as the MSs were reluctant to lose competence in the area of internal safety. Although a solution was adequate at that time, it was not the final one. The substantial changes were brought to this setting with the enforcement of the Lisbon Treaty. The institutional structure of three pillars merged, and the area of freedom, security and justice was put under the tag of shared competence,
meaning that the MSs maintain and exercise a right to legislate only to the extent it aligns and does not interfere with the EU ‘vision’[15 p. 155]. Furthermore, according to Articles 82(1) and 83(1) of the Lisbon Treaty (TFEU) it has became possible to adopt directives related to matters of this field and in this way harmonize the law of the MSs[30].

In the 90’s with somewhat miraculous pace of technological development and increasing number of issues falling under the regulatory scope, the European legislative and regulatory actors were no longer able to withstand new challenges that technology brought. The lack of legislature’s expertise encouraged questioning the legitimacy of their actions and gave an incentive to include private actors and stakeholders (meaning NGOs, various associations, and private companies) into legislation and decision-making process. A principle of a better involvement of stakeholders into the decision-making process eventually was embedded in the White Paper on Good Governance, which despite being a soft-law instrument had a great impact on the functioning of European governance[15 p.157]. In particular, this document emphasized the importance of consultation procedure at the early stages of policy initiatives development[31]. Following the ideas proposed in this document, the Inter-institutional Agreement on better law-making between the EU institutions, namely, the European Parliament, the Council of the European Union and the Commission, was signed. The significance of this document is not only that for the first time the EU institutions agreed upon greater coordination of their actions, but it also made an explicit reference to alternative methods of regulation, namely co-regulation and self-regulation. The use of two alternative methods aligns the principles of subsidiarity and proportionality, which are embedded in the EU legislative framework[30 TEU 5]; the EU institutions adopt legislation only when they have the competence to do so, or when it is the most efficient and effective to act on the EU level. Obviously, this regulatory approach affected the regulation of technology and the Internet as well; the EU is following the path of minimum harmonization and sets only the essential requirements, which protect public good. For example, the EU has politically agreed to adopt a directive on combating sexual abuse, sexual exploitation of children and child pornography, which covers criminal activities and fights criminal behavior[32], whereas the EU leaves up to the private parties to set requirements for quality or content of their services, and the MSs to adopt regulation setting higher level of legal protection[33]. Given, this situation it is possible to conclude, that at the moment the question of responsibility for the online safety is scattered. All parties involved in the Internet activities are responsible to some extent.

7. What is the most appropriate level for adopting regulation of children’s online safety in the European region?

Thus far the thesis described several regulatory approaches and addressed the question of responsibility for online safety. Therefore, at this point it is worth to consider, whether there is a most appropriate level for adopting regulation of children’s online safety in the European region.
The Internet does not recognize any frontiers and its regulation is a complex topic, and yet the Internet regulation becomes even more complex when one includes the issue of children’s online safety, which has already turned into the international debate including diverse stakeholders. Due to the limitations of this paper, only two main actors in the European region, namely the EU and the Council of Europe, will be considered. At first glance, the EU and the Council of Europe seem to head one direction and approach the issue of children’s online safety alike, although the two act without any coordination of their actions. For example, on the EU level the Council Framework Decisions on attacks against information systems and on combating the sexual exploitation of children and child pornography reiterate provisions embedded in the Council of Europe Convention on Cybercrime. The overall impact of this overlap is unknown, and thus, the following paragraphs will consider the appropriateness of each jurisdiction to fight the problem.

Lately, the EU takes an active stand as regards the rights of a child. It promotes the rights of children in the Charter of Fundamental Rights of the European Union (article 24) and an exhaustive list of policy documents (please see Chapter I, section 8 elaborating on the regulatory action). The protection of the rights of a child are among the objectives of the EU regarding Article 3 of the TEU, and that according to Article 6 of the TEU human rights, including children rights, constitute an integral part of the EU legal system. However, based on those provisions the Union cannot expand its competence reasoning the need to protect those rights. Noteworthy, with the enforcement of Lisbon Treaty in December 2009, some significant changes took place in the structure of European governance and the issue of lack of competence is no longer relevant. According to the TFEU Articles 82 and 83, the EU institutions by following ordinary legislative procedure can adopt minimum rules in the form of directives on crimes related to sexual exploitation of children and computer crimes. Empowered by this article, in the co-decision making process, which is renamed by the Lisbon Treaty to ordinary legislative procedure, the EC, the Council and the European Parliament adopted a directive on combating sexual abuse, sexual exploitation of children and child pornography by the end of 2011. This changed Framework Decision, which was adopted only by the Council[34]. The significant difference between two legal instruments lays in the supervision of its implementation. In the case of directive the implementation of Member States is controlled by the EC and its interpretation questions can be addressed by the European Court of Justice[15 p. 85]. Both of these options are not present in a case of framework decisions. Certainly, the directive has a limited scope as it has a focus on the definitions and sanctions related to the crimes of children’s sexual exploitation or abuse[35]. Realizing limited reach of the directive, the EU continuously promotes support for the action plans aiming at safer online environment of the Member States and private actors. This support is emphasized in the context of the Communication on A Digital Agenda for Europe, in which the EU calls for a safer Internet and then, leaves the realization of this goal at the discretion of the market players[1]. The EU contributes to the realization of this goal by providing a platform for discussion. Although the EU recognizes a particular need of safer internet, it is active, only when it comes to the challenge of minimal harmonization in criminal matters related to child’s safety online.

The Council of Europe has never been confronted with the problem of lack of competence in the field of children’s safety, starting with the European Convention on
Human Rights, children were an integral part of its framework. The Council of Europe contributes to the common European regulatory framework by creating a common ground for action in the form of international Conventions and recommendations related to the issues of online child safety. The most outstanding achievements are marked by the Council of Europe Convention on Cybercrime (2001), which came into force in 2004, and the Council of Europe Convention on the Protection of children Against Sexual Exploitation and Sexual Abuse (July 2007), which came into force in 2010; both Conventions have additional protocols. Once these Conventions are signed and ratified by the Member countries, they become integral part of a country’s legal system, unless certain reservations are made while negotiation processes. Alike most of the EU’s legislation, especially directives, the Council of Europe documents leave limited space for the deviation from the initial content of the provisions. The main advantage of the Conventions is a broader legal reach as countries which are not members of the Council of Europe can also sign Conventions and then incorporate them into their own legal systems[36]. Nonetheless, entry into force of the Conventions is not always smooth; the members of the Council of Europe are not obliged to sign and ratify Conventions and sometimes signing the treaty does not lead to its ratification[36].

Consequently, it appears that both actors, despite their substantial differences in the initial aim and scope, seek to establish a legal framework providing minimum harmonization which would protect children from various forms of harm and abusive behavior. In order to provide judgment stating which jurisdiction is more appropriate, further comparative reach, covering the impact of both legal orders to the national laws, has to be done.

8. Heading towards regulatory action enhancing online safety in the EU

This section describes the developments on the European level which consolidated together form a regulatory approach towards internet regulation and children’s online safety. As the qualitative research shows, the last decade has proved that the protection of children’s rights constitutes an important part of social and legal policy in Europe. Indeed, the EU has developed a comprehensive policy framework recognizing holistic and universally applicable children rights. Article 24 of the Charter of Fundamental Rights of the European Union was a green light, which fostered this development.

The Framework Decision on combating the sexual exploitation of children and child pornography of the European Council in 2003 was one of the first legal documents which focused on the protection of children as the most vulnerable group in society. Later, several policy documents followed. The EC in the Communication on Strategic Objectives 2005-2009 pointed out that ‘a particular priority must be effective protection of the rights of children, both against economic exploitation and all forms of abuse with the Union acting as a beacon to the rest of the world’[37]. The follow up of this policy document was presented in the EC Communication ‘Towards the EU Strategy on the Rights of a Child’ in 2006. This document aimed at establishing a ground for developing a long-term strategy for the EU on children’s rights[38]. The document emphasizes the cooperation in the form of a ‘systematic dialogue’ among the Member States, the European bodies and international organs addressing
children’s rights. Regarding the same Communication, the EU, being an important international actor, should challenge itself and ‘bring essential and fundamental added value in the field of children’s rights’ ‘building on its long tradition of legal and political commitments’ through the policy documents and laws, ensuring full enjoyment of children rights. Another Communication concerning children rights was adopted in 2008. In particular, this document on ‘A special Place for Children in the EU External Action’ prioritizes the rights of the child as it declares, that ‘investing in children and young people today means investing in the future’.

Encouraged by those documents, private actors have developed four self-regulatory initiatives, namely the EU Safer Mobile Framework and the national codes of practice in 27 EU Member States, the EU Safer Social Networking Principles, the Mobile Alliance Against Child Sexual Abuse Content, and TeachToday.eu. The EC in support of those initiatives presents annual reports based on the voluntary self-declaration reporting system. The promise to scrutinize self-regulatory initiatives is embedded in the Inter-Institutional agreement[39 paragraph 22]. The effectiveness of those initiatives is measured by compliance with the guidelines[e.g.40]. Interestingly, neither the overall impact of self-regulation, nor the most effective form of self-regulation protecting the rights of a child on the European level is addressed. However, some changes in practice might be expected as the EC called for the revision of the established self-regulatory initiative of Safer Social Networking Principles. These principles received a lot of criticism by the public because of the following reasons, firstly, the principles have been developed without any transparency, they were very generic, and the compliance of the principles has been based on self-declarations, which do not reflect the real effort of a company to meet requirements on which it had agreed.7

a. The primacy of self-regulation ensuring children’s online safety

The origins of the European approach to the Internet governance, and children’s online protection in the EU date back the mid 90’s. At that time the debate on the most appropriate form of the Internet regulation included diverse standing positions for and against Internet’s regulation, yet policy documents of that period do not reflect that debate. Nonetheless, it is widely acknowledged, that self-regulation was regarded as a compromised solution between all stakeholders involved in the debate and the European legislative actors.8 Following this compromise based solution, neither the EC’s Communication on Illegal and Harmful Content on the Internet published in 1996, nor the European Council’s Resolution on Illegal and Harmful Content, which was published in the following year, gives any ground to doubt that there is any better solution towards the problems and challenges that the Internet brings than self-regulation. Subsequently, this position was confirmed in the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services in 1998. These three policy documents provided a framework promoting self-regulation in the Internet matters, which has been maintained ever since. Only recently, with the rapid growth

7 The statement is based on the transcript of in the interview, which can be found in the Annex I.
8 Ibid footnote 7.
of minors involved in the online world, the public debate regarding the appropriateness of the current regulatory approach has started.

9. Troublesome aspects of children’s online safety regulation

The issue of children’s online safety is controversial, it fuels interesting public debates, and is difficult to address by regulatory tools. The debates on the issue are not productive ones as they lack objective perception of risks and clear definitions related to the subject matter. Both troublesome aspects will be addressed in the following paragraphs.

a. Risk and its perception

Risk and its perception play an important role in the debate on the internet regulation enhancing children’s online safety. Risk is a conventional denominator of situation that might have negative consequences or impact, which in other words could be referred to as a hazard. According to J. Black, most of contemporary policy documents and legislation are risk based[41 pp. 302-303]. The trend of risk based regulation developed in the 80’s and 90’s in the UK; and it was followed by other European countries. Risk based regulation became a common practice as it was regarded a beneficial tool by governments; once risk was encountered in a particular field, the government could use findings as justification or evidence for the necessity of regulation[41].

Subsequently, the risk based regulation was picked up by the EU. The importance of risk and evidence based regulation was emphasized in the White Paper on Good Governance and eventually it was embedded under the notion of impact assessment, developed in 2006. Impact assessment is a part of a legislative procedure, in particular, proposal in ‘major policy initiatives and legislative proposals on the Commission's’[42]. In short ‘it identifies and assesses the problem at stake and the objectives pursued. It helps to identify the main options for achieving the objectives and analyses their likely impacts in the economic, environmental and social fields’[42]. In the context of impact assessment, risk is used as an organizational tool or justification[41 p. 303]. The identification of risk provides various implications, however it remains unknown how much risk is enough for a subject matter to be legible for regulatory action, and how much risk is acceptable.

On the other hand, the importance of risk is predetermined by its perception in society[41 p. 313]. People consider an activity [...] to pose a lower risk if they are familiar with it, have some degree of control over it, the consequences are not ‘dreaded’ or catastrophic, the impact is widely distributed, they are not significantly aware of the adverse event occurring, they have exposed to themselves to the risk voluntarily, and they think benefits will derive from it to themselves[41 p. 313]. Thus, in the case of children’s online safety, the identification of various risks that children are exposed to online does not play the decisive role, whereas the perception of this risk by society members is crucial. The attention of the society at large is brought by cases of young victims which receive a lot of media attention[23], such as a case of Megan Meier. Thus, society members, while following their duty to protect the most vulnerable, might overestimate or underestimate the importance of

9 Ibid footnote 7.
risks in this particular field. Given this possibility, regulation based on the precautionary principle might be a proper solution, avoiding the trap of one sided risk evaluation[23]. Finally, it is important to note the following three points, which should be considered while adopting any legal or policy measures. First, there is no one online risk per se as the online risk covers three categories of a wide scope namely, content, contact, and conduct; second, the intensity of online risk differs according to the age of a child; and third, with the rapid development and convergence of technologies new forms of risk occur[23].

b. Definition of children’s online safety

The other peculiarity, which makes regulation of children’s online safety difficult, is the lack of clear definitions related to the topic. While analyzing information on the public debate regarding children’s online safety on the European level, it appears that this debate operates without any established concept of children’s online safety or even child safety. As there is no formal agreement elaborating on what online safety means, ambiguities in the discussion are inherent. This situation can be explained by the following points. Firstly, the issue of children’s online safety to a large extent was addressed only in the context of criminal law, where children under the statutory provisions are regarded as a vulnerable category and in most cases they are captured by the notion of minors. Mostly legislation concerning child pornography covers children under the age of 18[43 p. 15]. Secondly, the concept of a child, age of consent for sexual activities, as well as the level of children’s protection differs among the Member States. For example, in Spain a thirteen year old child is legally entitled to decide for its own actions related to sexual engagements, whereas in Belgium, Netherlands, Finland, Latvia, and the UK the age requirement for the same decision is 16[43 p. 15]. The highest age requirements to give consent for sexual activities is 18, and it set in Greece and Malta[43]. Lastly, the definitions of children safety and children online safety are commonly referred to as welfare of child, and thus, left at the discretion of the MS.

10. Conclusion

Concluding this chapter, several findings can be drawn. First, it appears that there is a number of studies identifying risk related to children’s engagement online on both national and the EU level. Second, several countries can be identified as examples of good practices while addressing the issue of children online safety, yet at the same time it should be noted that their actions are not coordinated. Third, the EU and the Council of Europe are two dominant actors, which actively contribute to the development of legal framework securing children while engaging in various activities in the online environment. Forth, the decision to evoke self-regulation as a regulatory tool seems to be a balanced solution, presenting a consensus between private and public parties. Finally, the chapter identifies that because of

---

10 The statement is based on the transcript of in the interview, which can be found in the Annex I.
11 This statement has been determined by the literature search findings, which show that initially the public prosecutors were facing a problem of sentencing persons who conducted misdemeanors towards a child.
the lack of well established definitions and not adequate risk perception the regulation of children’s online safety so far is a troublesome task.
Chapter II

Insights to the debate on children’s online safety

1. Chapter overview

This chapter aims at providing the relevant insights to the debate concerning children’s online safety. This is done by incorporating two different information sources, namely an expert opinion and direct observations of debates which took place in two workshops of the Assembly on the Digital Agenda for Europe. Direct observation and expert opinion have been used as qualitative research methods to gather data, which allowed capturing differences between knowledge available for the public and actual practices in the field. It is foreseen that because of interpretation techniques the chapter inescapably includes both objective and subjective information[44 p. 34]. The chapter takes a funnel approach and is organized in the following order. The first part of the chapter introduces the ultimate goals set for the EU by the Communication on Digital Agenda, and then, it continues with reflections on Action 37, which specifically addresses the issues of self-regulation enhancing children’s online safety. The second part of the chapter provides a description of the Digital Agenda Assembly and sums up the debates of two workshops, namely a workshop on cyberspace security and children’s online safety.

2. The Communication on the Digital Agenda: the way forwards

The EC’s Communication on the Digital Agenda (CDA) is the latest attempt to contribute to the framework concerning the Internet’s governance. This document is one of the seven ‘flagship initiatives’ set in the 2020 Strategy provided by the EC. In essence, this document supports Prof. L. Lessig’s opinion that although ‘perfect control of the internet is not possible, [this] does not mean that effective control is not possible’[9 p. 73]. The following paragraph will present the general goals of the Agenda, which subsequently will be continued with its specific relation to children’s online safety.

The EC, specifically referring to the Director General for Information Society and Media, by means of the CDA as a policy document aims to achieve several interrelated goals. One could say that this is determined by the fact that this document has two main objectives - ‘to maximize the social and economic potential of ITC’[1 p. 3]. In order to achieve those goals the document invites to fight the following problems - fragmented digital markets, lack of interoperability, lack of investment networks, insufficient research and innovation efforts, lack of digital literacy, rising cybercrime and risk of low trust networks. The problems are tackled by planned actions. Although every action plan tackles a very specific issue, for example, Action 9, which has been established so the ecommerce Directive is updated or Action 46, which aims at encouraging the Member States to develop national broadband
plans, the overall goal of all those actions is to lay down a proper ground for a flourishing digital single market.

Currently, 101 actions of the Agenda are grouped into 7 pillars, which have international dimension, namely the Digital Single Market, Interoperability and Standards, Trust and Security, Very Fast Internet, Research and Innovation, Enhancing e-skills, and ICT for Social Challenges. The following section will elaborate on Trust and Security pillar, and specifically it will analyze Action 37.

a. The Core of Action 37

Action 37 is a part of Trust and Security pillar, which has an ultimate goal to increase the extent to which the Europeans will engage into the online activities. In order to achieve the overall objective of the pillar, it is divided into 14 actions. Action 37 has a slogan ‘Foster self-regulation in the use of online services’ and is of a crucial importance while discussing issues related to children’s online safety. It aims at promoting a platform of stakeholders discussing options of self-regulation for European and global service providers, ensuring minors safety.

Interestingly, although on the EC’s website it is declared that Action 37 addresses the safety of minors in general, the following discussion considers only children’s online safety. Noteworthy, this is the only action, which approaches the issue of children safety. At a glance, Action 37 reveals the EC’s position regarding the issue of children’s safety online. The regulation of the issue is left for an ‘invisible hand of the market’, meaning that private and public parties, being stakeholders, should take care of the problem in question. At this point, one could claim inappropriateness of such approach because of the different weight that public and private parties have. Although both groups are regarded and treated as equally important, this assumption is wrong from its very beginning as public or civic groups have less financial and human capital to contribute to the debate and decision-making process. Therefore, the current situation regarding children’s online safety is somewhat awkward: the EC in its Communication on the Digital Agenda calls for a prompt action regarding trust and security of online activities, enhancing online child safety and invites the private actors to resolve the issue without interference of obligatory regulation.

b. Politicians shape the regulatory approach towards children’s online safety

Despite the fact that children’s online safety is addressed only in one action, the attention to the problem is drawn by politicians’ speeches, which subsequently can influence and shape policy actions. The latest speech, given by N. Kroes, who is the European Commission Vice President responsible for the Digital Agenda, depicted the not only the ‘state of play’, but also is expected to influence the future of regulatory developments. This speech of N. Kroes is important because it emphasizes the need to have a sensible approach towards cyber security, which would go beyond the criminal matters and include the voice of stakeholders. A substantial part of her speech on the Digital Agenda Assembly was devoted
to the need of enhancing trust of online activities and the protection of children, the most vulnerable and affected group of the Internet users. In particular, the Vice President said that the potential which the Internet brings ‘can only be unlocked if we overcome the barriers to trust’[47].

3. Reflections on the workshops of the Digital Agenda Assembly

a. The Digital Agenda Assembly

In 2011 the EC for the first time organized a meeting, in a form of two-day conference, titled ‘The Digital Agenda Assembly’. The event aimed at providing a platform for of all stakeholders to meet and hold debates regarding the Internet’s governance. The event attracted 1600 participants, who presented different occupations, undertakings and countries. Noteworthy, the EC did not seek to reach this outstanding number of participants. This number has been chosen as the optimal number of participants given the limitation of the space; almost one thousand of registered people were not provided an opportunity to participate in the event. The aforementioned numbers prove that there is a vigorous interest in the field for many. Obviously, people are driven by different interests, and thus purposes, due to many topics that fall under the scope of the Digital Agenda. This event ‘paid-off’ as it was a benchmark measuring the present achievements and indicating the goals of the future[47].

It has been a rewarding experience for the author of this thesis to participate in the Assembly. The author attended the workshops in the Trust and Security pillar- on cyber security and children’s online safety, which to a large extent attracted different audiences, however, the debates and questions that were addressed greatly related to each other in both seminars.

b. Observations of the workshop on cyberspace security

Noticeably, the workshop on the cyberspace security was more generic as it involved all the aspects of both the Internet (technical side) and cyberspace (virtual space), such as the Internet transactions or purchases and various entertainment related activities. The workshop included three presentations by guest speakers reflecting the state of the art in public and private sectors addressing issues related to cyber security. Due to elaborate presentations of the speakers the debate was limited in time and lacked profound solutions. The discussion between audience, panel and profile speakers addressed the following questions:

- What is cyber security about? Is it a technical, market or even political problem?
- What do we want to secure? What are legal and technical tools that could ensure security?
- How to ‘fight’ lack of awareness or digital illiteracy?
• How to keep the Internet open, while ensuring its security? What defines the word ‘open’?
• What groups should be targeted in order to ensure or enhance cyber security? Who has a duty of care? It is hosting providers, service providers, governments or software developers who should be held responsible?
• What position should the EU take in the debate of Internet governance?

Interestingly as it appeared, the scholars and practitioners who took part in the debate are concerned about the same issues; they have been raising the same or closely related questions. However, this common agreement on the issues of a major concern does not bring the debate any further because reliable scientific information, and thus answers, is still missing. The debate was closed with the following two outcomes. First, the workshop recognized the advantages of public private partnerships which can be brought in the area of cyber security, and thus, emphasized the need to develop such partnerships by national governments and the EU [48]. Second, the debate concluded that the EU, while being one of the most important players in global cyber security, should make a clear stand in the debate on the Internet governance[48].

c. Observations of the workshop on children’s online safety

The workshop on children’s online safety seemed to be more thought off. In advance the participants of this workshop received the relevant information, including a draft of the Principles for the safer use of connected devices and on-line services by children. Therefore, the majority of participants were ready to discuss critical points of the proposal in 8 working groups, which were composed ad hoc. All groups led by a group leader ‘coordinator’ spent one hour on brainstorming and discussing points of improvement on the proposal. As a direct result of the discussions, groups prepared enlightening presentations, providing valuable input for the private parties, which work on the improvement of the Safer Social Networking principles.

In general, the debate of the workshop concerning children’s online safety considered more focused, yet open-ended, issues in comparison with the debate on the cyber security. In particular, the participants asked:
• What should be added to the existing self-regulatory framework aiming to secure children’s well-being in order to enhance the trust of the Internet?
• To what extent is it possible to safeguard children’s engagement in online activities?
• What is the exact role of the stakeholders, namely public and education sector, business sector, and parents?
• Who should be responsible for monitoring the implementation of self-regulatory initiatives?
• Who should be involved in establishing self-regulatory measure (service or technology providers)?

12 According to the data presented during the Digital Agenda Assembly.
• How could self-regulatory initiatives be more inclusive?

Despite the positive atmosphere of the meeting, the working method of the EC was highly criticized. According to Dr. V. Donoso, the organization of this workshop, should not impart the EC to declare that it provides a platform for a dialogue of all stakeholders.13 Very alike remarks were expressed by several representatives of the private sector. The EC invites the most important stakeholders for meetings, which are unconstructive as parties feel intimidated to present ones views and have no time to engage in thorough discussions.14

The workshop provided a surprise to many, when after a coffee break of 30 minutes, the industry representatives grouped together proclaimed the establishment of a European Online Child and Youth Safety Forum on their own initiative. This forum was developed in order to ensure that industry, while preparing the final version of Principles for the safer use of connected devices and on-line services by children, will take ‘into consideration different legal frameworks and attitudes and pursue sustainable child safety protection policies’[49]. No further information as regards to the participation in this forum was provided.

4. Concluding remarks

The methods of direct observation and a semi-structured interview provide exclusive insights to the debate on children’s online safety, which would not be possible otherwise, and which lead to the following findings. First, it appears that the issues of Internet safety and trust in online services inherently relate to the issue of children’s online safety. This connection is also emphasized in the EC’s Communication on the Digital Agenda for Europe [1 p. 5]. Second, the main concerns in the field of the online safety are identified and well known to scholars, private parties and policy makers; they address the same issues. Third, this mostly descriptive chapter leads to the conclusion that the problem of children’s online safety is still a novel problem, which on the European level raises open-ended questions and is dealt by means of policy documents proclaiming actions. Finally, the EC has a limited influence over the debate on Internet governance as it acts only as a medium actor, which experiments and provides a platform for discussions and incentives to adopt self-regulatory measures enhancing the Internet safety for the benefit of all users, and especially children.

13 The statement is based on the transcript of in the interview, which can be found in the Annex I.
Chapter III

The Normative Analysis of the Safer Social Networking Principles for the EU

1. Chapter overview

This chapter critically examines the self-regulatory initiative titled ‘Safer Social Networking Principles for the European Union’ (Principles) in the context of good regulation. The chapter focuses on this particular self-regulatory initiative in order to enrich understanding of the current approach to Internet governance on the EU level. The chapter applies a good regulation test proposed by proposed by Baldwin and Cave in order to identify advantageous and disadvantages that self-regulatory initiatives face while tackling the issue of children’s online safety.

The chapter proceeds in the following order. The first section of the chapter introduces the reader to the notion of good regulation, which is considered to be one of the most important features for European regulatory instruments. The following part presents the content and rationale behind the development of the Principles. The subsequent part addresses five key questions of a good regulation proposed by Baldwin and Cave. The test aims at providing a balanced evaluation of the Principles, and thus covers both advantages and disadvantages of the self-regulatory initiative. The final part of the chapter summarizes the main findings of the analysis.

2. Diverse perception of the notion ‘good regulation’

Regulation is an indispensable feature of contemporary society. Legal, social, moral, and so-called architectural constrains shape and regulate people’s behavior[9]. Legal constraints, which are imposed by a legislative branch, are the most visible form of regulation, and thus, they are evaluated by lawyers, academics, experts and laypeople. Obviously, people representing different fields have different preferences for regulation; therefore, the same law or regulation might be perceived and evaluated differently by a lawyer and a finance person. From purely economic point of view, good regulation is considered to be regulation, which is efficient and maximizes overall wealth[50 p. 76]. However, social scientists tend to emphasize the element of public interest while explaining the notion of good regulation. For example, according to S. B. Thomadaki ‘good regulation serves the public interest through supporting ongoing confidence in processes, such as the market process, in which the public participates and in activities, such as auditing, on which the public relies’. Despite different opinions what constitutes good regulation among the scholars, several common principles can be established. On the EU level these principles are embedded in the White Paper on European Governance (2001).

The White Paper on European Governance signified the change in the European regulatory strategy as it introduced five key principles of good governance:
1. Openness - refers to the transparency and enhanced public awareness of actions related to adoption of policy actions or regulations.

2. Participation - emphasizes the importance of consultation procedure in which representative sample of stakeholders is involved.

3. Accountability - this is essential feature of the regulation, it requires European institutions to clarify their roles in the relation to regulatory measures.

4. Effectiveness - requires achieving policy goal to its full extent on time.

5. Coherence - is analogy with a principle of reasonable expectations, according to which the development of a policy line should follow a systematic approach[31 p. 10].

Each principle is important and while evaluating a regulatory measure cannot be applied separately from the other. In general, the application of those principles aligns the governing principles of the EU, namely subsidiarity and proportionality. However, these five principles are not the only one method to analyze regulation. A good regulation test, which is applied in this chapter, very closely relates these principles. The preference is given to the test of good regulation, proposed by Baldwin and Cave, instead of good governance principles because the test is formulated in questions presenting clear benchmarks.

3. Introduction to the Safer Social Networking Principles

Generally, it is referred to the Principles on Safer Social Networking as a self-regulatory initiative, which has been developed by social networking services. Twenty actors with a dominant position on national or regional markets, including such names as Google, MySpace, Hyves and Facebook, committed to the safer future of the Internet as they signed the Principles. Usually it is also emphasized that while drafting this initiative social networking services consulted the European Commission “as part of its Safer Internet Plus Programme, and a number of NGOs, to provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services”[51], meaning that the regulatory initiative by the private actors, such multinational giants as Facebook or YouTube, included not only a position of prevailing actors, but also, a representative variety of stakeholders. Apart from this brief reference to the drafting stage in the introduction part of the document presenting the Principles, no additional information, containing the formation of the provisions, is available neither on the website of the European Commission’s Director General on Information Society and Media, nor in any other media source. Despite the lack of transparency the European Commission (EC) supported this initiative and committed to present an annual report analyzing the compliance of these Principles. The initiative was adopted in 2009, thus, the annual reports of 2010 and 2011 are available online.

However, the lack of transparency in the drafting processes have not been forgotten, it has given a raise for a harsh criticism by many regarding the EC and private actors, which
signed under the initiative. This resulted in public pressure, and thus the idea of reviewing these principles was developed. However, contracting parties instead of revising the Principles for Safer Social Networking introduced principles setting good practice ICT principles titled ‘Principles for the safer use of connected devices and on-line services by children and young people’.

In order follow the normative analysis of the Principles, their content is presented by introducing each of the principle in the following order:

1. Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and care takers in a prominent, clear and age-appropriate manner.
2. Work towards ensuring that services are age-appropriate for the intended audience.
3. Empower users through tools and technology.
4. Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service.
5. Respond to notify cautions of illegal content or conduct.
6. Enable and encourage users to employ a safe approach to personal information and privacy.
7. Assess the means for reviewing illegal or prohibited content/conduct.

As the formulation of these Principles reveals that they are not legal principles as they do not have any legal implication. They are more like guidelines, pointing the direction in which companies should develop their online applications.

4. The rationale behind the development of the Principles

In order to understand the rationale behind the development of the Principles, two following aspects have to be considered. Firstly, the existing empirical data (for the exact details please see the Chapter I, section 3 on the empirical data) proves the presence of a problem and in this way empirical findings serve as a spark for public debates, which subsequently put both the legislator and various internet service providers under the pressure to act. Secondly, aligning a vast amount of empirical data pointing out the potential risks, one can find another reason explaining the development of the Principles. The second reason can be found in the wording of the background information on the Principles. In particular it says that “a common goal [of the Principles is] to maximize the benefits of the internet while managing the potential risks to children and young people” and while doing so companies have to develop safety strategies [51]. Given the focus on economic gains, it is possible to state that this sound statement of an extremely broad scope represents an economic approach. Despite clear economic incentives, one has to question the extent to which this statement is steering towards the identified goal. Indeed, what does it mean ‘to maximize’, what do ‘the benefits’ include, what are those ‘potential risks that children and young people’ are exposed to while being online, what falls under the notion of children and young people, and finally,
what does constitute a safety strategy? After all, does this goal present a real reason why social network providers in corporation with the European Commission have developed the aforementioned Principles or this is just an attempt to avoid legal measures imposing fines?

Unfortunately, there are no precise answers to any of the questions above, as well as there are no established concepts of children’s safety or children’s online safety. The absence of answers and the lack of clear concepts clearly impede public debate from thoughtful outcomes. Nonetheless, the situation should not be portrayed only in the dark colors; the adoption of this self-regulatory initiative implies that the private sector recognizes the threats that the Internet poses for the youth and that they are willing to act accordingly and minimize the level of potential risk.

5. Can the Principles on the Safer Social Networking be regarded as a good regulation?

This part of the chapter will examine the Safer Social Networking Principles while applying the test of good regulation, which is proposed by Baldwin and Cave in their book “Understanding Regulation: Theory, Strategy, and Practice”. Although it was pointed out that these Principles have been highly criticized because of the lack of transparency in the drafting stage, this will not be considered as the most important benchmark while evaluating the Principles. The section will proceed with five key questions[50 p. 77] and will provide the observations to the following questions:

1. Is the action or regime supported by legislative authority?
2. Is there an appropriate scheme of accountability?
3. Are procedures fair, accessible, and open?
4. Is the regulator with sufficient expertise?
5. Is the action or regime efficient?[50]

Question no. 1

At first glance, it seems relatively easy to answer the first question as no self-regulation is introduced following a democratic process. Yet the Principles can be considered as co-regulation. Indeed, it has been already mentioned that the self-regulatory initiative on the Safer Social Networking Principles received support from the EC in the development process; the EC provide stakeholders with a platform for meetings. In addition to this, the EC contributes to monitoring of the Principles as it publishes annual reports on the compliance and implementation of the initiative.

However, the declaration of support, following the commitments expressed in the Inter-institutional Agreement on Better Law-making, does not contribute to the legislative mandate. The EC’s in support of the initiative has committed to present annual reports, yet this cannot be considered as a partial transfer of legislative authority that it posses on the
European level. The partiality of the EC’s legislative competence is implied by the EU institutional setting. The EC’s legislative authority differently from any state’s Parliament, does not have a legislative power to enact any legislation, meaning directives or regulations, independently. Following the provision regarding the ordinary legislative procedure, which before the enforcement of the Lisbon Treaty used to be called a co-decision procedure, the EC “may alter its proposal at any time during the procedures leading to the adoption of a Union act”[30 TFEU 293]. The Council and the European Parliament have to support the proposal in order to create a legal measure. Following this line of reasoning, it is obvious that this self-regulatory initiative is lacking so called ‘legislative mandate’ to act in the name of the public interest.

Yet on the other hand, this self-regulatory initiative has a different legislative mandate. The initiative is developed by stakeholders playing a key role within the field of ICT, and thus, it not only reflects the state of the art as regards technology but also increases the compliance of the commonly agreed standards[52 p. 124].

**Question no. 2**

The second question of good regulation test concerns issues related to accountability. In case of the Principles, touching upon the accountability equals opening of a Pandora’s Box, meaning that according to the present monitoring system no one is held responsible for the implementation of the self-regulatory initiative. The EC monitors this initiative by presenting annual reports, which are based on the voluntary and self-declaratory reporting systems. Following requirements of the reporting system, experts of a particular contracting party are assigned a task to fill the form, which is attached as the annex to the Principles.

The EC presents evaluation of the overall compliance based on these self-declaratory reports, usually prepared by (internal) experts, and reports on additional testing system, developed by assigned researchers[40 p. 11]. The testing system includes two or one attempt ‘to act’ on a particular application (social network) in a socially harmful way, which is expected to cause adequate reaction of the ISP.16

No measures are imposed to the ones who do not comply with the guidelines, even more, the contracting parties do not care for each other, meaning that they do not interfere in the internal policies aiming at implementation of the Principles.17 This all raises a question, whether this self-regulatory initiative is a form of agreement or it is a part of soft law not having an explicit legal effect. In a case of a self-regulation, it could be regarded as a multilateral agreement, which is *pacta sunt servanda* for the contracting parties, and therefore, the provisions of such agreement should be implemented duly. Furthermore, every party should have a possibility to bring action against a party which does not implement agreement duly in order to foster the impact of the agreement. Yet this is not the case with the Principles, as the initiative is regarded as a soft-law instrument, with which compliance is not compulsory.

---

16 The statement is based on the transcript of in the interview, which can be found in the Annex I.
17 The statement is based on the transcript of in the interview, which can be found in the Annex I.
It can be suggested that the principle of accountability, which is also mentioned in the White Paper on Good Governance, and proper implementation of the initiative cannot be ensured without an agent explaining the vague wording of the provisions and imposing measures for a not satisfactory compliance. Interestingly enough, the questions of accountability scheme and implementation have never been raised; the stakeholders meeting at the Digital Agenda Assembly for the first time addressed the issue publicly. Moreover, the reports presenting the compliance of self-regulatory initiative in 2009 and 2010, the EC neither addresses the issues related to the overall impact of self-regulation, nor questions the measures that should be taken in the cases of non-compliance. Besides, if one considers a broader perspective of this regulatory initiative, it appears that the regulation theorists in the case of the ‘authoritative’ intervention into the regulation drafting stage (referring to the fact that the EC provides a platform for discussions) and oversight, the term of co-regulation is used instead of self-regulation[50 p. 133]. Whatever the name is attached to this initiative, the issue of accountability remains the core element of it, as of any good regulation, which assures transparency of the regulatory process. Therefore, both, the contracting parties and the EC should put effort to change the current situation.

Question no. 3

The subsequent element to be discussed is a due process. According to Baldwin and Cave, the due process captures the principles of fairness, accessibility, and openness of the procedures[50 p. 79]. Without proposing a proper criterion for measuring each of the elements, authors proclaim these factors having a legitimizing effect for a regulatory measure[50 p. 79]. Yet in a given context of the self-regulatory initiative, it is crystal clear that the aforementioned elements have a lot of space for improvement.

For example, considering the principles of fairness and accessibility, it seems that a list of the contracting parties, which includes 21 actors having a dominant position in the national or regional market, indicates a failure, as actors with a smaller economic power are left aside. Yet this situation should not be regarded only in a negative way because the presence of a more inclusive list is possible. All network service providers are invited to join the initiative. However, a general rule is that the stand of actors having a dominant position within a region can shape the behavior of less significant market players (small or medium size enterprises) in e-commerce environments.

Then, one should consider the principle of openness in the relation to the due process. Obviously, in order for the element of openness to foster, the minutes, or at least the main points, of negotiations or meetings regarding the implementation of the regulatory initiative between and among the contracting parties should be available for the public. Yet this information is not available. In addition to this, the openness of the procedures and actions of the contracting parties relating to the initiative might be a solution, which could enhance trust in the social networking services, and thus, the Internet.

18 The statement is deducted from personal observations.
These observations lead to the conclusion that contracting parties should reconsider three elements of the due process as this might provide that missing link ensuring the adequate functioning of the initiative.

**Question no. 4**

The question four of good regulation test addresses the topic of regulator’s expertise to act. It is valid to ask, do the private actors have sufficient expertise to initiate a self-regulatory initiative? The straightforward answer to this question cannot be provided because it depends on several factors. First of all, the level of expertise depends on various internal and external factors of a company. Internal factors refer to the existing human capacity, which possess required skills or knowledge on a topic in question, whereas external factors refer to the public pressure calling for transparency of the representative’s actions. Therefore, although expertise is considered to be one of the main advantages of the self-regulation[52 p. 123], the level of expertise it may vary given the individual approach of an entity. Certainly, a person working ‘inside’ a company might posses more knowledge about the issues that company is involved.19 But at the same time, it becomes hard to measure, if one works in the public interest.20 Finally, the two must be distinguished; the expertise of the company’s policy or activities does not imply the knowledge of the potential risks that youth might face while engaging in online activities.

**Question no. 5**

The last question to be addressed in this “five key question test” explores, whether the regulatory action that has been taken is efficient. Obviously, measuring and evaluating efficiency is difficult because ‘it is not a value independent of distributional considerations’[50 p. 81]. However, the evaluation can become a more bearable task, if it is based on one of the two distinct claims. The first claim implies that the level on which the regulation was created is the most appropriate one, and thus, a regulator had a mandate to act[50 p. 81]. This claim refers to the first question, and as discussed above, the legislative mandate to act for the private actors on the behalf of the public interest in this specific setting is hard, yet possible, to find. The second claim refers to the efficient results of the taken action and is blind towards the answers relating the expertise; it has a practical approach and is interested only in the final effect of the taken action[50 p. 81- 82]. After the second claim is placed into the context of the self-regulatory initiative in question, it appears that taken action has influenced and shaped the Internet applications of social networking services. For example, Facebook introduced the possibility to delete unwanted comments and to report bullying cases.

---

19 The statement is based on the transcript of in the interview, which can be found in the Annex I.
20 The statement is based on the transcript of in the interview, which can be found in the Annex I.
Concluding remarks of the good regulation test

To conclude this normative analysis, it is possible to say that answering a five key question test is a mind stimulating activity, which requires considering a broad picture of the situation, which includes perspectives of private as well as the public actors. Presenting a balanced evaluation of the Principles is a challenging task as it appears to be relatively easy to criticize a self-regulatory initiative while comparing it to the common requirements for legislation enacted via democratic process. Positive features of self-regulation, such as ‘efficiency, flexibility, an incentive for compliance, and reduced costs for government’, should not be outweighed by features and criterions applicable to legislation developed by elected representatives. Furthermore, a test of good regulation seem to blind to the following aspects. First, self-regulation is lobbying free, and thus presents more balanced positions of stakeholders[52]. Second, self-regulatory initiatives can be regarded as better regulatory measures for the internet environment as ‘rules usually evolve gradually’ and are easier to update with technological developments[52]. Finally, the observations, provided above, reflect an individual position, an educated guess, and thus, they are not value free. A further in-depth research is required in order to confirm or deny the claims about lack of accountability, openness, expertise, efficiency and proper monitoring systems. The following section will discuss peculiarities of the Principles, which have not been addressed by the test.

6. Other peculiarities of the Principles

Apart from the points discussed in a relation to the test, several other peculiarities draw one’s attention while analyzing the Principles. In particular, the issue of the language of the self-regulatory initiative and reports evaluating its compliance should be considered. The importance of language is well recognized in legal matters; there is no doubt that a proper use of language helps to articulate chosen aspects of rules as well as it helps to understand the law or regulation[53 p. 136]. In the context of the Principles, the language should play an important role because in order for the provisions of the agreement to be understood and implemented by contracting parties, they have to be interpreted and understood correctly. However, the question is, whether it is possible to do so, as the Principles are embodied in a vague wording and serve like guidelines rather than rules or laws, which supposed to be followed duly. For example, the principle no. 3 entails the contracting parties to ‘empower users through tools and technology’[51 p. 7], yet no specification is provided.

The langue of the self-regulatory initiative, as well as of the annual reports, is an informal business language, which puts in question the reliability of this initiative and its capacity to minimize the potential risks of online activities for children. Moreover, given that there is no independent agent responsible for monitoring of the initiative as well as its coherent interpretation, the indiscrepancy might exist in the measures taken by various entities.²¹ Certainly, this is caused by the monitoring system attached to the initiative; no one

²¹ The statement is based on the transcript of in the interview, which can be found in the Annex I.
can receive a legal or any other measure apart from negative publicity for not following the vague wording of the provisions.

In addition to this, in some cases the reasoning of the EC’s or parties’ taken actions in the annual reports seems to lack rational explanation. For example, it is said that ‘for ethical reason Principle 5 is not tested’, without any further elaboration what constitutes these ethical reasons. Furthermore, apart from indentifying insufficiency of the self-declaratory system[40 p. 1], no suggestion how to tackle this problem has been anticipated. Finally, the annual reports propose somewhat astonishing ideas by the following sentences saying that ‘safety is not an exact science’ and ‘not stating does not imply not doing’, basically implying that the EC supports the action of private actors in any event[40 p. 13].

7. Concluding remarks

As this chapter reveals, the desire for good regulation is expressed on national and European levels in policy documents. Academics from different disciplines also seek to define features of good regulation. Yet the field of regulation poses new questions as it is constantly developing and expanding to new fields and forms of regulation, such as self-regulation or co-regulation.

The analysis of the Principles in the context of good regulation encounters several drawbacks of the self-regulatory initiative, of which the most important is accessibility and openness. While applying the test it becomes clear that private parties still have to find ways to overcome the efficiency problems of a taken action. The application of test also reveals that it is relatively easy to criticize self-regulation while leaving behind the advantages that it brings in comparison with legislation enacted via democratic process. Yet the debate on the usefulness of self-regulation should be continued in order to establish benchmarks for high standard self-regulatory measure, which could secure and ensure the exact interests of society.
Conclusion

Firstly, it is apparent from this state of the art report that self-regulation in relation to children’s online safety in the EU is a controversial topic. Recently, it is addressed by policymakers, private parties and academics and it is claimed to be the top priority of the policy agenda. However, there is little information that this attention is caused by economic reasons. Ensuring children’s online safety would ultimately enhance the overall trust of the online activities, and thus, foster the Digital Single Market, which is the ultimate end aim of the Digital Agenda.

Nonetheless, so far the topic still lacks a comprehensive legal research establishing definitions of issues related to children’s online safety (Chapter I, part 9) and determining criteria for effective self-regulation (Chapter III). Yet there is enough empirical data gathered by various surveys depicting the scope of the problems occurring with children’s use of ICT and providing policy makers and society members with detailed knowledge about the online risks (Chapter I, part 3). However, developing risk based regulation has to be considered with precaution since it might be one sided (Chapter I, part 9).

Secondly, there are policy documents and legal tools developed within the frameworks of the EU and the Council of Europe to secure children’s rights and their well-being online (Chapter I, parts 7-8). Most of them provide guidance for action or minimum requirements, granting the MS with a wide margin of appreciation for the implementation of those measures. Consequently, this leads to diversified regulatory measures among the countries, which reduces the effectiveness of legal tools.

Thirdly, on the European level four countries (Chapter I, part 4) have developed elaborate regulatory frameworks aiming at securing children online, and therefore, they are encountered as examples of good practices, which could be followed by the other countries. Noteworthy, most of the considered countries have combined substantive law provisions with self-regulatory initiatives.

Fourthly, based on the observations provided in the second chapter, there is an oblivious need for a real platform, which would include various stakeholders related to the topic of children’s online safety at all levels. So far, the EC declares the existence of such platform, yet it might be criticized. The platform functions to a very limited extent; it provides stakeholders with a possibility to meet each other twice per year and usually has tight schedules. Therefore, the thorough discussions of relevant issues never take place.

Fifthly, with a growing amount of self-regulatory initiatives it is important to establish and determine a certain level of requirements or criteria for good self-regulation. The third chapter reveals that applying a good regulation test, which is primarily developed for regulatory measures enacted by democratic process, makes it easy to spot weaknesses and points for improvement of the self-regulatory initiative on the Safer Social Networking Principles. A good regulation test is also blind to positive features of self-regulation, such as efficiency, flexibility, enhanced compliance, reduced costs, adaptation to new technologies (Chapter III, part 4).

Finally, it must be noted that though the origins of self-regulatory approach to solve the issue of children’s engagement online can be traced back to the 90’s, there is no
substantial evidence providing the extent to which self-regulation can protect the rights of minors, and therefore, further research is needed.\textsuperscript{22}

\textsuperscript{22} The elaborate study as regards the minors’ rights online is provided by E.Lievens, \textit{Protecting Children in the Digital Era: The Use of Alternative Regulatory Instruments} (Martinus Nijhoff Publishers 2010).
Bibliography

1. The EC, A Digital Agenda for Europe, in Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 2010, The European Commission: Brussels.
2. The EC, Communication on Illegal and Harmful Content on the Internet, 1996.
38. The EC, Communication on a special place for children in EU external action, 2008.
44. Rauterberg, G.W.M. *Tools and Techniques Direct observation*. 2012 03 29]; Available from: http://www.idemployee.id.tue.nl/g.w.m.rauterberg/lecturenotes/UFTdirectobservation.pdf.
49. The EC, Report from the workshop "Every European child safe online". 2011.
Annex I

Interview Report

This interview report consists of a brief summary of the interview, a questionnaire, and a transcript.

a. Summary

This summary includes several parts, namely the part reasoning the choice of the interviewee, a part describing preparations regarding the interview and lessons that have been taken for the future interviews.

The decision to get in touch with this researcher was determined by the fact that Dr. Donoso research closely relates to the interviewer’s research interests. The interviewer got in touch with the researcher by the e-mail after the Digital Agenda Assembly, which took place on 16 and 17 June in Brussels. The interviewee was leading a group that the interviewer joined as a participant in the workshop on children’s online safety. The researcher was open for the interview, and therefore, the date and time for the appointment were set.

Two main tasks in order to prepare for the interview were to order a recorder from the library and to set up a questionnaire. The questionnaire was sent a few days in advance to Dr. Donoso. The main goal of the interview was to get information, which is of an added value and relevant to the research on self-regulation aiming to secure children’s online safety. This goal setting specified the design of the questions and the type of interview that was conducted. There was no doubt that the interview should be based on the qualitative approach and that the interviewer should employ self-completion questionnaire as a possibility to semi-structure the interview regarding the circumstances, meaning that the interviewer recognized a possibility to pick up on particular aspects that might be mentioned in answers. Most of the questions were about knowledge and some included opinions regarding particular issues. Finally, the choice of this particular method indicated for the interviewer that she will have to be an active listener, as the interference might be necessary in order to develop the interview in a way that the most valuable input towards the research is gained.

The interview went particularly smoothly. The interviewer was clear in her goals and knew what information is looking for and the interviewee had a clear expectation setting of the questions, since she received a questionnaire in advance. Thus, the overall atmosphere of the interview was relaxing for both sides. The interviewee was open, communicative, explicit and sincere in her answers, especially on the issues related to the Safer Social Networking Principles. Therefore, the interviewer felt comfortable deviating from the questionnaire and in several cases asked for specification of information that was provided. The interviewer deems the interview of a significant importance to the development of the research due to the
information, which was observed. It should be noted that the value of information is measured by the way it is perceived. Strangely as it appears, but details, which look small at the first glance, might have a bigger impact than the overall goal of the interview. The following two paragraphs will introduce to the most significant and interesting findings of the interview.

First, the interview provided the possibility to grasp the complexity of issues that surround self-regulatory initiatives. Currently, the debate regarding the issue is artificial, and thus, it does not bring any tangible results. This situation could be easily changed once the platform involving all stakeholders is established. Of course, the openness and commitment of stakeholders would be appreciated as it could accelerate the pace of the debate. However, the existing situation is not only about an unsuccessful communication among the parties, which is predetermined by the lack of clear concepts and vague wording of the guidelines, it is also about the regulatory aspects. Dr. Donoso emphasized the importance of two features that are essential in order for a regulatory measure to be effective, namely, the process of drafting and assessment/monitoring. Apparently, if the drafting and assessment stages are done prudently and thoroughly, they can ensure a well-functioning regulatory measure. In addition to this, the researcher identified critical aspects of the current regulation trend, which aims at adopting more inclusive regulatory measures. Dr. Donoso noted that an assessment should not be perceived as a final phase of a regulatory measure, on the contrary, it should mark the end of only one cycle, and thus, it should lead to improvements of a regulatory measure. Finally, in the end of the interview Dr. Donoso asked a rhetorical question, which could be used as a guiding light for the further research. In particular, she asked “What could make the online environment a safer place?”

Apart from the points, which can be labeled as the most important ones, other interesting information was observed. For example, the interviewee found it interesting to hear Dr. Donoso’s opinion that the distinguishing line between the technical layers and content layer is not possible. According to interviewee, ‘content and the way it is presented are intertwined’. Additionally, the interviewee identifies the intervention programs as an interesting point to look up.

The interview provided the interviewer with a valuable experience of conducting a qualitative semi-structured interview. First, the interviewer found out that the atmosphere and positive attitude towards the interviewee are important aspects in order to get the needed information. Then, this interview confirmed a rule that the effort which is put in the preparation of the questionnaire pays off in the form of the qualitative information. Third, the record of the interview is perceived as an important tool, which can be used not only in order to prepare the report, but also, in order to maintain the knowledge that was gathered. Lastly, to the interviewer’s surprise the recorder didn’t not cause any discomfort for the interviewee. Likely, the negative impact of the recorder was avoided due to the fact that the person was warned about it in advance.

b. Questionnaire
1. Please, briefly introduce yourself. What are you doing now? What was the topic of your PhD thesis?
2. What did determine your choice for the topic related to children’s online safety?
3. The debate regarding children’s online safety is very intense, many stakeholders, presenting opposing views, are involved. What do you think about this debate? What are the issues that are not addressed, addressed in a wrong way or even neglected? Do you envision any solution regarding the problem in question?
4. Your opinion/comments: What is or what should be the role of the European Commission in this debate?
5. Your opinion: What particular aspects of children’s online safety should be addressed by sociologists and what should be left to resolve for lawyers?
6. Is self-reporting system enough to tackle the problem? How to ensure compliance of self-regulation?
7. Your opinion: Can self-regulation be a proper tool to ensure children’s online safety in the EU?
8. Your opinion: How would you comment on the skeptical statement that ‘all this hustle about children’s online safety is a fake bubble and the EU seeks to gain more control over the information online’.
9. What are the next steps to be taken? What should be done in terms of policy action and research?

c. Interview transcript

Parties:
Interviewee: V. Donoso (V.D.)
Interviewer: L. Jasmontaitė (L.J.)
Place: Leuven
Date: 7 July, 2011
Time: 58 min.

Abbreviations:
The European Union - the EU
The Member States - the MS
The Safer Social Networking Principles- the SSNP

The interview transcript does not include introduction and closing parts of the interview as they are of no relevance to the thesis.

L. J. Could you briefly introduce me with your PhD thesis and your current work at the University of Antwerp?
V. D. Well, I wrote my PhD thesis some time ago. It was about children experiences with the online technologies in Chile. At that time in Chile there was almost no information about the Internet and what children do online. I took an approach which was more orientated to the developmental issues. In general, I tried to see, if the use of the Internet is impacting the way adolescences are developing. The main finding was that there is an impact, especially in terms of identity development, as adolescences are at the age where they want to find out who they really are or who they want to be. They also question their place in the world, and thus, they usually experiment a lot in order to find answers and in the online environment they do it more than in the offline world. Online provides them with spaces where they can pretend to be someone else, upload pictures, they can see how the others react to their changes, they can present themselves in any way they want to. So, one big focus of my PhD thesis ended up to be the way that new technologies can help the adolescences to develop their sense of identity. I am saying that it ‘ended up’ because in the beginning it was a very big exploratory survey of the uses related to the Internet. I wanted to map what was going on in Chile with adolescences. Since there was no research about that, I had to ask very typical and basic questions about the frequency and uses.

L. J. What sample did you take?

V. D. I took a sample from ten different schools of adolescences from 14 to 19 year olds. The sample was not representative as I made a survey only in the capital (Santiago). However, I did take into account the different types of schools. This task was very difficult since you have catholic, non-catholic, within catholic you have public and private, then you have separate schools for girls and boys. So every school was very different; spectrum of school was wide because they have different locations in the city and the society. It was interesting to see that children across the society, except the poorest ones, were using the Internet. At that time, the media was photo log, social networking was just starting. It was just before the arrival of Facebook.

L. J. But I thought you did you PhD while being in Leuven?

V. D. Yes, I was at Leuven but my research was about Chile, and thus, I collected all necessary data there; the analysis of the research I wrote here. My thesis also touched upon the internal learning as from the interviews, which I conducted, it became clear that children do not use the Internet much at school. So, I was wondering, whether they are learning anything from it. It was interesting to find, that actually, they are learning many things that have little to do with school. Children were rather keen on copying some things to their assignments than learning. The real learning process takes place, when children are looking for the information about the things they are interest in. The best illustration could be browsing for their hobbies. For example, one boy was very religious and he was learning things about the Bible. The other child was learning to play a guitar on his own by gathering information online. My research was very broad and in parallel with that, I started working as the collaborator with the EU Kids Online I. Participation in this project introduced me to the online safety issues. For the EU Kids Online I as was a representative of Belgium. This, of course, shifted my research focus and I got acquainted with situation in the EU.
V. D. I finished my PhD at the University of Leuven, and then, I moved to another department within the same university. In my second department, I had to deal with the users’ experience research. It was quite a move, instead of researching about children’s security; I started working with people developing various software and technologies. Firstly, I was involved in the projects developing e-learning environment for children. I was working for two years on that. Then, I applied for the position of a coordinator at the project of cyber bullying, by the way, it is about to finish. It was a call for tenders by the Safer Internet Program for which the Commission was looking for an expert to run a project. There is a difference between call for tenders and projects. For example, EU Kids Online is a big project coordinated by one institution, whereas a call for tenders is an achievement of a smaller scale. Nonetheless, the Commission invited people from all over the Europe to apply for the assessment of the Safer Social Networking Principles. Preselected candidates had to prepare evaluation of the existing guidelines. I was selected but this project lasts only for one year.

L. J. It seems that your scholarly career has a very clear path. Could you tell me what has determined your focus on this specific topic?

V. D. I always was very interested in things that are happening in a relation to new technologies and how they help adolescences to develop. I started doing research and then I found out that there are dangers as well. It became very obvious in the part of interviews, which constituted a very interesting part of my PhD thesis. I interviewed 30 adolescences and most of them have met with someone whom they got to know online in their real lives; people they met were not pedophiles or strangers, they were friends of their friends. The case was very obvious. Pupils from gender separated schools found it very difficult to meet the opposite sex and online technologies helped them to overcome this ‘problem’. So students were exchanging their contacts on the MSN and in this way they were getting to know friends of friends and so on. This finding inspired me to think that online activities can be risky as adolescences dare to transfer the online experience into a real life. This situation was alarming that we should do something about it. Interestingly enough, at the same time the project of the EU Kids Online I appeared. As I was interested in the topic, I started working on that project. I think that the leading coordinators, namely Sonia Livingstone and Leslie Haddon, are the main accents of the project as they have a gift of motivating people. Imagine they manage to have a big research network in Europe, in which everyone works on voluntary basis because of the ideals and the fact that they are such good leaders. The most of the money for this project goes for the data collection and analysis; no one is getting money for it. Of course, it is not only their authority, which makes you ‘to follow’ them, but it is also their openness towards your ideas and thoughts. During the EU Kids Online I, twice a year we had meetings of all members just in order to discuss all the ideas that we have, and though I was a PhD student at that time, I had a chance to contribute to the debate and they valued my ideas. So, I would say that it is not only the topic that inspired me to become so engaged in the topic, which is a very interesting topic; that brings a lot of practical aspects that have to
be changed or resolved. For me it was very important the way of working towards one goal, and of course, finding the right network. At the moment there a lot of findings available regarding the potential risks and harm, but somehow they are not taken into account in the reality.

L.J. Indeed, this is what I am also missing. Actually, this is what I wanted to ask you in the following question, which is about the ongoing debate on the issue of children’s online safety. What do you think about this debate, what is missing and what is neglected? What are the issues that are not addressed, addressed in a wrong way or even neglected? Do you envision any solution regarding the problem in question?

V. D. This is a very interesting and difficult question. I think this is a necessary debate and this is something that we should be debating more. There are many stakeholders involved at many different levels; therefore, at the end of the day, it is important to take into consideration everyone’s views. I think that there is something missing. For example, as you saw yourself, at the Digital Agenda Assembly the most important stakeholders were represented; they take part in these meetings. However, it is not that they initiate their participation; they are basically invited by the Commission to attend several meetings or forums per year. Yet there is no real platform for all stakeholders to work together or to listen to each other. As you saw, we had some time, we had a nice workshop, but when the time is so limited, there is no time to listen to each or to talk thoroughly. It is intimidating for adolescents and for academics to talk in front of the representatives of private actors, as well as for the industry side it is hard to communicate with academics because of the stereotypes that are widely accepted. The industry side is thinking that they know about the problems in question better because they deal with real people while running their daily tasks, whereas academics are thinking that the industry side is interested only in profits. Therefore, there are a lot of issues in this debate about the internet safety of having stakeholders apart. This separation leads to the lack of real communication, not meaning those artificial one-morning meetings twice a year, but real work together. I have seen some companies trying to make an effort and sending their personal to schools or various institutions to talk with people about the threats that the Internet brings and how to protect children, but this is not enough. Apart from having an instance for communication and indentifying the problems, the other big problem is developing intervention programs that can help children to tackle and deal with risks. Obviously, the pace that technology is developing is hard to be ahead, but the field is pretty much covered as most of the risks have been already identified. There is enough scientific and reliable knowledge, but then, there is a big gap as none takes responsibility to act.

L. J. Could you please elaborate what do you mean by intervention programs?

V. D. For example, let’s take a concrete case with cyber bullying. Of course, there is a lot of overlap between bullying and cyber bullying. Most of the schools have developed specific policies how to deal with cases of traditional bullying. Everyone is aware of his/her role. Children know that, if someone beats them, they should go to the head of the class, school or psychologist and talk about that; by the help of adults they will develop a strategy how to
deal with a certain case. For example, they might develop a strategy how to prove empathy of a child, as it scientifically proven that, if children are more empathetic, they bully other less and other way around. Basically, in the cases of traditional bullying specific programs are chosen in order to develop certain skills. The same happens in cyber bullying cases to a far lesser extent. Teachers at school are not aware and sometimes do not have skills enabling them to deal with the problems that occur online, meaning that they cannot look for a solution. Therefore, I think there is lack of knowledge of the people – care-takes, meaning teachers and parents, who traditionally deal with those problems. In the contemporary world of online technologies, we have a lot of parents who are not aware or do not manage technologies very well. It is hard for parents to help their children to tackle cyber problems because sometimes they are not aware of the existing technologies. Thus, I think concrete measures, materials, and actions at school or at the community level could be established. As I am concerned, there are initiatives, but then, they are not centralized, they are scattered. There are some NGOs and schools which are trying to contribute to creation of the safer internet, but then there are other schools which follow do-nothing policy, even the police forces are dealing with cyber crimes differently depending on the country. There is no tendency towards safety, as at the moment, there is no policy on the Internet safety in place.

L. J. Do you think it should be done on the European level or the Member States should find solutions adequate for their specific situations?

V. D. I think that the general guidelines could be set on the European level. It would enhance the importance of the issue, if the EU takes the lead. However, there should be enough space for countries to adapt these general guidelines in a way that reflects specificity of each MS because even with one country the situation regarding the online safety might vary depending on the region. For example, some schools are advancing the topic more than others; some members of the society are very skilled internet users whereas many are not. So, the creation of general guidelines on the EU level is welcome, they would give an incentive to act. However, the formulation of those rules is a very hard task. What does it mean e-safety? (Rhetorically)

L. J. Indeed, it seems that definitions constitute the trickiest part. There is no definition of children’s online safety or children safety, although everyone debates about it.

V. D. Indeed, it is an issue. The definition of safety changes according to the one, who is talking. We assume the safety is minimized risks, but this is a common definition, without any real parameters to measure it. What is the standard to measure and determine that one child is safer than the other child?

L. J. Yes, it is a tremendous task. Following among the same lines, I would like to ask you, what should be the role of the European Commission in this debate?

V. D. The problem in question touched upon is on a very sensitive political ground, thus, the Commission plays very safe. Anything that is said by the Commission has a very big social impact on all levels of the society. I believe that the main role of the Commission is to enable a dialogue among the stakeholders; only afterwards comes the determination of the things
that should be done. I think it is very important that they create real platforms that could foster the dialogue among various parties. Additionally, I think the Commission should continue supporting various self-regulatory initiatives because otherwise companies will be left aside and they will be able to act in their own discretion. The Commission as a key player on the EU should assume the greater burden for itself as not all the MS have enacted specific laws regarding online safety, especially in the relation with the protection of children safety, although children are exposed to higher risks and they are more vulnerable than other groups because they do not identify the threats that await for them.

L. J. This is a very interesting opinion. Being a social scientist you should see the difference between lawyers and sociologists while approaching the issue in question. What are the particular aspects of children’s online safety that should be addressed by sociologists and what should be left for lawyers to resolve? Do two groups understand each other?

V. D. I think the boundaries between legal and sociological aspects are very blurred. Moreover, this relationship depends on each country’s legal system. For example, laws regarding privacy requirements, freedom of expression, or how to deal with information provided by users on online surveys differ a lot. There are countries without laws regulating those issues.

L. J. And what about the directives setting the minimum requirements for the common ‘play ground’?

V. D. Yes, there are directives. I am not that well acquainted with them. However, in general I think, that instead of dividing the tasks that one should do, the sociologists should be in a position to inform lawyers and legal experts about the findings of their research, whereas lawyers should inform social scientists about intellectual property rights (IPR) and other legal issues. I am certain that interaction between two is very important in order to make righteous decisions and create laws that protect children. However, I myself know only one lawyer working on the IPR issues. Of course, there are people specializing on the criminal law matters of the cyberspace. It is amazing to see how our perspectives differ as they look only on the legal acts. However, on the cyberspace there are a lot matters that are not considered as crimes, such as cyber bullying. But then, what does happen when a child commits a suicide because of being a victim of cyber bullying? In this case, it is difficult to draw a distinguishing line between legal and social aspects; it becomes difficult to determine liability. I sometimes think that it is an unnecessary distinction as some of the issues are penetrating both fields at the same time. Let’s think about the other example. What does happen to your data provided on the websites? There are services where you cannot delete your profile, if you have made one. This means that they will own your information forever. Is this legal? I do not know. Should it be legal? Probably not, and this is what lawyers should tackle by the means of legal measures. So, the sociologists should share the information in the field with lawyers. Finally, I think it is a good match, which could ensure the protection of all citizens, not only children.
L. J. Now I would like to go back to the topic of self-regulatory initiatives. Do you think a self-regulatory initiative is a proper tool to tackle the problem?

V. D. I myself, I do not know, if it is a good or the best measure. I think that because of the political reasons, self-regulation is the only way that has been accepted by all partners. I think that big companies would not like to be regulated from outside. However, self-regulation, if it is not assessed, or if it is not evaluated externally, it does not make any sense. Companies while opting for self-regulation expect to preserve their freedom in decision making, for example, what are the best things to do, according to the philosophy of the company, or their customers. Companies want to remain in power of determining their action. Thus, self-regulation to a certain extent is a good option because you have a variety services, customers, and people. Following this, companies have a right to decide what measures they should take, but the problem is finding out, if these measures are appropriate. This is impossible without any evaluation. So, self-regulation within the framework which is serious and independent, and well designed is O.K. to me. But if the evaluation part is missing, this kind of measure is useless; it becomes a nice way of saying ‘We do what we want because it is our option to regulate ourselves and we do not want anyone to intervene into our internal matters’.

L. J. But isn’t what has happened with the Safer Social Networking Principles on the EU (SSNP)?

V. D. The problem with the SSNP firstly lays in a fact that they were designed by the companies and a few external people advising them. So basically, the SSNP are problematic because of the way they were drafted. As people, who drafted them, were not experts on the issue, it becomes difficult to evaluate those Principles or apply any methodology to measure the compliance with the rules. Compliance maybe is not a proper word, as there is a whole debate arguing that, if they are self-regulated, they are not legally liable. This means that you can assess, only if they are implementing measures well or not; you cannot establish any benchmark while assessing them in the way the principles were drafted. There are too many open questions that are prescriptive and that are suggesting the best practices, if it is only a suggestion, someone from outside cannot say, well, you are not implementing this principle in a right way. The party will answer you, ‘but this was only a suggestion and I (company) implement this in a different way and I am aloud to do that’. So once you are confronted with this kind of the answer, you realize that, if the principles are not properly drafted, a whole assessment afterwards is a contempt to evaluate something that has been wrong from its very beginning. Evaluation becomes very difficult and subjective.

L. J. So do you think that the revision of those Principles will enhance the quality of this self-regulatory measure?

V. D. Definitely, I think it is a key point in self-regulation, meaning any principles or guidelines, that after every evaluation, a regulatory measure should be reviewed because evaluation points out the weaknesses of the measure, which can be changed.

L. J. So what do think about self-reporting system set in the SSNP? Is it enough to tackle the problem? And finally, how to measure compliance?
V. D. Do you mean self-declarations?

L. J. Yes.

V. D. The process in the specific cases of the SSNP is based on their structure. As you know, they consist of seven guidelines, and companies, which are committed to those principles, have to prepare self-declarations, in which they describe how they implement each of the principle. So basically, the companies declare to the world how good they implement the provisions related to children safety and this story usually does not reflect the reality of what they are actually doing. Furthermore, even if the reports include the real information, it is does not mean that this is the best what that company could do or the best approach towards online safety. I think the next step, which should be a part of any regulation, is an independent assessment. So this is basically that I want to show with my recent project in which I developed a two-step methodology. The first step is to analyze those self-declarations in the relation to the guidelines, then, I question, whether the approach that has been taken is in favor for a particular principle, and whether the measures contribute to the implementation of the principles. Usually self-declarations are positive; therefore, at first glance it seems that companies are following their commitments duly. After this first step of the assessment is completed, we move on with actual testing of the websites. I have developed several tests, which were applied by the different researches in the different parts of the EU. The researchers mostly had to create fake profiles of children, adults, and strangers, some of the researches were assigned tasks to pretend to be an adult, who wants to get in touch with children, or to create cases, for example, a case of a girl sending messages and asking for a help from a company to deal with bullying or unknown people. The companies were not aware of this testing system, and therefore, the results enabled us to see, whether the companies have followed their promises. Based on this exercise, we published evaluation report. The biggest issue that we found, which Neelie Kroes mentioned as well, was the privacy by default. We tested 14 websites and it appeared that only two of them keep the information of minors private, whereas if you look at the self-declarations you find written that the profiles of minors are private. There is no reason to think that companies are providing falls statements in those declarations, they just use different concepts of privacy. The definition of ‘privacy’ that is provided in the principles sets higher standards than it was interpreted by the most of the companies. However, this situation stresses the obvious lack of clear definitions, such as privacy by default. Also, it is not clear who should be included in the accepted list of contacts. Who should be able to contact minors? For example, companies, such as Facebook, allowed friends of friends to contact minors and they did not realize that until we pointed this out. So the evaluation tests should not be seen as a critique but as a way to develop ideas how to improve their applications. As independent experts we are not allowed to make suggestions for a company, but we can point out problematic issues, which can be easily changed or resolved. Interestingly, the companies instead of changing something usually start defending themselves and deny the existing situation. Then, we have to send information proving things that have pointed out. For example, one company denied the existence of alcohol commercials, so we sent the data, meaning advertisements of alcohol,
which we found on that website. This means that we have to work very carefully and preserve the evidence of all the information that we find.

L. J. But the pace of the online technological development is accelerating, so it is challenging to keep up to date, and then, websites are dealing with the content layer issues. Do you think there is a distinguishing line between two?

V. D. What do you mean by content layer?

L. J. Well, the Internet deals with technological issues whereas cyber space and websites deal with content.

V. D. I think that it is a difficult distinction to make. The online technologies cannot be separated in content or format. This is exactly that makes them so interesting and so difficult at the same time. Even the very nature of content and the fact that it is hyperlinked makes it so different from the static sources of information, such as a book. Therefore, I think that content itself and the way it is presented online are intertwined and not separated. It deals with all types of formats, video and music files, and self-generated content. So this is not only the question of content. Certainly, we try to deal with it by questioning, whether it is enough that the company provides safety information on the bottom of the page in a tiny font or on the footer of the page adds a link to the safety information. Of course, then companies argue that they are compliant with guidelines as they have a button for help under which you can find terms of use and under this you can find safety tips for children. Then the question raises, whether it is enough to provide content, and in what way this content should be provided. I think that the content in the online environment should be provided in an accessible, interactive, attractive way for children and in a way it can be easily used and understood by parents. In general, information should be user friendly and findable, thus, I think that the question of safety has a lot to do with design mechanisms. The child in case of a problem, if s/he does not dare to talk about it with her/his parents, s/he should be able to deal with it online. I think that the content and the way the content is presented, is essential for children. Of course, children at different ages have different needs and they favor different things.

L. J. This is a very interesting point. Differentiation of age groups is what I am missing in the current debate on the online safety.

V. D. This is a very important issue. We paid a lot of attention to that while conducting evaluation tests. We asked questions differentially, for younger children and for adolescents, if the services were open for all kind of ages. Most of the services in the terms of use say that they accept children profiles from 13 years, however, this does not prevent children from getting on those websites earlier. Of course, the company continues to say that children under age are not allowed to register, and this way they withdraw from the problem. If they do not take responsibility, then who should do that?

L. J. Yes, the questions of responsibility and liability are problematic, for now there is no answer. Following among the same lines, I would like you to comment on the skeptical
opinion that was in the air of the workshop at the Digital Agenda Assembly that all this hustle about children’s online safety is a fake bubble and the EU seeks to gain more control over the online information.

V. D. I do not think that this is a valid statement. Of course, it is always convenient for institutions in power to have control over what is happening and information. However, the EU is seriously concerned about children’s online safety. So I do not deny that some other issues might be involved, but I do think that the Commission’s action favor children. Certainly, they could do more and invest more money into the social research and education. If we follow the rationale that the sum of money invested in the field determines its importance, then, obviously, the research on engineering and medicine issues would overtake any social science project. Thus, I would conclude that the interest is limited as it is not the primary goal of the Union.

L. J. This is a very interesting remark. As we are approaching to the end of the interview, I would like you to talk about the next steps that are about to be taken, apart from the revision of the Safer Social Networking Principles. What do you think should be done in terms of policy action and research?

V. D. Well, there are different directions. One direction is of a self-regulation. The more self-regulation is being demanded and the more is being produced. We have not only the Safer Social Networking Principles; we have the European Framework for Safer Mobile use by Young Teenagers and Children. In a short while we will also have the Safer Internet Principles in very general terms, the ones we were discussing during the Assembly. These principles will cover not only social websites, but all type of services which have to do with children and online technology. So the current trend is that regulation is becoming more general. However, I do not think it is a right way to go, I think the regulation should become more specialized. From my point of view, the Safer Social Networking Principles are already very broad. Furthermore, as you saw, there are parties who are not social networking sites but they do have social networking functionalities, for example YouTube. Following the assessment process both types of websites are evaluated according to the same principles. I encounter some inconsistency here. I think the broader is the scope of a certain regulation, the harder it becomes to evaluate and assess the compliance. So the current trend to develop broad principles for everything is a wrong approach. Although they can be applicable for all, at the end of the day they are applicable for none. I am certain, the if the EU engages in a self-regulatory approach, then the right direction would be to establish a stricter benchmarking and develop guidelines together with standards, that those guidelines should respond to. It is not enough to say what could be done, evaluation systems should be developed together with guidelines because this is the only way to see the problems of your guidelines.

L. J. What do you mean by standards?

V. D. Evaluation standards for principles. However, I am not sure that establishing principles is a way to go. Maybe instead of principles there should be something similar to the
technological standards that replace principles, which are too general, liberal and free for interpretation. On the other hand, some basic things could be regulated in a stricter way, for example, all children should be able to report cases of inappropriate content in an easy way. Maybe this could lead to developing a standard of a red-button. Yet there is a huge debate about this type of reporting system, and maybe it is not the best solution, but this example just illustrates that many things can be done. Of course, I understand companies, they do not welcome any external regulation as they are the only ones, who posses expertise in the field and know all the information about future developments.

L. J. Do you intend to say that some minimum requirements could be established by means of directives or other legal tools?

V. D. Directives might be a solution, but they should concern only some legal issues. All the parties should agree on the issues that will be regulated. However, the debate on the top issues of children’s online safety still has to take place; all the parties have to agree what is crucial to achieve in order to protect children. At this very moment, we have some principles, though this end phase of the debate has not been reach. There is no research proving or demonstrating that the online environment becomes safer because of the principles, we just have assessment of self-declarations. So we can conclude that Bebo is implementing the SSNP better than Giovani, and thus, Italian children are safer on Giovani. But what are the implications of those principles in practice? I think that at the given time, we speculate more, than we make meaningful conclusions. The compliance of the principles is tested by one person per website, without knowing, if those principles are really protecting children. I see inconsistency in policy as the principles are not based on any empirical or academic research. In my opinion, the things had to proceed in the following order. After the risks were identified, the principles had to be developed. For example, children are confronted to greater risk on this and that platform; therefore, it should be done this and that in order to ensure their safety. This reflection would enable us to develop principles that tackle real problems. If we go back to the Safer Social Networking Principles, it is unclear who developed them and under what basis, it also unclear, if any of those principles prevail over the other.

L. J. But isn’t it that the current situation is a direct consequence of the choice that was made in mid 90’s based on the discussion on the way the internet regulation should developed? At that time it still was not clear who should take responsibility for the Internet’s regulation. As states at the time realized that they are not cable of regulating cyberspace, they in a way delegated ‘legislative powers’ to the private actors. From that time onwards, it was assumed that self-regulation is the best option, without having any information proving this position.

V. D. I am not sure if self-regulation is a better option. Of course, there is an issue as we talk about new technologies and companies which are upfront in technology. Self-regulation makes sense as only the companies know what their customers want. I am sure that they know, which direction to go, but how can one make sure that they choose not only a way to increase their profits but the well-being of their clients as well. However, I assume that for the companies it might be hard to be regulated by government, if they feel that the legislator does not have expertise. Thus, if one seeks to develop a legal measure, one should gather top
experts, engineers, developers of graphic software in a field as they possess knowledge in the field. In general, some real work has to be done in order to develop regulation; academics should be heard and children should be consulted. At this point maybe there are companies which would like to contribute to this kind of regulation, but this attempt is not enough. There is a need for a platform, which would include stakeholders which would be open towards each other and willing to hear and understand opposing views. I usually feel like someone in between the two worlds, academics and industry. At the given time, problems go beyond self-regulation. Furthermore, there is one thing that I wanted to mention regarding the self-regulation. If principles are meant to protect children online, the first thing that we should do, is to discuss what do online safety and other relevant definitions mean. And before developing tools and self-regulatory measures we should discuss the issues of media and literacy, those two are the points that currently are absent in the SSNP or anywhere else. Therefore, the final question that remains open for the further research follows like what “What could make online environment a safer place?”

L. J. Indeed, this is the question, which should be answered as soon as possible; it could contribute to solving the problem in question. Thank you so much for your answers and time.

The interview was closed with an agreement that the interviewer will forward the report to the interviewee for a revision. The report and transcript was revised by the interviewee.