



## Growing up digital – how can we make the internet safe for children and young people?

**AGF European expert meeting  
3 July 2017, Berlin**



# Growing up digital – how can we make the internet safe for children and young people?

3 July 2017, Berlin

## Agenda

Background .....	2
Key findings of the expert meeting .....	3
Facebook, WhatsApp, Instagram – how dangerous is the internet for children and young people? .....	4
EU regulations for a safer internet.....	7
Country Report: Estonia.....	10
Country Report: Denmark .....	12
Online security for children – Legislation and additional measures in Germany .....	14
What does it need to make the internet a safer place for children and young people? .....	18
Discussion and first conclusions.....	22
Related Links .....	24



## Background

The internet and online services such as WhatsApp or Instagram are an everyday part of children's and young people's lives. Nowadays, they are not only users and consumers of online content, but also producers as well, who create and distribute their own content, for example by participating in social networks, writing blogs, designing websites and a lot more. This, however, also exposes them to risks, for instance from harmful content, heavy advertisement or the violation of their privacy. Therefore, children and young people often appear in their online activities as digital experts and vulnerable users as well.

The European Commission and also many EU countries have already introduced measures to improve the access to the internet for children and young people and, at the same time, to make it a safer place for them. But what are the actual risks children and young people are facing and how do the threats and the existing efforts within the various EU member states differ? How helpful are the measures taken so far on European and national level? Who are the key players when it comes to creating a safer internet and how should they each be involved?

Following the AGFs invitation, experts from politics, organisations and academics got together at the European expert meeting to discuss these and other questions. The event focussed foremost on the existing measures to protect children and on concrete experiences from some member states. However, it was also discussed which further steps are necessary for a better online protection nationally and on EU level. The introductory input about the results of the EU Kids Online study started by pointing out the crucial internet risks for children and young people and gave a first insight into the various conditions and problem areas in different member states. From the following country reports from Denmark and Estonia, two pioneer states regarding the use of the internet, participants learned about their most frequent risks and current approaches to achieve more internet security. While the report from Denmark focussed mostly on fostering media literacy among children and young people, the input from Estonia looked at the political instruments for regulation and awareness raising. The country reports were complemented by a detailed look at the legal conditions for online child protection in Germany. In the concluding inputs, two European organisations outlined possible future scenarios in handling online risks and made proposals on how to improve the online safety for children and young people, especially at EU level. The requests and the panel discussion showed that a safer internet for children and young people is a challenging task that can only be successfully mastered when all stakeholders will be involved.



## Key findings of the expert meeting

Internet risks	Risks for children and young people are mostly inappropriate content, like pornographic images and depictions of violence, the vulnerability of their privacy and person, child pornography, but also advertisement. However, a risk does not necessarily lead to an actual threat for children. It depends on the reaction to the risks and therefore on the existing media experience and literacy. Insufficient media education is an additional risk.
Current measures for more online safety	The member states in focus place their emphasis on awareness raising, media education and regulation. The latter includes laws but also self-regulation through providers as well as technical means. How these measures are mixed and organised differs among the states. Denmark and Estonia predominantly count on media literacy and awareness raising, while Germany rather expands regulation.
EU priorities	The EU predominantly counts on self-regulation, it has no political competences for educational measures. There is hardly any EU law for a better online security (exception: AVMSD, GDPR). However, the EU seeks for binding agreements with social platforms, for example in regards to hate speech and illegal content.
Importance of teachers and parents	In Denmark and Estonia, media education is already an integral part of school curricula. However, in both countries teachers are insufficiently prepared for this task. Media topics are not part of their professional education, also suitable trainings as well as an appropriate financial and conceptual support for schools are widely missing. Parents play another important role, but are often equally unprepared and rarely informed about problems. Families should be informed about the importance of media literacy as early as possible.
Responsibility of businesses	The internet economy is crucial to achieve a better protection of children and young people as it strongly influences their online behaviour. However, they mostly do not assume responsibility because their economic interests often conflict with the protection of children. But without the businesses, a notable protection will not be achieved. Stronger regulations in this area were seen as useful.
Limited influence	Because of the fast pace of the internet, studies can only measure the internet's development and risks retrospectively. Thus, proactive policies and a long-term development of the skills needed by children and young people seem difficult.
Need for action	The measures discussed mostly concentrated on the expansion of media literacy and on suggestions for more effective regulations. However, the optimal balancing of these two central instruments remained controversial. A multi-stakeholder-approach was demanded, including all stakeholders as well as teachers, parents and children themselves. Obstacles for more online safety were seen in the economic interests of internet businesses, but also in insufficient legislation and the inadequate equipment of actors in the field of media literacy.



## Facebook, WhatsApp, Instagram – how dangerous is the internet for children and young people?

In her thematic introduction, Claudia Lampert provided an overview over online-media development in general and the internet use by children and young people. Her presentation was mostly based on studies by the EU research project EU Kids Online, which the Hans-Bredow-Institut participates in. Her contribution outlined children's and young people's use of the internet in Germany as well as in other EU countries.

### Changes in the digital world

One of the most characteristic developments of the internet is, according to Claudia Lampert, the mobilisation of the internet and the use of touch-screen-media. In addition, children and young people are nowadays always online, or „permanently connected“, which means they are continuously ready to receive incoming data. For today's young generation, to be online is predominantly a synonym for a permanent communicative connection with friends and family. At the same time, the social web as well as many apps offer many new possibilities for using the internet. Children and young people use online services mostly for communication, gaming and for entertainment purposes, less for information research.<sup>1</sup> An essential feature of communication on the internet is the possibility to address various publics: from certain (sub-)groups, like one's own family, friends, study groups or class mates, to the general public. The role of the media users has changed as well over the past years. They are no longer consumers but rather become more and more providers of their own content, for example via Facebook, YouTube or Snapchat, so that research often speaks of „prosumers“, to clarify the changed role of internet users.

### Online experiences of children and young people

In 2010, the EU Kids Online study recorded the internet experiences of 1.000 children in each of the surveyed 25 EU countries at the age from 9 to 16 years and their parents. This project originated from the EU's Safer Internet Program. It examined, among others, factors influencing risks and dangers on an individual, social, and national level. So, in a first step, the countries can be placed into roughly four groups according to the distribution of internet use: Scandinavia and The Netherlands as forerunners of the internet, followed by continental Europe, most of the East-European states, and finally the states of Southern and South-Eastern Europe as latecomers. Germany lies in the second group, as well as the East-European leader, Estonia. One main result of this grouping is the finding that children are younger when making their first contact with the internet the longer the internet has already been provided in a country, and that the longer internet access has been provided the more online abilities they have as well.

---

<sup>1</sup> Here, it remained open, what children and young people consider as „information“.



The study has also shown that children and young people encounter risks more often, the more they are active online. Concerning the number of risks, Germany is midrange. Children and young people in Scandinavia for instance experience significantly more risky situations. It is also true that risky contact with the internet increases with growing age. But, if one compares the statements in the study made by parents and children about negative experiences on the net, it shows that parents often underestimate the problems of their children online, whereas among children and young people there exists a relatively high risk awareness. For instance, only eight percent of parents knew about negative experiences of their children on the net, whereas twelve percent of children stated that they already had encountered negative situations. Even two thirds of the children and young people interviewed said they knew that also bad things existed on the internet and that other children had already made negative experiences. However, Claudia Lampert pointed out that the risk awareness varies considerably among EU countries. In Denmark and Spain, for instance, there is a very high risk awareness, however, there are clear differences in risk management. For example, 28 percent of Danish children stated that they have had negative experiences on the net, compared to only 14 percent of the Spanish children. German children and parents reported rather rarely on negative experiences, but the risk awareness also lies relatively low and well below the European average.



*„Studies show that children and young people with a higher media competence experience more risks on the internet but at the same time they are less threatened by them.“*

Dr. Claudia Lampert,  
Senior Researcher at  
Hans-Bredow-Institut für  
Medienforschung, Ham-  
burg University

## Concrete risks

The EU Kids Online study looked at various online risks, like cyberbullying, meeting strangers, sexting as well as contact with sexual images and pornography.<sup>2</sup> Exposed to the latter risk are mostly older children, boys more than girls. In Germany, the contact risk to sexual images lies clearly under the European average (10 percent compared to 23 percent), however, here, more children report negative experiences with those images (35 percent compared to 32 percent). Cyberbullying, meaning mobbing on the internet, poses another risk, even if, according to the data, it rather takes place in real life than online. On the internet, especially social networks or messenger services are used for that. Affected are mostly older children and predominantly girls. Twelve percent of the children and young people that were asked during the EU Kids Online project said they had already once harassed others by bullying them, but less online than in real life (Germany: 16 percent).

Sending or receiving sexual messages is another risk when using the internet and it affects mostly older teenagers. With 27 percent, the percentage of those having made negative experiences with such messages in Germany, lied relatively high. But, only three percent of children and young people in the EU stated to have sent such messages once. Compared to this figure, it is much more common to have contact with strangers on the net. Almost one third (30 percent) of the children and young people asked stated they already had contact once with persons whom they only knew online. At least every eleventh child – in particular older teenagers – has even already met with a stranger. This risk is highest in Estonia, where every fourth child has already met once with a stranger. For Germany, the numbers lie below

<sup>2</sup> The survey was conducted in 2010, so that some newer phenomena such as hate-speech are not yet taken into account.



that but again somewhat above the European average, with 38 percent already having had contact and 11 percent real dates with strangers. Because usually children and young people do not share their online experiences with their parents, they often do not know, what risks their children encounter. For example, when it comes to mobbing, parents only knew about such incidents in one fourth of the cases; instead, in almost half of the cases the parents were even convinced that their child was not being mobbed.

## Similarities and differences among countries

In general, following Claudia Lampert, children and young people can be divided into four types according to their use of the internet, the risks, and their parents' handling of both. Mostly children and young people from Scandinavian countries and from the Netherlands belong to the first type, the „supported risky explorers“. There, parents accompany the internet use quite actively, however, the risk for children and young people to come into contact with

The expert meeting focussed on the existing measures for creating a safer internet for children and also on the experiences in selected member states.



sexual images is higher than in other places. Germany and most European states, in contrast, can be placed in the category „protected by restraint“, which means minimalizing the risks but, at the same time, also the positive use of the net. Children in Eastern and South-Eastern Europe, including Estonia, are to be characterised as „semi-supported risky gamers“. In these countries, the internet is often used for entertainment purposes and parents try to be pro-active and also restrictive but they rather remain unsuccessful. In the fourth and smallest group of the „unprotected networkers“, the children and young people act to a great extent unaccompanied by their parents. Risks in using the internet exist, but the threats are not very big. The focus of the use strongly lies in social networks. Mostly children and young people from Austria, Hungary and Slovenia belong to this category.

In general, the results show that in EU countries the internet use by children differs a lot, depending on context factors, for example popular activities, risk awareness as well as social

guidance of internet use. Therefore, various approaches are necessary to achieve more internet safety in Europe.

## Media literacy and parental support

Claudia Lampert pointed out that it is important to underline that not every risk leads to a threat (in the sense of children and young people making negative experiences) automatically. Rather are a lack of media literacy and insufficient support when using the internet additional risk factors. The results of the EU Kids Online study have also shown, among other things, that even though a higher media literacy increases the contact with internet risks, it is less likely that these risks turn into negative experiences and harm the children and young people. In turn, though a restrictive media education reduces the risk contact, it also comes with a lower media literacy of the children. So, negative experiences from risks on the internet can especially be prevented through an active media education and a high media literacy. Furthermore, the children and young people need to learn to handle the existing risks and to competently face them. Therefore, parental support is needed too, for instance, by parents talking to the child about the internet, possible risks and possible problematic experiences, but also by encouraging them to try out (appropriate) services and by staying around while their children are using the net.

## Future needs for action

In order to be able to adequately accompany and support children using the internet, there is a need to increase parents' but also teachers' awareness of children's and young people's internet use. Media literacy training is a cross-sectional task, which – according to Claudia Lampert – can only be truly successful if parents, teachers and adolescents cooperate with each other. In addition, an update of the research is needed in order to keep up with the fast, technical development and the ever-changing user behaviour. For 2017/2018 there is a plan to repeat the EU Kids Online survey in various countries, which will address current topics, for example, health consequences of internet use or new risks like hate speech.

## EU regulations for a safer internet

Elisabeth Kotthaus's contribution focussed on the competences and capabilities of the EU Commission in regards to internet security for children. She informed about current measures on EU level, such as the ongoing revision of the directive on audiovisual media and the just adopted General Data Protection Regulation. It became clear that the EU Commission, regarding the protection of children and young people in the internet, put emphasis on self-regulation of the various internet protagonists.

At the beginning, Elisabeth Kotthaus pointed out that the EU Commission has fundamentally only a coordinating role within the educational sector. Laws can transfer competences to





the Commission, but they have to be passed by the Council (in which all member states are represented) and the European Parliament. Yet, at the end of the 1990s, the EU Commission decided to address online safety of children for reasons that are still obvious today when livestream of child abuse has significantly increased in 2016, as well as cybercrime in general. Also, recently a British study has shown that almost every child between 8 and 13 years has already been confronted once with hate speech on the internet (82 percent). Therefore, in 1999 the EU Commission initiated the Safer Internet Program, however, these measures remain quite isolated and under the responsibility of the member states. In 2011, the council reached an agreement to bundle the various national activities into a coherent strategy. The European Council thereby defined that regulatory measures shall not be excluded completely but being avoided in favour of a more flexible self-regulation and additional awareness raising. Thus, the EU commission has, in 2012, suggested the "European strategy for a better internet for children". This strategy rests on four pillars, reinforcing each other: the support of high-quality online content for young people, raising awareness and qualification to create a safer online setting and the fight against sexual abuse and sexual exploitation of children. According to these strategy, recommendations to the various stakeholders followed, whereas the EU Commission coordinates the different players at the different levels.

## Current legal measures

However, there are laws on the EU level with regard to internet security for children. For example, at the moment the existing directive on audiovisual media (AVMSD) is being revised and relevant, proposed amendments of the Commission are being discussed by the council and the parliament. In regard to the internet an initiative of the Commission demands to take the protection of children in „non-linear“ media into account more strongly and to treat all media the same. Also under discussion is the protection against harmful content through special access codes such as PINs or encodings. The Commission also suggested a fundamental orientation towards the principle of the "significant audience", which means that regulations should not only take effect on services explicitly meant for children but apply to all services, which are to a relevant amount also used by children. However, so far, neither the council nor the parliament have taken this idea into consideration for their proceedings. Generally, there are still some differences to this question between council and parliament. As an additional legal instrument, Elisabeth Kotthaus named the E-Commerce-Guideline, which, among other things, deals with the liability of internet service providers for illegal content. The current guideline states that a responsibility for such content only begins from the time when the service provider knows of it, in which case, however, the relevant content must be made inaccessible as fast as possible.

The recently adopted General Data Protection Regulation (GDPR) also includes special regulation for minors.<sup>3</sup> The regulation especially demands that in the future, children under 16 years need the approval of their parents or their guardians, for the transmission of data, and

---

<sup>3</sup> *The General Data Protection Regulation (GDPR) standardises the rules for processing personal data by private businesses and public authorities. This regulation is meant to guarantee the protection of data in the EU and at the same time to ensure the free data traffic within the internal market.*



that such an approval of a third party has to be identifiable as such as well. The technical implementation is being discussed at the moment by data protection authorities, national legislators and the internet economy. The member states can lower the age limit nationally to 13 years. The General Data Protection Regulation enters into force in May 2018. It will then become equally and directly effective for all EU countries.

Moreover, Elisabeth Kotthaus pointed to the Directive on combating the sexual abuse and sexual exploitation of children and child pornography. It explicitly provides for the deletion of such content from the internet. In doing so, the EU also relies on a broad network of hotlines, such as the Safer Internet Centres, which receive relevant reports and which work towards blocking access to such content completely. However, this is not easy because very often the service providers are not located in Europe, which complicates the enforcement of the blocking.

## Self-regulation and financial support

A safe and attractive digital setting needs self-regulation, that preferably includes all stakeholders, meaning the member states, civil society and also the internet economy. Following the invitation of the EU commission, these stakeholders founded, in February 2017, on the Safer Internet Day, the "Alliance for a better protection of minors on the internet". Its predecessor was the CEO coalition for a better internet, which had emerged from the strategy with the same name for more protection on the internet, and which was now transferred into the Alliance. The road of self-regulation is increasingly used by the EU, because legislative proposals often turned out to be too slow and inflexible. So far, the Alliance has agreed on better enabling the users, to improve cooperation and to consider new technological developments, as well as supporting awareness.

A third pillar, next to the EU directives and regulations and the push for self-regulation towards a better internet, is the financing of European projects and measures, most of all through the "Connecting Europe Facility" (CEF). It also supports the Safer Internet Centres, which currently exist in 27 EU states, as well as in Iceland and Norway, and which carry out awareness raising campaigns (through the INSAFE network) and also support the fight against pornography and sexual exploitation (coordinated by INHOPE). Working together with prosecution authorities the centres already have quite a good success rate. 90 percent of reported content get deleted within 72 hours, however, the goal is complete deletion within 24 hours. The European Commission also coordinates the platform [betterinternetforkids.eu](http://betterinternetforkids.eu), which offers information about online-security and the Safer Internet Day for everyone.

## Code of conduct with the big players

Following the new German social network act, the EU, together with Facebook, Twitter, Microsoft and YouTube, has recently worked out a code of conduct<sup>4</sup>, which provides targets



*„The EU Commission aims for legislative measures (hard law) on the one hand and for self-regulation on the other hand. The self-regulation of the stakeholders clearly shows first positive effects.“*

Elisabeth Kotthaus, Deputy Leader of the Political Department of EU Commission Representatives in Berlin, responsible (inter alia) for consumer protection and digital agenda

<sup>4</sup> For details see: [http://europa.eu/rapid/press-release\\_IP-16-1937\\_en.htm](http://europa.eu/rapid/press-release_IP-16-1937_en.htm).



for the handling of illegal content.<sup>5</sup> Already after the first six months, positive changes could be seen. Especially Facebook has paid greater attention to incoming reports and has followed up on almost all critical content within the prescribed time limit. However, most services paid more attention to reports of so-called trusted flaggers<sup>6</sup>, whereas charges made by „normal“ citizens hardly get treated with the same vehemence, also the efforts of the other service providers lag way behind expectations. Nevertheless, according to Elisabeth Kotthaus, the EU Commission sees no need so far for a legislative initiative and will continue observing the development of self-regulation.

## Country Report: Estonia

In her report, Malle Hallimäe talked about education policy and legal measures aimed at achieving higher internet security in Estonia. Even though the topic has become more important in the last couple of years and media education is firmly integrated into the school curricula, according to Malle Hallimäe, the result is still not yet satisfactory.

Estonia is a highly interconnected country with a population of 1,3 million inhabitants and a high online activity. More than 90 percent of the population use the internet; more than four fifths of all households have an internet connection. In Estonia children and teenagers use the internet and digital devices very actively; almost all of the nine- to sixteen-year-olds are online on a daily basis. Children are around eight years old when they use the internet for the first time. Current surveys by Lastekaitse Liit suppose an even earlier start at around preschool age. In 2014 already more than a third of all six- to eight-year-olds owned a smartphone and among older children (12-14 years) it was even already 75 percent. However, according to results from the EUKidsOnline-Study of 2010 internet usage by Estonian children is seen as quite risky.

### Measures for more child protection

According to Malle Hallimäe, the topic of child protection online has become more important in Estonia during the last years. She positively emphasised the incorporation of teaching digital competence as a cross-sectional task into the national school curricula, starting in primary school and leading up all the way to the level of obtaining high school qualification. Such a curriculum also includes the topic of internet security and the safe use of online-services. Discussing the risks of online-communication, critically evaluating information taken from the net, learning to acquire ethical norms and behaviours, as well as getting informed about privacy protection are all part of it. In 2016, the Ministry of Education and Research developed a model

<sup>5</sup> The code, which is exclusively concerned with hate-messages, states that valid requests to delete illegal entries must be checked within less than 24 hours. Businesses are responsible to set up clear and effective procedures as well as their own verification teams to handle complaints. More information and the exact wording under: [http://europa.eu/rapid/press-release\\_IP-16-1937\\_de.htm](http://europa.eu/rapid/press-release_IP-16-1937_de.htm)

<sup>6</sup> These include for example the Safer Internet Centres and their members as well as other organisations or associations within media protection on European and national levels.



for pupils to assess their own media behaviour and to acquire digital competence through tasks and exercises.<sup>7</sup>

Additionally, children and parents shall be sensitized to questions of internet-security. This happens mainly through media campaigns and training courses, but also by means of especially organized advisory services, like for example the Safer Internet Centre.<sup>8</sup> Estonian Safer Internet Centre activities are joint initiative of four organizations: Estonian Union for Child Welfare (Lastekaitse Liit), Information Technology Foundation for Education, NPO Estonian Advice Centre (operating Child Helpline 116111) and Police and Border Guard Board. The Centre mostly organizes awareness raising activities on positive and safe use of internet and digital communication devices (workshops, seminars, campaigns) and works out different thematic educational resources. Via its partner Child Helpline 116 111 the Centre offers help and advice on internet usage to children, parents, and educators. Estonian Union for Child Welfare is operating web-based hotline service which is aimed at fighting against child sexual abuse material spreading online.

In addition to awareness raising and media education, stricter rules have been introduced in the criminal law in order to improve youth media protection. Most of all, this relates to cyber “grooming”, sexual enticement of minors and exhibiting violence against minors. Children and teenagers particularly accept the Estonian service of a web-police. These are members of the police who offer online advice and help for the whole population, but they are especially very popular among children and teenagers and are frequently consulted by them about internet topics. These members of the police are partners of the Safer Internet Centre, they also go directly into schools or offer trainings on internet security, also for parents.



*„In Estonia digital competence has recently been incorporated into the school curricula as a cross-sectional task. However, what is still missing is the appropriate training of teachers and also the support by parents.“*

Malle Hallimäe, Laste-  
kaitse Liit, Safer Internet  
Centre Estonia

## Stronger cooperation and solid financing necessary

Malle Hallimäe concluded that the topic of online security has made it quite to the top of the political and social agenda. In the case of the „Blue Whale” phenomenon, an online-game that calls for partly life-threatening actions, even the Ministry of Education together with the police sent letters to schools to inform and to appeal for preventive work. However, according to her view the efforts taken so far are still not enough. There is a lot of unnecessary duplication and overlap of activities, which means a better cooperation of agents is absolutely necessary. At the moment, the Ministry of Justice is working on an overview of all the activities and the people responsible within the different agents on the federal level. Besides, especially NGOs, which mostly are responsible for awareness raising, are in need of secure financing.

<sup>7</sup> Responsible for working out the model was the Information Technology Foundation for Education. This foundation is mostly financed by the Ministry of Education and it also designs teaching units dealing with online-security and is responsible for training teachers in media education.

<sup>8</sup> Safer Internet Centres currently exist in 27 EU-countries. They all stem back from the EU’s Safer Internet Program from 1999. Each Centre consists of an agent who focusses on awareness raising, a reporting office for alarming content, and a helpline for children, parents and educators. In Germany, these tasks are accomplished by the network “Saferinternet DE”, in which “klicksafe.de” acts as focal point for the awareness raising. Other actors in Germany are the so-called “Nummer gegen Kummer” (Helpline) and the German reporting office, run by organisations and controlling bodies of the internet economy as well as by “jugendschutz.net”, a common service of the Federal Government and the Länder.



## Putting teachers and parents into focus

Despite the incorporation of media education into school curricula, still there is less activity in schools. More trainings are needed for teachers to integrate digital media into lessons and about the topic of media education. Also, so far, there is still not enough support for the kids by their parents. They are often aware of online-risks, but they lag behind their kids. In many cases they do not know how to deal with the topic, do not understand the internet nor their children's activities. That is why many parents hold back when it comes to media education even though they are concerned. So it is urgently necessary to integrate parents more, best by means of the kindergarten and the schools.

## Country Report: Denmark

In his contribution, Christian Mogensen gave an insight into the work of the media education center and provided information about online-risks and solutions in Denmark. In doing so, he made clear that for him media literacy is the key to more online safety.

In Denmark, there are about 1,5 million children and young people, most of them are highly educated when it comes to media, but that does not mean that Denmark is free from problems with online safety. For example, there were indeed some concerns over the already mentioned Blue Whale game. But answers from children and young people showed that they rejected that game and the self-destructive actions it demanded. It was mostly the grown-ups who were worried because of the media coverage the game received. Under these circumstances, there was no need for special measures, because on the part of the children and young people simply no need for action was required. This approach is basically symptomatic for Denmark and the work of the Center for Digital Pædagogik.

## Addressing children and young people specifically

The Center was founded in 2004 as a helpline within the Danish Safer Internet Centre, whereby initially the children and young people came to the staff members with all their questions. Later, the helpline grew to become an online meeting point and gradually it involved the internet more and more as well, so that eventually in 2012 the Center was further developed into a knowledge center for digital issues. This includes a special online counselling and help service for children and young people. In order to specifically address boys, a separate website has been developed since 2014 to involve them more and to invite them to share their questions and views. The idea is to reach the boys through their topics such as football and competition, e.g. by awarding them high-score points for answering and asking questions or for using the page.<sup>9</sup> Targeting children and young people specifically has proven to be effective - especially among the boys, but in general, too.

<sup>9</sup> The website *mitassist.dk* has become the most popular helpline for boys in Denmark.



## Tightening the law against the distribution of sexual images

Concerning the internet risks, Denmark has to deal most of all with the distribution of sexual images as revenge porn, for example after a break-up. This also has to do with snap chat's high popularity in Denmark. Since about 2015, the Center's perception of this problem has risen significantly and it has also gained greater awareness in society and politics. In 2017, Denmark saw a tightening of the law, confining the sharing of sexual images without the consent of the affected people. To set a signal, the penalty for violating the obligation to obtain consent was quadrupled, so that imprisonment from two to up to four years, in severe cases, is now possible. The law intends that from the age of 15 years – the age of sexual consent in Denmark – sexual images or nude pictures may only be shared with one other person. From 18 years on, there is no longer a limitation of the number of persons, but the consent to distribute always needs to be obtained, and it can under no circumstances be given by a third party.

As crucial measures when it comes to online security in Denmark, Christian Mogensen named awareness raising and media education through NGOs, anonymous helplines and direct and indirect media education, but also a growing focus on political legislation. The Center is active in all of these areas and there is an increasing demand by parents, teachers and also children and young people themselves for media education.



*„In Denmark, most children and young people have a lot of internet experience and a healthy risk awareness. However, there is still need for action, mostly within media education.“*

Christian Mogensen,  
Center for Digital  
Pædagogik

## Information and media education in school

Despite good basic conditions and children being well informed, there is still a need for action in Denmark. A crucial area is the question of who is responsible for the media literacy of children and young people. Teachers as well as parents point to each other, even though media education is a solid part in the schools' curricula. However, up to now, teachers are not being prepared sufficiently for this task. Media education is not a subject in teacher training, so that many of them do not feel well prepared to tackle media topics and hence refuse to fulfil this task.

The increasing distribution of sexual images is also caused by many young people believing that it is normal behaviour among their peer group. Young people are convinced that up to 80 percent of their peers upload such images. In reality, it is only a minority of 20 to a maximum of 40 percent. What becomes clear here is how much the pressure to belong determines the online behaviour of children and young people, too. That is why it is even more important to clarify how easy it is to distribute these images widely, in order to reduce the number of simple followers. Moreover, victims of the distribution of sexual images are often criticised for making such images at all. However, it must be acknowledged that nowadays a great part of today's children's and young people's lives takes place online and that is obviously also true for their sexuality. In Denmark, there is a helpline that is devoted only to the question of how images that appeared on the web unwanted can be deleted.<sup>10</sup> It is known by around 90 percent of young people, as helplines in general have a vast reach of around 500.000 users per year.

<sup>10</sup> [www.sletdet.dk](http://www.sletdet.dk)



## Current need for action

Christian Mogensen concluded that legislative efforts can only be one part of the answer to online risks. In his view, media literacy plays a significantly greater part in reducing risky experiences. Particularly, the risks that are important to children and young people need to be focussed, but also the needs of parents and teachers, with the aim to allay their fears regarding the internet. In addition to these rather soft factors, concrete improvements are necessary, too, for example when it comes to the financial resources of public schools. The Center for Digital Paedagogik sees an increase of requests by teachers regarding media education training, but because of limited resources, these trainings can only be offered against payment, which for many public schools is hardly possible. Additionally, it would be desirable to have guidelines for the pedagogical praxis of media education in schools. So far, schools have to develop them themselves, but they lack the knowledge and the time to do so. Moreover, Christian Mogensen criticised the often insufficient potential for penalties. For instance, when a 14-year-old minor, who is not criminally liable, publishes pictures of his ex-girlfriend without her consent nothing will happen to him: there will be neither an expulsion from school nor any other, noticeable penalty against him. Difficulties also show up for the unauthorized distribution of images across country borders, there is hardly a possibility to have such pictures deleted there. Here, Christian Mogensen stated, a closer European cooperation would be extremely desirable and he also suggested a mutual exchange across Europe about new technological and content-related developments of the internet.

## Online security for children – Legislation and additional measures in Germany

In her contribution, Jutta Croll informed about the legal basis for youth media protection in Germany. She pleaded for a further analysis of the effects of children's rights guaranteed under the UN Convention of the Rights of the Child (CRC) regarding participation and protection of children in times of the internet. She also underlined that laws and technical means of protection can only be part of an overall protection concept, which has to be supplemented by teaching media literacy. According to Jutta Croll, the protection against risks is a right which derives also from the UN-CRC.

In Germany, both political levels, the federal as well as the Länder level, are simultaneously responsible for child protection in the web. Crucial content-related questions are especially regulated by the Federal Youth Protection Act (Jugendschutzgesetz) and by the Interstate Treaty on the Protection of Minors in the Media of the Länder (Jugendmedienschutzstaatsvertrag). These fundamental media laws are, according to Jutta Croll, complemented by further legal regulations, such as the still very new Social Network Act (Netzwerkdurchsetzungsgesetz), or also by links to the social security sector (Kinder- und Jugendhilfe). In addition, there is European legislation, as for example, the audiovisual Media Directive and the EU General Data Protection Regulation. The German legal framework for the protection of children and young people on the internet is flanked by supranational law, like the UN Convention of the



Rights of the Child, and the Lanzarote Convention to combat sexual abuse of children. All these regulations address the various aspects of protection in different ways.

## Limiting access and blocking inappropriate content

So far, measures for youth protection have primarily addressed internet content inappropriate for children and young people by the Youth Protection Act and the Treaty on the Protection of Minors in the Media. The laws distinguish between content which jeopardizes development and content which is absolutely inadmissible. While usually in the first case an age-specific limit to access is put into use, for example in the case of television by choosing the broadcasting time, absolutely inadmissible content leads to a complete distribution ban. The content evaluation is carried out by various organisations on different levels, for example by the federal department for media harmful to young persons (Bundesprüfstelle für jugendgefährdende Medien) or self-regulation organisations. Depending on the way in which the content is distributed, it either falls under the regulations of the Youth Protection Act, which registers content on usually concrete, physical media such as DVDs or films, or it falls under the regulations of the Treaty on the Protection of Minors in the Media, which addresses the distribution by so-called tele media. Because content is increasingly distributed through different channels at the same time, the aim is to converge existing regulations, for instance in the course of the intended revision of the Youth Protection Act. Also, the new social network act is an attempt to fight against illegal and dangerous content, such as incitement to hatred and violence or racism.

Also, in order to protect children and young people from being confronted with inappropriate content, a special protection software can be installed onto the end device, such as a computer, smartphone or tablet. In Germany, this kind of software must be approved before distribution, which is also regulated by the Treaty on the Protection of Minors in the Media.<sup>11</sup>

## Protection against contact risks

However, the existing measures, technical tools and legal regulations address the manifold risks for children and young people which can occur from online contact to unknown persons, only insufficiently. Especially chats are very risky, because one never know who really sits on the "other side". Other contact risks to children and young people arise from providing personal data, especially during video-chats as well as by live-streaming and simultaneous chatting. During chatting, participating persons can also actively seek to influence the acting of children and young people in front of the camera. At the moment, there is hardly anything that can be done technically to handle such contact risks. Automated monitoring, which blocks the content in case relevant words appear, leads in real-time transmission at least to a slight delay, which usually will be noticed and not tolerated by users. A possible protective measure on the provider's part would be the moderation of all chats by staff. For highly fre-



*„Laws and technical tools are an important contribution to more internet security for children and young people. But educating about risks and providing children, parents and pedagogic professionals with media competence is also necessary, so that no protection gaps remain. Additionally, in order to understand the internet's opportunities and risks more from the perspective of the child, children's rights regarding the web should also be reinterpreted.“*

Jutta Croll, Stiftung Digitale Chancen (Digital Opportunities Foundation)

<sup>11</sup> On the European level, such software was tested in the SIP Bench III Project. The results show that the detection and filtering of sexual or pornographic content is quite high when they are distributed in English; the results in other languages and with other content such as racism, violence or Hate Speech are significant lower. The complete results and the tested products are available under: [www.sipbench.eu](http://www.sipbench.eu).





quented services, this would mean high personnel expense. Therefore, it must be evaluated whether a legal obligation to such measures, which so far do not exist (yet), could solve the problem. Education and awareness raising with children and young people are also necessary to reduce contact risks.

## Data protection and privacy

Data protection is addressed predominantly in the EU General Data Protection Regulation, which will come into force in all European countries on May 25th in 2018. What is relevant here in regards to the protection of children and young people, is especially the introduction of an obligation of parental consent or the consent of legal guardians when children and young people under the age of 16 use "information society services", which was already mentioned in Elisabeth Kotthaus's contribution. However, until now, there is no clear definition, which services in fact fall under this regulation. The GDPR gives EU member states the opportunity to lower the age limit nationally down to 13 years. But, at the moment, it is neither clear whether the legal regulation will apply to the child's place of residence or the location of the service provider. Answers to these questions are in the interest of all stakeholders involved, including the businesses, which will have to develop the technical tools to ensure legally binding identification of young users and authentication of parental consent. In view of this and other open questions, there are expert meetings taking place in Germany right now, which will lead to a roundtable at the beginning of 2018 to discuss questions regarding the implementation of the General Data Protection Regulation. So far, it can be assumed that in Germany, at least when the regulation will come into force in May 2018, the obligation of consent will be necessary up to an age limit of 16 years.

Moreover, the General Data Protection Regulation intends to strengthen the protection of children against so-called profiling (recital no. 71), hence, taking into account that children rarely are aware of the consequences of their online acts and the potentially resulting data protection risks. In addition, the regulation demands a clear and for children and young people understandable explanation of the processes of surveying, saving and processing of their data. Also, information education about the purpose is obligatory, so that children know what happens to their data, which they provide voluntarily or involuntarily, for example through location detection (recital no. 39, art. 12).<sup>12</sup>

## Commercial risks

Both regulations mentioned, the Interstate Treaty on the Protection of Minors in the Media and the Youth Protection Act, also address commercial risks, which can result from internet use, and aspects of distributing advertisement to children and young people. Other initiatives are self-commitments of the media and advertising industries within the German Advertising Standards Authority. The General Data Protection Regulation considers this risk as well by limiting the processing of user profiles for advertising purposes and by demanding special protection of

---

<sup>12</sup> A good example from practice of what this understandable wording may look like is shown here: [www.jugendsupport.de](http://www.jugendsupport.de).



children in this respect (recital no. 70ff). The previously mentioned audiovisual Media Directive (AVMSD) also includes measures for the protection of children and young people against unsuitable advertisement. However, there are some areas which are not covered by the existing protection laws. There are, for instance, the so-called „unboxing-videos“ on YouTube, which show children and young people unwrapping objects and which are usually to be seen as product placement, but which are currently under no regulation at all. Apps, too, could hold commercial risks, especially if they are financed by In-App-Purchase. A study by “Stiftung Warentest” and jugendschutz.net have shown, in the first half of 2017, that there is currently no App that can be unconditionally recommended for children.

## Sexual abuse and violence

Relevant regulations dealing with punishable offences such as pornographic and especially child pornography material are included primarily in the German Criminal Code. Here, an amendment of § 184b, that came into force in January 2015, led to an intensification regarding the inadmissibility to distribute certain forms of posing images of children at the age of under 14 years. With regard to the internet, additionally, the new social network act, which will come into force in October, demands from internet service providers to delete illegal content within the shortest period of time, in order to prevent the distribution of such images. Other pornographic material is subject to age restriction and may only be made accessible, as mentioned before regarding unsuitable content, after appropriate age verification. Germany, according to Jutta Croll, is also committed to comply with the Lanzarote Convention, an agreement of the European Council, which aims at protecting children from sexual exploitation and sexual abuse.

## Digitalisation and the child’s rights perspective

To further address the topic, Jutta Croll encouraged the reinterpretation of the rights in the UN Convention of the Rights of the Child with regard to digitalisation. Die UN-CRC was ratified by the United Nations in 1989, the same year the program code of the WorldWideWeb was developed, which made the internet accessible for everyone. Back then, today’s almost natural use of the internet as an everyday medium by children and young people could not yet have been foreseen. From the perspective of children’s rights, new questions are raised about the protection and about the freedom rights of children and young people.<sup>13</sup> This does not only involve internet risks, such as the protection against sexual violence, but also the new digital opportunities of better participation, for example in regard to the right to information and freedom of expression but also to freedom of assembly and the right to free time and play. Not least, from the guaranteed children’s rights in the UN-CRC a right to media education and media literacy, to the protection of privacy and to safety in the net can also be derived. A group of experts at the European Council, the so-called CAHENF-IT, is currently working on recommendations for newly interpreting the UN children’s rights in regards to the digitalisation of children’s everyday lives. They are to be passed by the Committee of Ministers of the European Council in January 2018 and then implemented by the 47 member states.

---

<sup>13</sup> More information on this aspect under [www.kinderrechte.digital](http://www.kinderrechte.digital)



## What does it need to make the internet a safer place for children and young people?

**John Carr** pointed out that the discussion about online security for children and young people suffers from two fundamental problems. On the one hand, it is often forgotten that children and young people are not a homogenous group. Rather they possess different abilities and knowledge, even within the same age or social groups. Therefore, generalizations in the discussion about a safer internet have to be questioned. Creating a one hundred percent safety online is impossible. But even if the solutions were tailored to suit the vast majority of children and young people, a large number of children would still remain in need of other, more specialized measures or instruments. Therefore, when it comes to measures create a safer internet finding solutions which work for the largest number of children is not good enough. Every child and young person has to be considered. On the other hand, the shortage of usable data is highly problematic. Even the comprehensive study EU Kids Online only provides data from 2010. But the internet has continuously changed since then, many businesses and services do not exist anymore and new ones have taken their places. When it comes to media content, offers, and use etc., studies so far only allow a glance backwards into the past but basically none into the current state of the art.

### Businesses' low sense of responsibility

In order to illustrate the difficulties of cooperating with internet businesses, John Carr talked about a study on children's and young people's concrete experiences with various social platforms such as Facebook, and others. He and Sonia Livingstone, who is also responsible for the EU Kids Online study, as well as other researchers were part of the study's group. They knew from several previous studies that children and young people stated repeatedly that it was not so much the content of these platforms that concerned them but rather the experience that, when they did report problematic content, they did not get any feed-back on the process or the effects of their reports. This led children to believe their experience does not count. Whatever they do or whatever they report it makes no difference so eventually they don't bother reporting at all. Because of this phenomenon, a sub group was convened together with providers of social platforms to study and improve the course of action after reports had been made. However, in total only three businesses agreed to participate: Facebook, Disney and the communications service provider Telefónica,. A few weeks later, Telefónica dropped out: claiming the business had too little capacity to deal with the topic and generally too much to do right then. In the end Facebook ended their cooperation and involvement. The company's headquarters issued a statementsaying they would only provide information if there was a legal obligation to do so. Even though the study took place on behalf of the British government, the data was considered to be "commercially sensitive". So, the research project failed. Looking back to this experience, John Carr asked whether sensible internet policy making was possible at all without any access to relevant, current information. The minimum requirement for a secure internet is business transparency and sense of responsibility. Governments and NGOs must know what happens on the internet in order to develop meaningful measures.



## Failure of the system

Solutions like the ones discussed here try to make the best of the prevailing circumstances, but the circumstances are fundamentally wrong and in the long-term not sustainable for a safe internet. John Carr did not exclude that even liberal democracies might conclude, that under the prevailing conditions of a chaotic, unpredictable internet, businesses will never employ enough personnel or develop suitable technical instruments to effectively fight dangers, and that therefore neither the businesses themselves nor the police can master the internet. For years now, no police force in the world has been able to stem the vast amount of child pornography on the internet. Also with other risks a similar powerlessness is apparent, too. Most potential dangers result from user generated content and from the platforms that then distribute it. In light of all this, John Carr considers it not unlikely that governments might decide to act here, because the risks for children are unacceptably high. Governments might see the internet, as it is now, as failed and therefore could consider resetting it from scratch.

Unaffected from such a reset would probably remain the online business models such as amazon, eBay or PayPal, which pose relatively low risks for children and young people. In contrast, user generated content would probably be reduced considerably, fuelled by terrorism and hacker attacks like the recent one on Britain's health care system. Of course, one could argue that, by doing so, governments would curtail the fundamental right to freedom of speech and exercise censorship, however, the internet is not an essential good. Hence, it does no longer seem impossible that the moment of a reset might soon be reached. The uncooperative behaviour of Facebook and other internet businesses' mentioned earlier, further encourages this possible development, whose first signs are already becoming apparent.

Martin Schmalzried of COFACE-Families Europe saw instead some chances in developing a common European course of action. He named politicians and internet businesses, as well as civil organisations like NGOs, and the users themselves, as key players for a better online protection for children and young people. From the perspective of his organisation, the foremost obligation of political decision-makers lies in establishing laws that stronger regulate the internet economy, but that also prevent phenomena like society's digital divide by age or social groups. Martin Schmalzried emphasized that big players like Google, Facebook, YouTube, Twitter and others have great influence on the online behaviour and experiences of children and young people. In this context, Families Europe supports EU regulations because many businesses operate internationally and member states alone often lack the power and the influence to have an impact on the internet economy, which is especially true for smaller states. Measures and laws would gain more weight through joint action from all of the EU. At the same time, member states could influence these measures on EU level and introduce their own topics and experiences, mostly through the council but also through the EU parliament, which is made up of national representatives. These opportunities should be used more to urge the EU to act more thoroughly when it comes to online child protection.



*„It is entirely possible that the internet as we know it might soon be over. Because of the industry's apparent inability to manage and control some serious risks, governments might conclude that a complete reset is necessary.“*

John Carr, eNACSO  
(European NGO Alliance  
for Child Safety Online)



## Better regulations on EU level

Martin Schmalzried saw imperfections subsist in current EU regulations. Looking at the Audio Visual Media Directive, which has been mentioned several times before and which is currently under revision, Families Europe demanded much stricter advertising regulations concerning children. Existing regulations that already apply offline, as for example for television, should be transposed in some way to the internet. This includes, for instance, limiting the maximum duration of advertising to 20 percent per hour of broadcasting time, which, however, has not yet been included into the recommendations of the commission. Hence, children and young people are still exposed to limitless advertising on the internet. Also, the content of advertising has to be restricted to protect children. This especially relates to advertisements for unhealthy products or that show gender stereotypes. Overall, many internet services with audio-visual services do not get covered by this directive because they do not place a special focus on their video services. Moreover, jeopardizing content and the fundamental approach for dealing with it remains an important question, especially when it comes to audio-visual services.

Also, he stated, the General Data Protection Regulation leaves out certain problems completely and does not go far enough on many issues. In contrast to this regulation, Families Europe stands up for a fundamental reorganisation of how to deal with personal data. They should no longer lie in the hands of the different social platforms, but should be uploaded from the users to a general cloud. The users themselves could then give various providers access to them, eventually restrict this access right or cancel it again easily. This would enable the users to much more control over personal and published data. At the same time, such an approach allows a better exchange of texts, images etc. between different providers. However, this approach contradicts the goals of internet businesses. So far they strive to collect as many data as possible and to fully bind users to their service, their formats, and terms and conditions. There is only one case in which such a comprehensive data portability already exists: emails can be sent and received independently from the actual account provider. But, so far, the social platforms do not follow this concept.

## Limiting data collection and advertising

Also, the problem that data processing is increasingly dependent on algorithms has so far been taken into account insufficiently. The use of data by computing processes and self-learning machines leads to decision-making processes becoming less and less directly controllable. The GDPR clearly remains too weak when it comes to questions of who is responsible for decisions in these cases – which can indeed be quite serious, for instance with concessions of insurance policies, indexed health risks etc. – and how these automated decisions will be controlled. Martin Schmalzried argued that such decisions should not be made automatically and human appraisal should always be provided.

Instead of the planned parental consent concerning data transmission of minors under 13 or up to 16 years, there should be a general ban of the transmission of children's data below a certain age. In this way, their data and information would be protected regardless of their parents' con-



sent. However, major difficulties can be expected, because Facebook, for example, generates a lot of money by collecting and passing on data. Moreover, agreeing on a common age limit within the EU is already difficult right now and there is the danger that children themselves evade the ban by indicating a wrong age when prompted for. The problem of increasing personalised advertising should basically be tackled, too, by enabling every user to simply deselect advertising. But many business models in the internet are based on advertisement and it had to be made clear what would happen to them if everyone could really reject these advertisements.

## Child protection vs. business interests

For Families Europe, the next urgent step is to take a precise look at responsibilities in the internet. Here a distinction needs to be made between centralised and decentralised providers. Centralised providers like Facebook, YouTube etc. offer internet services on the basis of a business model with self-imposed conditions and standards. Therefore, securing compliance with these standards necessarily belongs to their natural business tasks. However, the providers often lack the structures needed to enforce their standards in practice. Martin Schmalzried underlined that it is the businesses' responsibility to implement their own standards and that therefore, they are also obliged to undertake necessary interventions, like deleting content which violates their community standards.

Decentralised providers, who are open to everybody's active participation, processes and content cannot be centrally moderated or deleted. Therefore, democratic structures are important, which exert a certain pressure and allow moderation or if necessary censorship from inside. Wikipedia is a positive example for this effect.

However, the idea of protection often gets into conflict with business interests in the internet. For example, Families Europe has proposed a feature that would allow private access only to children's posts after a certain time period. But businesses like Facebook reject this because their business model is based on the permanent display of as much personal information as possible. Facebook's increasing use of algorithms to filter according to preferences and interests is alarming, too. These algorithms could lead to so-called „filter bubbles“, which only echo present views and therefore threaten plurality and democracy. Considering these conflicts, creating a safer internet for children and young people is still a great challenge for politics, businesses, civil organisations and for the users themselves. The debate about it has thereby not only to address the interests of children, but, more fundamentally, also the role of general interest and democratic principles in the internet.



*„European regulations have to be pushed forward because the internet does not stop at national borders and many of the internet service providers are international businesses. Actions carry more weight if a European alliance of member states stands behind them.“*

Martin Schmalzried,  
COFACE-Families Europa



## Discussion and first conclusions

During the various inputs as well as during the requests and the final discussion, two instruments were discussed as crucial for a better protection of children and young people on the internet: a reasonable legislative regulation and a high media literacy. During the final discussion, the participants talked mainly about the appropriate balancing of these two instruments but also identified important key players and further areas of action for a better online protection. They especially focused on the involvement of businesses to achieve more transparency on the internet, but also on the role of teachers and parents for the necessary media education of children and young people.

Several participants pointed out that the internet's fast-moving development considerably complicates an anticipatory approach and proactive legislation to the topic of internet security. This leads to a hardly solvable contradiction, trying to keep up with the changes as well as aligning the media policy measures with future changes. Moreover, the discussions about media education in schools and families showed that also the adult generation has to be taken much stronger into account regarding the educational measures. Between the generations, there is often a wide gap when it comes to the use of digital media and the knowledge about it. In many families, cutting across all socio-economic milieus, there is a lot of uncertainty handling media literacy topics.<sup>14</sup> As shown in the country reports from Denmark and Estonia, the situation of the teachers is similar. The introduction of media education as a cross-sectional task in schools can obviously not change anything when accompanying measures are missing.

Criticised was not only the collecting of comprehensive data from users of digital services but also the power resulting from it as well as its increasing concentration among a few internet businesses. Despite the quite depressing scenario which John Carr had painted in his input, regarding the involvement of businesses, the German social network act was acknowledged as a first step towards more transparency and towards a stronger commitment of service providers. Actually, the law has not yet been passed, but the initiative itself and above all the demand to lay open the numbers of users allows for the hope for more pressure to achieve transparency.

During the discussion about risks and misconduct on the internet, some differences in basic attitudes showed up among participants. On the one hand, it was noted that the aim to minimize online risks for children and young people should not lead to over-regulation because the same activities would just move on to other providers or platforms. Many of the things that cause problems there, like sexual images or mobbing, are expressions of normal, adolescent behaviour, which gets predominantly criticised and judged by the older generation. Over-regulation and prohibitions do not help; they only prevent learning and a comprehensive media education. This view was countered by saying that the experienced risks could not be

---

<sup>14</sup> There has been a recent report in Italy about the use of social networks of families and their members. The report will soon be published, an English translation will presumably follow. More information at Centro Internazionale Studi Famiglia, <http://cisf.famigliacristiana.it>, or through AGF.



defined as simply part of adolescence and growing-up. Yes, children and young people do inconsiderate things, however, a relaxed attitude towards the effects, for example, of sexual pictures is unacceptable. There was stated a significant difference between risky online behaviour today and doing risky things in earlier days, as, once published, pictures or alike can hardly be removed from the internet and remain public for years. Such a laissez-faire approach is exactly what many businesses advocate for as well. Regulations, like age limits, do not guarantee better protection, however, they are at least an attempt to improve the current situation of children and young people. Finally, a responsible solution also has to be found for families or children, who, for whatever reasons, can not be reached by media education. Still, the consensus was that there cannot be an either or, but that regulation and media education are both important parts of a strategy for a safer internet. To create more safety online, the interaction of all stakeholders, each in their specific area of action, is necessary. However, a certain criticism of judging the online behaviour of children and adults cannot be denied, because often double standards are applied here.

In regards to regulations on a European level it was suggested to face the reality that, especially online, children often use services that were not made for them. It should be ensured that providers cannot withdraw from their responsibility by arguing that their service was not designed for this young target group. This reality needs to be addressed right through all medias, but especially for the internet. It was also suggested that NGOs should become more involved in European policies and make clear the need for regulation to the EU commission.

Also, it was considered necessary to bring parents much closer to media literacy topics. The discussion focussed mainly on creating interest and awareness for their children's online activities and to make media literacy a family topic. In Germany, the Ministry for Family Affairs is currently trying to sensitize families for media topics and to exchange their ideas of a reasonable media use, via so-called family laboratories.<sup>15</sup> In addition, the demand was made to engage children and young people in the search for suitable measures for more safety online. They should be asked which expectations they have, especially when it comes to the role of their own parents. The children should be able to make clear which questions they are concerned about in regards to their experiences with the internet and which information they need. It was mentioned that, in order to bring children and also their parents into contact with media topics and media professionals, it would be most promising to meet them where they already regularly are.

At the end of the discussion, the AGF's family organisations announced they would continue to actively participate in the debate for more online security, to search for own positions regarding a safer internet for children and to continue the exchange with stakeholders of different levels. In this way, the family organisations will play their part to support and strengthen families and children facing the digital challenges.

---

<sup>15</sup> The kick-off-event for the family laboratories took place only after this expert meeting. Information to the topics and to the concept can be found at: [www.familienlabore.de](http://www.familienlabore.de)





## Related Links

### Europe:

**EUKidsOnline, background information and results:**

<https://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx>

**GlobalKidsOnline, background information and results:**

<http://blogs.lse.ac.uk/gko>, <https://www.unicef-irc.org/publications/869>

**EU Strategy Better Internet for Kids:** <https://www.betterinternetforkids.eu>

**European Safer Internet Centres (INSAFE und INHOPE):**

<https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope>

**General Data Protection Regulation:**

[http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

<https://gdpr-info.eu/> (detailed information, though not an official EU website)

**Audiovisual Media Services Directive and current revision:**

<https://ec.europa.eu/digital-single-market/en/audiovisual-media-services-directive-avmsd>

<https://ec.europa.eu/digital-single-market/en/revision-audiovisual-media-services-directive-avmsd>

<http://eur-lex.europa.eu/eli/dir/2010/13/oj>

**Survey to technical control tools:**

[www.sipbench.eu](http://www.sipbench.eu)

### Germany:

**Basic laws for the protection of children online:**

<https://www.kjm-online.de/service/rechtsgrundlagen/>

**Safer Internet Germany:**

<http://www.saferinternet.de>, <http://www.klicksafe.de>, <http://www.jugendschutz.net>

**Help and advice service for children:**

<http://www.jugendsupport.de>

**Search engine for children:**

<http://www.fragfinn.de>

**Family labs of the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth:**

<http://www.familienlabore.de>

November 2017

Association of German Family  
Organisations (AGF) e. V.

Edited by:  
Ivonne Famula, Sven Iversen

Translation:  
Marco Atlas

Photo Credits:  
Title - patat / shutterstock.com  
AGF e. V.

Layout & Typesetting  
manuka.p.r



The AGF campaigns for the rights and interests of families in politics and society. It supports the cooperation of organisations and stakeholders for families and those responsible in family policy on a national and international level.

**Contact and Information:**

**Association of German Family Organisations (AGF) e. V.**

**Karl-Heinrich-Ulrichs-Str. 14  
10785 Berlin**

**Fon: + 49 (0)30 2902825-70**

**Fax: + 49 (0)30 2902825-89**

**E-Mail: [info@ag-familie.de](mailto:info@ag-familie.de)**

**Web: [www.ag-familie.de](http://www.ag-familie.de)**

The AGF Expert Meeting was supported by



German Family Association (DFV) · Protestant Working Group Family (eaf) · Catholic Family Association (FDK)  
Association for Single Parents (VAMV) · Association of Binational Families and Partnerships (iaf)