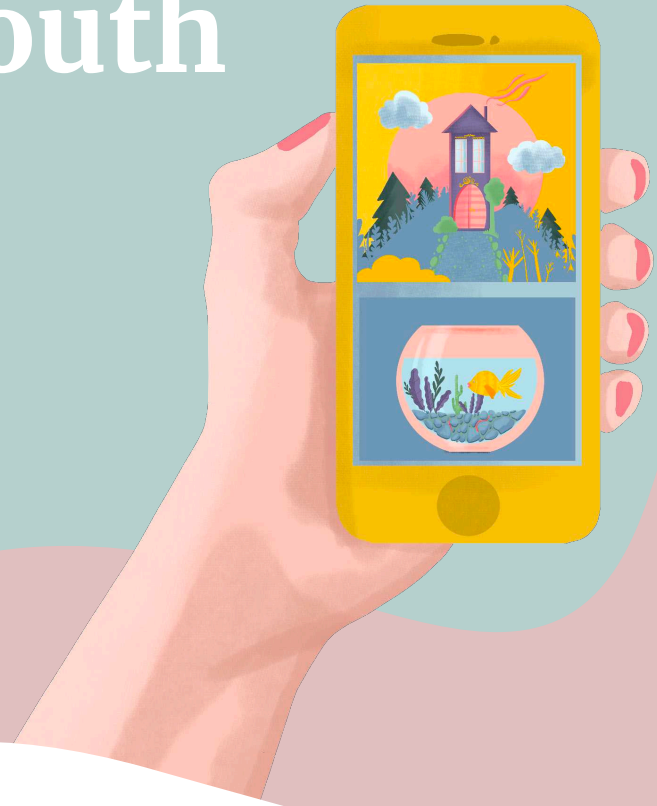
Safer Internet for Kids and Youth



Partners

elf

INSTITUTE FOR POLITICS AND SOCIETY

FRIEDRICH NAUMANN FOUNDATION For Freedom.

IMPRESSUM

PUBLISHER:

European Liberal Forum (ELF)

AUTHORS:

Martin Kožíšek, Martina Viewegová, Jan Kolouch, Kamil Kopecký,

Yana Humen

FOREWORD:

Dita Charanzová

EDITOR:

Institute for Politics and Society

ILLUSTRATION + GRAPHIC DESIGN:

Hana Mára

Year: 2021

Published by the European Liberal Forum asbl with the support of the Institute for Politics and Society and the Friedrich Naumann Foundation for Freedom. Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the authors alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum asbl.

CONTENTS

Dita Charanzová
Vice-President of the European Parliament, Ambassador of the Safer Internet Project CR

FOREWORD

Online safety presents a growing concern as well as a challenging political goal of the modern digital era. We see how easily fake news is spread among people, how social media can affect public opinion, and how new digital tools change the things we used to take for granted. Despite these risks, I remain a committed advocate for digital technologies and solutions, and have worked for years to establish a borderless internal, digital market within the EU. I support and encourage European business to grow and believe in the big future of artificial intelligence. However, while our work continues on this path, we must also develop proper rules and mechanisms in order to ensure the safety of at-risk internet users – among which the most vulnerable are children. Such

safety is paramount to me not only as a politician keen on new technologies, but also as a mother of two small daughters. For me, this topic is one of the most important issues on the table, and I am therefore delighted to see that efforts are being made to strengthen these protections for our most vulnerable users.

A number of different pieces of European legislation include tools to help protect children online. For example, the Audiovisual Media Services Directive implements age barriers on streaming sites, and the new Digital Services Act (DSA) provides additional tools in this fight for online safety.

The first includes standardised regulations for the identification (Flagging) of content as well as rules for the flagged content's subsequent removal. Together, both of these regulatory mechanisms should greatly increase the removal speed of flagged content, therefore reducing their impact on vulnerable users. While the text will deal primarily with illegal media including child abusive content, most platforms are likely to apply the system beyond these parameters to include any content that is deemed harmful to children. For example, media deemed only acceptable for adults will not be permitted on children's websites under these new terms and conditions.

In order to ensure comprehensive effectiveness, the DSA will go beyond concrete regulatory instruments by encouraging platforms to take proactive measures against illegal content. Under the DSA, platforms will have greater legal protection in order to adopt voluntary filters to takedown content quickly, including measures which allow sites to act without prior notification. This so-called "good Samaritan" clause is intended to facilitate self-policing based upon a transparent enforcement system. Such measures will serve to protect freedom of expression and trade while simultaneously helping to combat the sale of unsafe products as well as the dissemination of unwanted content.

Finally, the DSA provides the option to establish legally binding Codes of Conduct for individual sites which will address "systematic risks" to be agreed upon by large platforms and the European Commission. Included within such "systematic risks" are any negative effects on the rights of the child as set down in Article 24 of the Charter. Under this directive, any platform which has elected to designate its site as safe for children must apply the necessary safeguards or risk fines and sanctions by the Commission. While the language contained within these regulatory codes must be carefully authored, they should also be strong enough to grant the legal grounds necessary to compel platforms to take action against content judged harmful to children. To this end, civil society must be involved to ensure that these codes are created and are widely respected.

Altogether, the Digital Services Act has the capability to provide valuable protection for children online. This protective capacity constitutes a crucial part of the wider DSA legislation, and though the act must balance the rights and responsibilities of all internet users, we have the responsibility to ensure that children are not lost in this discussion.

We must also develop proper rules and mechanisms in order to ensure the safety of at-risk internet users – among which the most vulnerable are children.

Martin Kožíšek
Head of the Safer Internet Center Czech Republic, CZ.NIC, z.s.p.o.

Martin Kožíšek

CHILDREN, PARENTS AND DANGERS ON THE INTERNET

Today's children are often said to be ahead of their parents with regard to technology. Children today are growing up with the Internet and other modern technological amenities. Do we, as parents, have a chance to protect them on the Internet? What are the biggest dangers that children face?

It is impossible to put together a simple manual, according to which the parents could learn how to protect their children in cyberspace. Parents do not have time to keep up with technology the way children do. However, parents who do not foster an open dialogue with their children about Internet safety are putting their children's safety at risk. It was noted that when children face an online threat, only two percent of the children

would go to the parent. Although parents often do not keep up with the technology, they should at least talk to their children, not only about school issues, but also about Internet issues. By fostering trust with their children, parents are better equipped to protect their children.

Some parents cut their children off from technology, as a preventive measure. However, this may not be effective, as the Internet is certainly an invaluable great tool. The Internet as such is safe, but what makes it dangerous are the people who misuse it. The generation of parents, who grew up without the Internet, has two worlds (online and offline) and still separates the two. Today's children have only one world, and technology and the Internet are part of their daily lives.

Children who are cut off from technology are, paradoxically, a very easy target for predators. When asked, "What is the biggest danger to our children on the Internet?" many would answer that predators are the biggest danger. We have been hearing about Internet predators quite often lately.

However, there are very few real predators in the virtual world who can physically harm children. There are far more ordinary people who hide behind the anonymity of the Internet and just seek to spice up their sex life. One stereotype is that the Internet predators are paedophiles or elderly guys. However, the number of paedophiles´ attacks on children in cyberspace does not exceed 0.1 percent of cases. The most common attackers who approach children on Internet are in fact 17–25 years old and are mostly from their neighbourhood. Today, in the context of the Internet, the term "predator" mostly refers to "cybergroomer". The cybergroomer uses virtual communication means or other technologies to evoke a feeling of trust in children (or young adults) through a false identity in order to lure them into meeting and to abuse them.

In the Czech Republic, which is one of the European leaders in the field of prevention of dangerous behaviour on the Internet, a number of projects have emerged in the past. These projects have drawn attention to the dangers associated with the use of the Internet – even before Facebook or other social networks have emerged. Nevertheless, it was the rise of social media that brought dangerous Internet behaviours to the fore. Notable documentaries which deal with predatory behaviour on the internet include Seznam se bezpečně (Meet Safely) and V síti (Caugt In the Net), the movie Na hory (To the Mountains), or the series #martyisdead, which even won an international Emmy Award in 2020 for the Best Internet Web Series1[1], which was dedicated to cyberbullying. There are also several significant local projects in the Czech Republic dedicated to prevention, education or intervention, such as Linka bezpečí (Children's Helpline), Dětské krizové centrum (Children's Crisis Center) or the project of Palacký University in Olomouc, E-bezpečí (eSafety).

SCOUT LEADERS PIŠKOT AND MELUZÍN

Probably the most well-known case of cybergroomerism in the Czech Republic was the case of Scout leaders nicknamed Piškot (Sponge Biscuit) and Meluzín (Howling Wind) from the Czech city Ústí nad Labem. This is one of the largest documented cases of child abuse in Czechia. The Boy Scout leaders led the boys' division. At first, the Scout leaders wanted to get the boys' personal information and later erotic materials. The way in which these materials were obtained can be described as one of the most sophisticated ways of manipulating by using modern information technology.

Under false girls' social media accounts, the Scout leaders "friended" the boys on social media accounts. They communicated with them through the network and later obtained their erotic photos and videos.

1 Czech serial #martyisdead wins country's first Emmy Award. Radio Prague International. 2020.

There are very few real predators in the virtual world who can physically harm children. There are far more ordinary people who hide behind the anonymity of the Internet and just seek to spice up their sex life.

The Scout leaders then blackmailed the boys with the embarrassing material in order to create even more material, under the threat of publishing their photos and videos. Soon, however, the material obtained in this way was not sufficient for them and forced the boys to create homosexual themed videos. They forced the boys to create videos in which they had sex with an older man and which they had to share with the Scout leaders within a certain time, under the threat of publishing their erotic materials. In total, 39 children were abused by the Scout leaders between 2007 and 2012, over the Internet or in person. According to the police record, they raped several boys, and some victims were abused repeatedly. The court sent the perpetrators to prison for crimes of rape, sexual coercion, sexual abuse, endangering the upbringing of a child, and the production of child pornography, for ten years and forbade them to work with children and young adults for the same period.

Although cybergroomer attacks are rare, their consequences may be fatal. Social media can be a breeding ground for groomers, where they can communicate with children through false and unverified identities. Statistics from the largest Czech social network operators found that 37 percent of attackers used fake identities and photographs that were commonly available on the Internet. Twelve percent of attackers used the photos obtained through communication with other users or from other profiles. The question therefore arises as to whether any restriction could limit this behaviour or eradicate it altogether. For instance, different age limits are set for the use of social networks in Europe. In the Czech Republic, this limit is set at 15 years. Nevertheless, this restriction is pointless in many ways, as children often get around it. In the Czech Republic, 52 percent of children under the age of 13 use social networks. Furthermore, the "social network" has not been clearly defined; it can be any service where one can create profiles and communicate with friends and work with the content in any way. Obviously, this definition already applies to most services, including YouTube.

A better way to control the network content would be to strengthen the role of prevention in families or schools and to put more pressure on service providers to deal with inappropriate content present on their network.

Social networks are undoubtedly a great tool. There is a widespread opinion among people who do not use any network, that users of social networks are mainly young people. Some social networks are indeed intended only for young people; however, the most widespread networks are dominated by an adult user base. We cannot, however, rely on the information that users provide about themselves on the networks. Recent research shows that almost 20 percent of network users do not provide accurate information. Users also stated in the questionnaires that they use more than one profile. Over 60 percent of network users even appreciate the possibility of using the network anonymously, for instance under a nickname.

The anonymity of the social network environment goes hand in hand with phenomena such as dating, partner search or sexting. There are many social networks or applications that offer anonymous entertainment and are very popular, especially among younger children, such as Snapchat, Chatroulette and others. It is these types of services that are far more likely to be prone to various predators.

POPULARITY OF SEXTING

The popularity of sexting is associated with the mass use of modern information technologies, not only by adults but also by children. The term sexting refers to the act of sending text messages, photos or videos with sexual content. There are two levels of sexting: exchanging similar types of messages with your partner or strangers. Both can be risky, especially in the latter case. However,

there are also cases where these materials are published by the partner after the breakup. We consider sexting to be one of the most dangerous behaviours, which can indirectly result in fatal consequences. In some cases, the victim is pressured, and this pressure can result in dishonesty, self-harm or suicide.

Although sexual intercourse is permitted by law in the Czech Republic from the age of 15, no intimate material (photographs, videos, stories, fantasies, etc.) may be taken of an individual until the age of 18. Otherwise, this content is then classified as child pornography and its production, distribution or handling is severely penalized. Nevertheless, sexting in the form of text is practiced by almost 25 percent of children or young adults; most of them rarely, while by eight to nine percent of children regularly. Sexting in the form of pictures and videos is practices by 15 and six percent of children, respectively.

Most children have been dealing with dangerous phenomena on the Internet since childhood, usually when they learn to communicate and write independently. Their parents' first attempt to protect them is often to set up parental controls. There are several solutions on the market that can filter out content that children can access online. Some controls are complex, allowing parents to monitor the time spent online and analyse the child's movement on the network. Also, as a parent, you can spend an evening by coming up with inappropriate words and pages where a child should definitely not go. Today's children, however, can often outwit such

restrictions. They can borrow a cell phone from a friend, connect to another Wi-Fi or find another way. It is necessary not only to entertain children, but also to be able to talk about what they do on the Internet or with whom they are chatting. Recently, we can observe the phenomenon when the so-called non-contact generation is growing up - that is, the generation of children who can communicate well through modern technologies but cannot cope with personal contact. And therefore, they escape into a more comfortable online world.

One of the topics that parents and their children should discuss is cyberbullying. Physical bullying and cyberbullying are closely linked. One cannot get rid of cyberbullying by unplugging the device. When a child is physically bullied, he/she is most likely to be bullied online as well. Unlike physical bullying, a child has no chance to anticipate cyberbullying, as it comes in many forms. The vast majority of cyberbullying originates as a failed prank, from insulting, sharing various pictures and videos, to more serious forms. The most serious forms can extend to various degrees of coercion or extortion. About 51 percent of children in the Czech Republic have experience with some form of cyberbullying and about seven percent of children have experienced coercion or extortion.

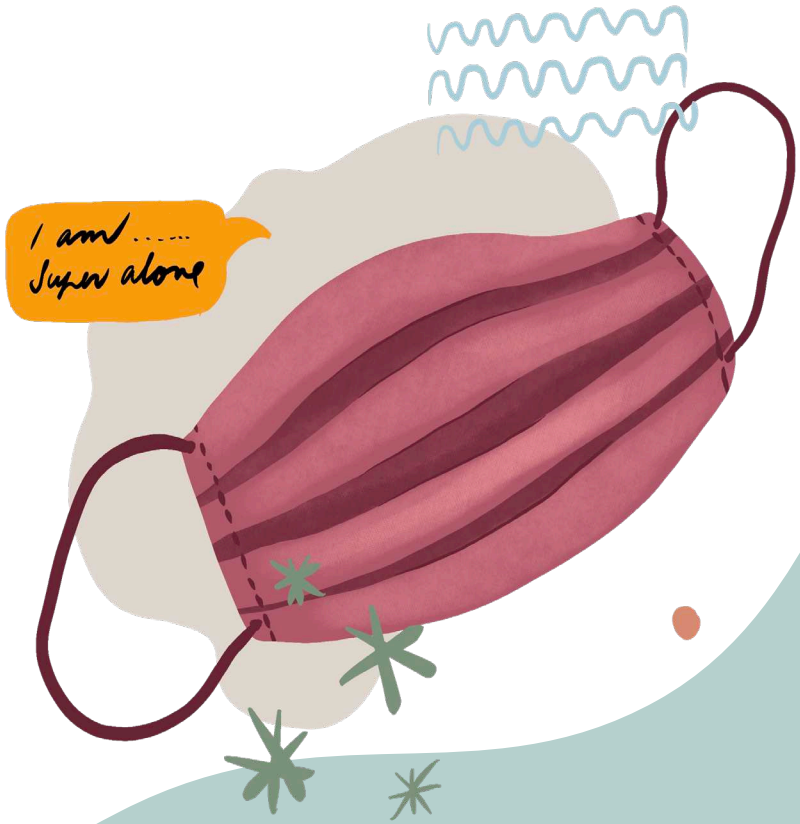
Parents turn to us quite often to report that their children are victims of cyberbullying. Cyberbullying is a crime. This statement, however, needs to be put into context. A criminal offense is an illegal act which the Criminal Code considers violating the moral standards of society and is defined in Code (§ 13, Art. 1). But what exactly

does that mean? To put it very simply, in order for an act to be labelled as a crime, it must be stated and described in our Criminal Code. Cyberbullying is any act intended to upset, harm, intimidate or otherwise endanger a victim using a modern information technology (especially the Internet or a mobile phone). We all suspect that cyberbullying is an inappropriate act, but it is not a crime. Cyberbullying as an act, it is not referred to anywhere in our Criminal Code. On the other hand, some manifestations of cyberbullying, for example, threats or blackmail, are already referred to in the Criminal Code and therefore these acts are prosecutable. Which means, although it is not possible to prosecute anyone in our country during the so-called cyberbullying, it is already possible for the individual manifestations of this phenomenon.

CHILDREN ONLINE AND THE COVID-19 PANDEMIC

During the COVID-19 pandemic, children spend far more time online, up to 25 percent of their day. Perhaps we used to want to spend more time with our children. This became our reality unexpectedly, so it unfortunately caused many troublesome situations, such as the escalation of various problems in families. The counselling lines report a 60 percent increase of children consultations regarding anxiety, depression, fear of illness and loved ones. Children quite often mention social isolation, worries about the future, and managing returning to school during their counselling sessions. The number of cases of domestic violence, disputes over children with divorced parents or the number of self-harms among children is increasing. The phenomenon of cyberbullying and its new form – digital ostracization – has also increased.

So far, we have discussed only a few dangers that children may encounter on the Internet: virtual environment, especially social networks, apps, games or messengers, and also dangerous behaviours, such as various forms of cyberbullying, sexting or blackmailing. However, there are more manifestations, and a number of new phenomena and forms of virtual dangers are emerging. If a child is the victim of some form of an attack, he may shut himself off and stop communicating. Quite often, parents can confuse this behaviour with the symptoms of puberty. Communication with an adolescent is difficult and there is no simple advice on how to easily overcome this difficult period of a child's life. But when it comes to protecting children in the cyber world, let's try to follow the advice given in the introduction. Trust between parents and their children is integral to a safer world. The parents might also want to consider showing their children the documentaries or series that explore issues like social media, Internet safety and cyberbullying.



Martina Viewegová
Psychologist at the "PSYCHOTERAPIE ANDĚL" in Prague, Expert on Children's Online Safety

PSYCHOLOGICAL ASPECTS OF THE RISKS OF THE ONLINE WORLD

— Martina Viewegová

From the point of view of human psychology, the virtual world is a challenge in all aspects. In the context of the development of the human psyche, this is a novelty. Scientific studies are currently underway on the impact of the virtual world on brain development. But how it will affect in the long run the human psyche, and especially the quality of interpersonal relationships. Only time will tell.

It is necessary to realize that the child is a digital native. For him or her, the virtual world is a reality that is full-fledged, as the real world is for us. In the real world, we are responsible for the children, our role is to prepare them for a quality life, and in the context of developmental psychology, to teach them that the world

is a good and safe place to live. Of course, it is our responsibility to prepare them for the pitfalls and risks and to give them good tools to defend themselves. It is similar to the digital world. We have a responsibility to educate the children about digital literacy, netiquette (etiquette in the virtual world) and to know what dangers may await them. And if they encounter them, they should know where to turn for help. With regards to cyberspace risks, we are going to focus on the possible impact on a child's psychological development in the context of cyberstalking, cybergrooming, sexting and cyberbullying.

A frequent occurrence common in all these phenomena is not knowing the perpetrators of this activity. We do not know whether there is one perpetrator, whether more people are involved, whether he really hides behind a profile that also belongs to our acquaintance, or whether his profile is misused for criminal activities. One perpetrator or the whole group can hide behind one profile. Similarly, instead of several people, only one person can hide behind several profiles. We don't know if it's a woman or a man, an adult or a child, we don't know if he or she knows us or if we were chosen randomly. This whole situation causes the victim great uncertainty and anxiety, which can develop into a paranoid perception of the world. Thus, a child may shop or walk down the street and he or she may begin to be terrified of normal daily interactions, such as eye contact or a smile, and interpret them as signs that there are possible predators. If a child/adolescent has a predisposition to mental illness, the stress associated with the role of the victim in the context of virtual risks can trigger that illness. However, this can happen even if this predisposition is missing.

CYBERSTALKING

The biggest difference between the virtual world and the real world is the fact that there are no boundaries. In the real world, we know that everything has its limit and restriction by a tangible boundary, the virtual world does not work like this. Although we can protect our psyche by turning off our phone for the night, in the morning it can be flooded with messages when we turn it on. This applies to other options that cyberstalker use. The victims of cyberstalking are gradually becoming alert, not knowing when and from where a new attack will come, and they do not know who will be attacked. It depends on the motive of the perpetrator, whether he focuses only on the victims themselves (often because he either "loves" the victim or wants to destroy his or her life) or on their social environment (either it is the intention – he wants to destroy their family, social life etc., or is trying to conquer the environment and win them over).

The victim's anxiety increases and other symptoms may add, such as food (anorexia, overeating) and sleep problems, concentration problems, their grades get worse, mood swings may begin, the person is irritable and cries more, panic attacks or depressive symptoms may appear. It is very important in what environment the victim, in our case a child or adolescent, grows up, whether he or she has a good support system around

them or not. What a stalking victim experiences is hard for anyone who has not gone through something similar to understand. The nervous strain to which the victim is constantly subjected is enormous. If the stalker involves people around the victim, then some time later (practice shows about half a year later), it happens that the people get back to the event, however, they misinterpret the event to the detriment of the victim (you were friends, or why did it happen?), which can be retraumatic (the victim experiences again the same/similar conditions as in the original event). This often leads to an additional disruption of social relations, which could have been the original intention of the aggressor.

What to do about it? It is necessary to realize that we all experience things and situations differently and that is absolutely fine. If a person is a child/adolescent, he or she perceives the situation in a different way than an adult. And that is alright. As adults, we are here to listen to the child, not to evaluate the situation, not to trivialize it, but to solve it. If it is our child, it is necessary to ensure their safety in the first place. We should ask them what they need, what we can do for them. They should know that even if we don't know what's going on, if the situation is unknown and new to us, we are here for them and we will do everything to keep them safe. If it is not our child, it is important to find out what the situation at their home looks like. Is the child safe at home, is there anyone he or she trusts with whom he or she can deal with the situation? If not, the child needs help from other sources. Here, it is necessary to ensure their safety as well (maybe at first it may be just a blanket and hot tea and a closed door). When it comes to virtual issues, the difference is whether we know who the stalker is or not. In any case, we deal with the situation, either at school or with the police.

SEXTING

Sexting has become the norm for adults in relationships. It is therefore quite logical that this is the norm for adolescents. It has become a natural part of courtship, and we also see that it is part of communication with younger people when they are bored. In practice, we hear sentences like, "He wrote me to send him a nude photo because he was bored."

In younger children, we see that sending photos of their genitals is sometimes not perceived as something bad and they are surprised when we confront them. In this case, it seems that basic education at home often fails. That is, education for intimacy. The question is whether overall or only education for intimacy in the virtual world.

Here we, as parents, may have room for change. We expect children not to take photos in sensitive situations, not to send such photos anywhere, but do we behave the same? In the Czech Republic, it is still the norm to take pictures of naked children, children in sensitive situations and then publish them on social networks. Parents often take pictures and film their children even in situations that children do not like and disagree with. What kind of an example does it set?

So what to do about it? Although it may seem surprising, education for sexting and sexuality in general begins in young children. It is more than important to lead them to know what bothers them, to be able to say "no" and to insist that the other party stop unpleasant behaviour, and we must also lead them to be able to respect "no" from others. There is a great challenge for us – if a child tells us that he or she does not like something, we just accept it! The most common mistake parents make is not trusting their children, they try to dissuade them, downplay their feelings, or make fun of them. If children grow up in this environment, they will not learn how to be in touch with their needs. They internalize the "voice" of their parents, and the moment they do not feel well, they begin to question themselves. Exactly as

Send nudes...

it was learned at home. At that moment, they easily succumb to pressure from the other party to send an intimate photo. In addition, the child is more inclined to do so to prove that he or she really likes the other party... It is different if there are unpleasant but necessary tasks for the child (medical procedure), and if there are unnecessary or even inappropriate ones.

In this context, it is important to emphasize another part of the education that we come across in practice, and that is respect for them when it comes to filming and sharing. According to the law on the protection of personality, I need informed consent from the other party if I decide to take or share their pictures or videos. But if the child does not wish to be filmed by a parent or sibling and we do not respect it, we are raising generations of children who will not respect this law either. So if a younger sibling is filming an older one (or vice versa) and he or she does not like it and does not want to be filmed, our role as parents or legal guardians is clear. We will step in, turn off the camera, and make sure that the child deletes the material. By doing so, we make it clear to everyone involved what the standards are, what we expect and what will happen if the standards are not respected. Such behaviour can then be applied by the child in their groups. At school, these rules should work on the same principle.

CYBERGROOMING

Cybergrooming is a manipulation-based activity that aims to obtain intimate and sensitive material from a minor. The material is then used for blackmail. The predator's goal is to lure a child into a personal meeting to rape or sexually abuse them. Cybergrooming has the following phases: selection and contact, friendship formation, relationship formation, offender risk assessment phase, exclusivity phase and sexual phase. It is important to realize that these phases do not last for weeks or months, but often take place over several hours, sometimes minutes. Here it depends on the age, personality and motivation of the child. And of course on the perpetrator. On their age and personality, whether they use their real or fake profile. The child will communicate with the supposed peer differently than with an adult.

The role of education plays a role again. If we raise a child to blind obedience to authorities and adults, i.e. to the need to obey them, the child will tend to obey the adult predator. Which of course does not mean raising a child to anarchy. It is about educating for healthy self-confidence, setting boundaries, the ability to say no and maintaining it, and also for healthy assertiveness.

The biggest risk of cybergrooming is the endangerment and disruption of the psychosexual development of the child or adolescent. For our requirements, it will be most suitable to use the concept of Zdeněk Matějček (a prominent Czech child psychologist), who divides the younger school age (6th–8th year of life), middle school age (9–12) and older school age, which coincides with puberty. This is because, according to research, children have had experience with cybergrooming since the age of nine (it is a question of how much it is due to the surveyed population, greater parental supervision and limited availability of the virtual world for children under nine). The beginning of school is a big change for a child. For younger children, their family plays the most important role, which is gradually changing. New authorities are coming in the form of roles associated with the school environment. The role of the family slowly recedes into the background and peers begin to become more important. There is a need to belong somewhere and a need for recognition by children of the same age. In nine-year-old children, we can already see how they are affected by the rejection of their peers, which is manifested by eating disorders, self-harm, or the development of mental illness. And into all this comes a virtual world, where acceptance or non-

acceptance is replaced by likes, numbers of virtual friends or followers, or number of video shares. If the need to belong somewhere and be accepted as I am is not well satisfied in the real world (it starts with the family), there is a high risk of becoming addicted to the illusory importance of the virtual world. A child like that is also more vulnerable to manipulation and extortion from various predators. As someone who wants to be loved by others, you will do anything.

If you are a child or a teenager, your self-concept, self-worth, or boundaries are not complete. The child learns all this when he or she starts school. The theme of this age is experimentation and the search for boundaries. And, of course, the same applies to sexuality, which awakens and comes to the fore at this age. The body often changes radically, and everyone needs feedback that it is alright. Ideally, the child grows up in a family and school environment where boundaries are clearly set, the child's forming boundaries are respected, and it is predictable what will happen if the boundaries are violated. The child can thus become responsible for their actions.

The moment the child encounters a predator who knows that the child is still looking for his boundaries and identity and at the same time knows that they cannot defend themselves against authority, the predator has unfortunately won. If a child is manipulated into such a relationship, it can have a significant impact on the development of their psyche. There is a risk that the children will learn to perceive themselves only as a sexual object and their sexuality as a way to become popular and valuable to others. The boundaries that should be formed in healthy development through personal contacts and sexual experiments will be shifted and sometimes even forcibly torn. Thus, the children may be paralyzed and unable to defend themselves, which can be traumatic and result in post-traumatic stress disorder or personality disorder. Children can learn to trade with their sexuality, either literally or in relationships. Their ability to establish and maintain quality partnerships can also be impaired, because the basis that it is a partnership, mutual trust, respect for the borders of the other, is not fulfilled.

It is important to realize that it is natural for children and adolescents to communicate with strangers online. They share with them their worries and afflictions, often those that belong to a psychologist's office. This is often the only way they can find "their" people if they do not have a confidant in their family or school. Thus, prevention cannot be based on an assumption that contact with a stranger is automatically bad, but on a skill of recognizing whom and how to trust, and possibly how to defend oneself if this trust is abused.

CYBERBULLYING

Although we may get the impression from the above that the risk to the child is an unknown predator, it turns out that the peer is a greater risk. He or she can be the perpetrator of both the above-mentioned acts and cyberbullying. If this is the case, and the perpetrator is also a classmate, it means that the child is excluded from the only social community that is important to them, and the security of their home is also compromised by cyberbullying. Of course, a child can have more than one peer group – he or she goes to clubs, etc., but there is a real risk of cyberbullying becoming part of them. This can happen by mistake, as a result of public cyberbullying, because the situation is spreading through private messages, or because it is the intention of the aggressor.

The target group we are talking about, children from the age of nine, is at great risk for many reasons. Some of them have already been listed above, one of them is the development of the brain, which is undergoing a major transformation during this period.[2] To put it very simply, the child is more emotional, takes risks more easily because he or she cannot assess the risks, and the seat of reason, the frontal lobe, is just maturing at this moment. It is therefore a very sensitive period from a biological and psychological point of view, in terms of personality development and formation.

2 Francis E. Jensen. The Teenage Brain. 2014.

Self-isolation

Preferring company of adults

Sadness, depression, dejection and irritability

Insecure behaviour

Emotional lability

Sleep disorders

Deteriorating school performance

Skipping classes

Avoiding computers and mobile phones

In the case of cyberbullying, the same applies as for other phenomena. The identity of the victim, his or her self-confidence and self-perception and trust in the surroundings is disturbed. As a rule, the child does not know who the aggressor is and naturally mistrusts everyone (usually someone from his or her surroundings), or he or she knows who is doing it and must constantly face them, for example in class. In both cases, the child is under permanent stress, which can result in a nervous breakdown.

If the child develops any of the following symptoms, it is always necessary to intervene (it can also be a symptom of another problem that bothers the child excessively):

- **Self-isolation**
- **Preferring company of adults**
- **Sadness, depression, dejection and irritability**
- **Insecure behaviour**
- **Emotional lability**
- **Sleep disorders**
- **Deteriorating school performance**
- **Skipping classes**
- **Avoiding computers and mobile phones (or an excessive need to control them)**

It is crucial not to underestimate the child's suffering. It is important to realize that a child thinks differently than an adult. Due to the context of brain development, he or she often perceives negative feedback or any reprimand fatally, long-term stress can affect him or her worse than an adult, and he or she perceives death in a different context than an adult. Adolescent suicide is a real threat. Before this step occurs, the child's behaviour often indicates that something is wrong. Self-harm, eating disorders, depressive symptoms, anxiety, signs of obsessive compulsive disorder, the child shows that something is happening by talking about it or making unusual comments. So it is more than important to take children's displays of emotions seriously, if they talk about something that is bothering them, they need to be helped.

The biggest mistake made by the school and the family is the downplaying of their troubles, denying of what they are going through (it's not so bad, man up, what you're going to do when...), blaming the children themselves (I told you not to do it..., it serves you right).

When in doubt, ask:

How does the child at whom the potentially violent communication is directed experience the situation?

Do classmates respect if the child shows that he or she does not feel good in the situation and does not wish to continue?

Are children solving conflicts as equal partners or is it one-sided violence?

Is it a rare phenomenon or are the attacks repeated?

Use open-ended questions! (i.e. not closed-ended, which the child answers "yes" or "no", an example of closed-ended question: "Is somebody bothering you?")

The virtual world is part of our world. If we do not know how to proceed, we should try to imagine how we would deal with the situation in the real world. It is important to realize that we are not alone in these problems. We have the opportunity to use support networks. The cooperation of the family, school, psychologist, or psychiatrist and other institutions that are involved in the fight against virtual pathology offer good prevention and subsequent support. We think that the positives that this space brings us still outweigh the negatives, and how we deal with this reality is up to us.

Jan Kolouch
Cybersecurity and Cybercrime Expert
at CESNET a.l.e. and C4e, Masaryk
University in Brno

CHILD SEXUAL EXPLOITATION ON THE INTERNET

Jan Kolouch

Recently, sexual abuse of children online (so-called "child online pornography") has become a phenomenon that is very often used as an argument underpinning the dark side of the development of Information and Communication Technologies (ICT) and related services. However, the truth is that this child abuse indeed occurs in an online environment, and due to the fact that ICT is easily accessible to almost all age groups, including very young children, there is a significant increase noted in this illegal and reprehensible behaviour.

The question is how to minimise this dangerous behaviour, or whether there are ways or means that would effectively protect children from sexual abuse online. Is child online pornography sufficiently

legally addressed? Is there a need to revise legal documents in order to provide sufficient protection for children from possible sexual abuse in the online world?

LEGAL FRAMEWORK

The issue of child sexual abuse, including the creation and dissemination of child pornography, has been discussed among experts since the 1960s/1970s. On November 20, 1989, the United Nations (UN) General Assembly adopted the UN Convention on the Rights of the Child (UNCRC). Article 19(1) of the UNCRC requires States Parties to "take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child."[3] This protection is subsequently provided in greater detail: "States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse. For these purposes, States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent:

a) The inducement or coercion of a child to engage in any unlawful sexual activity;
b) The exploitative use of children in prostitution or other unlawful sexual practices;
c) The exploitative use of children in pornographic performances and materials." [4]

It is therefore clear that the countries that have ratified the UNCRC have committed to protecting children from sexual abuse.

Further detailed regulation of the protection of children from sexual abuse was provided by Convention on Cybercrime (ETS No. 185), dated November 23, 2001.[5] This Convention is the most important legal document on Internet and computer crime, aiming to harmonise national laws on cybercrime. The Convention obliges the signatory states to implement certain mechanisms within their laws, that will enable the punishment for defined cybercrime. It is the thorough definition of the substance of the crime that is a condition for the use of the rules of criminal law in cyberspace.

An important step forward in the unification of law is the definition of four basic groups of criminal offenses (see Articles 2 to 13 of the Convention on Cybercrime).

Article 9 of the Convention on Cybercrime (Content-related offenses) obliges Parties to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and unlawfully:

a) Producing child pornography for the purpose of its distribution through a computer system;

b) Offering or making available child pornography through a computer system;

c) Distributing or transmitting child pornography through a computer system;

d) Procuring child pornography through a computer system for oneself or for another person;

e) Possessing child pornography in a computer system or on a computer-data storage medium.

3 Article 19(1) of Convention on the Rights of the Child. United Nations Human Rights. 4 Article 34 of Convention on the Rights of the Child. United Nations Human Rights. 5 Convention on Cybercrime. Council of Europe.

“States Parties undertake to protect the child from all forms of sexual exploitation and sexual abuse.”

However, there are pitfalls with regard to what constitutes "child pornography" and what pornographic works can actually be subsumed under "child pornography." The reason is the lack of a legal definition of the term "child pornography" in substantive criminal law.

A prerequisite for a fair trial of persons accused of activities related to social condemnation of child pornography is a clear (comprehensive) legal definition of the term "child pornography" itself. The first comprehensive definition of "child pornography" was adopted in the Stockholm Congress Against Commercial Sexual Exploitation of Children in 1996, as follows: "Any depiction of a child engaged in child pornography, real or simulated explicit sexual activity, whatever such depiction is made, as well as any depiction of the sexual organs of a child intended for primarily sexual purposes."

Another legal document that characterizes the concept of child pornography is the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, adopted in New York on May 25, 2000.[6]

The Convention on Cybercrime characterizes "child pornography" as material that visually depicts:

a) A minor [7] engaged in sexually explicit conduct;
a) A person appearing to be a minor engaged in sexually explicit conduct;
b) Realistic images representing a minor engaged in sexually explicit conduct.

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, adopted in Lanzarote on October 25, 2007, stipulates that child pornography refers to "any material visually depicting a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes."[8]

The most recent key document defining child pornography is Directive 2011/93/EU of the European Parliament and of the Council of December 13, 2011 on combating the sexual abuse and sexual exploitation of children and child pornography. The Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by December 18, 2013. According to this Directive, child pornography means:

a) "Any material that visually depicts a child engaged in real or simulated sexually explicit conduct;

b) Any depiction of the sexual organs of a child for primarily sexual purposes;

c) Any material that visually depicts any person appearing to be a child engaged in real or simulated sexually explicit conduct or any depiction of the sexual organs of any person appearing to be a child, for primarily sexual purposes; or

d) Realistic images of a child engaged in sexually explicit conduct or realistic images of the sexual organs of a child, for primarily sexual purposes."[9]

6 Refer to Article 2(c) which defines child pornography as "any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes". 7 The term "minor" includes all persons under the age of 18, and thus corresponds to the term child according to the Convention on the Rights of the Child. 8 Article 19(2) of Protection of Children against Sexual Exploitation and Sexual Abuse. Council of Europe Convention. 9 Article 2(c).

A comparison of the above-mentioned documents shows a slight difference in the terminology that is used to define the concept of child pornography, otherwise they are de facto identical.

It is therefore clear from the above that the regulatory framework for the protection of the rights of the child against sexual abuse in the online and offline environment is set sufficiently and appropriately within the European Union.

In fact, sometimes the limits of child protection are set even more broadly than those set by the legal requirements. An example is Europol's definition of "child sexual exploitation," which refers to "sexual abuse of a person below the age of 18, as well as to the production of images of such abuse and the sharing of those images online."[10] It should however be noted that the use of analogy in the subsumption of new acts, typically in an online environment under the facts of criminal offense, is nothing new and illegal if the legal elements of the criminal offense are fulfilled.

PROBLEMS ASSOCIATED WITH CHILD SEXUAL EXPLOITATION

First of all, it should be noted that child pornography is a much broader concept than it may actually seem. It can be stated that the forms of child pornography are primarily addressed, as it is perhaps understood by the society. However, only a few people realise that photos of a 17-year-old naked classmate in provocative positions, stored on a desktop computer, tablet or mobile phone, will also formally fulfil the elements of the crime of production and other handling of child pornography.

This may result in the legal penalty where two adolescent sexual partners (persons under the age of 18) exchange with each other "ticklish and intimate" photos, but at other times, serious conduct consisting of coercing a child is "only" punished by a conditional discharge.

The fact that smart devices and wearables have become easily accessible and, in the vast majority of cases, enable taking and subsequent sharing of photos and videos online, also significantly contributes to the expansion of child pornography. Furthermore, through these devices, the so-called sexting takes place.

At the same time, the availability of these technologies in children is closely linked to the growing number of offenders who commit crimes in child online pornography. The question is whether states, or their security forces, precisely and adequately record the crimes that take place in the online environment and include them in the crime statistics. It can often only be assumed that the act took place in cyberspace.

Although it is not obvious whether moral offenses (§ 190 Prostitution endangering the moral development of children; § 191 Dissemination of pornography; § 192 Production and another disposal with child pornography; § 193 Abuse of a child to produce pornography; § 193a Participation at pornographic performances, § 193b Establishment of unauthorised contacts with a child)[11] from the following statistics[12] took place in an online environment, it can only be assumed due to the relatively high number of children offenders (persons under the age of 18) and the COVID-19 pandemic.

10 Child Sexual Exploitation. Europol. 11 According to Czech Criminal Code.
12 Crime statistical surveys for 2020 (in Czech). Police of the Czech Republic.

Year 2020	Registered	Clarified								
	Number	Number	Clarified (%)	Commited by minors (0-15 yrs)	Commited by adolescentss (15 - 18 yrs)	Commited by children (0 - 18 yrs)	Commited by re-peatedly detained person	Commited by foreigners	Commited by persons under influence	Commited by per-sons under influence of alkohol
January	106	22	20.80%	2	1	3	1	0	0	0
February	162	55	34.00%	6	2	8	5	0	0	0
March	217	77	35.50%	10	4	14	7	0	2	2
April	258	93	36.10%	17	5	22	8	1	2	2
May	305	125	41.00%	21	8	29	14	3	2	2
June	390	169	43.30%	23	11	34	20	4	2	2
July	436	213	48.90%	28	15	43	23	4	2	2
August	482	244	50.60%	31	19	50	29	4	2	2
September	514	269	52.30%	37	20	57	31	4	2	2
October	551	295	53.50%	41	21	62	32	5	2	2
November	607	356	58.70%	47	32	79	35	8	2	2
December	647	398	61.50%	48	37	85	43	10	2	2

A significant increase in child sexual exploitation during the COVID-19 pandemic has also been reported by Catherine De Bolle, the Executive Director of Europol: "The COVID-19 crisis has resulted in a surge in online distribution of child sexual abuse material, which was already at high levels prior to the pandemic." Europol further reports a 106 percent increase in child sexual exploitation. [13, 14]

CONCLUSION

Theoretically, a simple solution that could limit online child exploitation would be restricting all ICT that children under a certain age could use.

A parallel for such restriction could be found in Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in particular, Recital 38 and Article 8 which refer to conditions applicable to child's consent in relation to information society services, where it is stated that children deserve special protection as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

I am aware that this analogy is quite broad, however it stipulates that in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. The question is whether such parental responsibility should also be exercised over other children's activities in cyberspace.

However, even I reject this argument and do not see it as realistic. I am convinced that it is appropriate to have a solid regulatory framework in the form of legislation that allows for the punishment of the most serious offenses. But I am certainly not in favour of the constant supervision of the child's actions in the offline or online world, which would be nothing but censorship and totalitarianism.

I firmly believe that cyberspace must not become an environment where a crime can be committed with impunity. On the other hand, the rules and conditions need to be set so that it does not become an environment in which censorship and repression prevail. There is no point in getting rid of ICT and the services associated with these technologies.

I find the answer in greater awareness. Awareness of the "world of information" or the "world of the Internet". Awareness of risks and dangers, as well as where to seek support in an emergency.

Reducing the negative phenomena in cyberspace and the effort to change should start with end users who are likely to be the first victim of an attacker. At the same time, users are the authority that can define what services, data or information will be searched, stored and provided in cyberspace.

I believe that awareness and continuous user education should be an essential part of the implementation of ICT into our lives. Building information literacy should be inextricably linked to the creation, distribution and promotion of products or services that are associated with ICT. Education in this area, or rather awareness of the possible threats, risks and cons of ICT, should be part of the education of all study forms at all levels of education.

13 COVID-19: Child sexual exploitation. Europol. 14 Europol reports 106 percent increase in child sexual exploitation. The Parliament. 2020.

Kamil Kopecký
Head of eSafety CZ, Digiden and
Centre for Prevention of Risky Virtual
Communication, Associate Professor
at Palacký University in Olomouc

Kamil Kopecký

POSSIBILITIES OF EFFECTIVE EDUCATION IN THE FIELD OF RISKY BEHAVIOUR IN THE ONLINE ENVIRONMENT

Digital, information and media literacy are important skills that need to be developed for all Internet users, especially children. The very important topics that need to be focused on in education include the safe use of the Internet (technical security, basic safety rules, etc.), safe communication and interaction with other Internet users, protection of personal privacy in the online environment (e.g. social networks), principles for safe information sharing (photos, videos, sensitive information, sexting) and topics related to managing risky communication situations (verbal aggression, cyberbullying, communication with other users of online services, etc.) and online dating (cybergrooming, etc.).

There are a number of ways in which pupils can be educated in this area:

1. Online safety education is part of computer science teaching (and other subjects and cross-cutting topics, such as media or sexual education).
2. The issue of risky behaviour is part of preventive activities implemented at school.
3. Topics of safe behaviour in the online environment are part of non-formal education.

In the past, online safety was usually not given enough space in regular teaching, teaching was very often focused mainly on the technical security of computers or mobile devices, the issue of risky behaviour in the online environment was only briefly mentioned by regular teaching. In recent years, however, there has been a massive development of Internet-oriented prevention, and schools have begun to use a wide range of prevention activities from external organizations in addition to their own prevention programs. The role of the school prevention specialist, who is in charge of the preparation and implementation of school prevention programs, is critical. The sad reality remains the overexertion of prevention methodologists, who unfortunately do not have a reduced teaching workload and devote themselves to preventive activities beyond their regular job, although their role is crucial in this area.

In the Czech Republic, a number of legislative changes are taking place in the education system, which have a positive effect on the prevention of risky behaviour in the online environment. These include, for example, The Methodological Recommendation on the Primary Prevention of Risk Behaviour in Children and Adolescents of the Ministry of Education, Youth and Sports, which systematically focuses on cyberbullying and clarifies in considerable detail how to proceed in a crisis situation from the perspective of victims, teachers and parents. Another positive change was caused by the innovation of the Framework Educational Program for Basic Education (2021), which fundamentally changed the teaching of computer science in primary schools, and which also deals with the issue of safety.

PREVENTION OF RISKY BEHAVIOUR AT SCHOOL

Prevention of risky behaviour at school has two basic goals – the goal of prevention is to minimize the possibility of risky behaviour at school (or out of school), the second goal is to minimize the impact that a particular incident has on the victim and his peers (e.g. school class or other groups). Specifically, we can imagine these goals by the school ensuring that there is no bullying (or cyberbullying) in the classroom... and if this happens despite all measures, the school will ensure an effective quick solution to the situation and at the same time ensure that the situation at the school will not repeat itself (e.g. using the school's crisis plan, etc.).

The objective of preventive activities is to teach students how to behave in a crisis situation, how to proceed, who to contact, while providing them with as much information as possible about risk phenomena and acquainting them with various types of risk situations that may occur in the online or offline world. Above all, the goal is to positively influence their attitudes towards healthy and safe use of IT. However, not every preventive activity is equally effective and has a desirable impact on pupils, so it is necessary to remember the principles of effective primary prevention.

PRINCIPLES OF EFFECTIVE PRIMARY PREVENTION

When implementing preventive (or other educational) activities focused on online safety, it is necessary to

“The objective of preventive activities is to teach students how to behave in a crisis situation, how to proceed, who to contact, while providing them with as much information as possible about risk phenomena.”

follow several principles that increase the effectiveness of prevention and the overall impact on the target group. For primary prevention to work, it must meet several basic points:

1. Primary prevention must never frighten or terrify children

Many preventionists think that fear-based prevention works. The opposite is true, fear-based prevention is the least effective form of prevention and very often has the opposite effect than the reduction of the incidence of risky behaviour in a given group of children. Importantly, the information that the preventionist communicates to children must be proportionate to the child's age (more in detail below), so it is very important to be aware of the age of children we communicate with and whether the prevention activity cannot traumatize them.

A practical example:

At a preventive event of an unnamed organization, I experienced a situation where children in the 4th grade of elementary school (age 10) watched a video shot by Amanda Todd as part of lessons on cyberbullying, who committed suicide shortly afterwards.[15] Impact? Pupils experienced intense fear for more than a week, urinating, they suffered from night terrors, and were afraid to go to school. Another example of prevention that works with fear is the presentation of a certain preventionist named Hell Called Facebook. The very name of the event evoked how it is oriented. Do we really believe that children will trust someone who will primarily demonize their favourite communication platform?

Of course, preventive actions can also contain more explicit shots from stories, but preventive workers must always clear up any misunderstanding and give children space to ask questions, let them express their own opinion and address possible discrepancies. The result must always be positive – children must feel that they gain new knowledge and skills, that they are better prepared to face potential risk scenarios, and at the same time understand that the preventive worker does not condemn their communication tools and shows them both negatives and positives. Preventive actions in the target group must never cause panic and hysteria!

2. Primary prevention of risk behaviour must always take place in a safe environment and must be controlled

Primary prevention must always take place in a safe environment - at school, at home, in the premises of a prevention organization or in other suitable places and must always be controlled. There is a reason for this – in this environment, confronting a child with dangerous content (such as a drastic photograph) cannot provoke a negative reaction – for example a reckless decision. Therefore, prevention does not happen with preventionists driving through cities with megaphones and shouting out how dangerous cyberbullying is and how children should not share intimate materials.

As I mentioned above, the preventive action must always be controlled – by a preventive worker, teacher or a parent who oversees the safety of his audience. A child who gets acquainted with new information has a number of questions that a preventive worker can help him answer, and most importantly, to clear up any confusion, refute myths and provide truthful information. And it is necessary to calm him down in a situation where the child's reaction could be impetuous. A typical example of a risk situation that requires control and safety are various risk challenges containing a large amount of false, shocking and misleading information. In the case of uncontrolled reception of information from the media – either from tabloid portals or from youtubers – unsubstantiated and exaggerated information can cause enormous damage.

15 Suicide of Amanda Todd. Wikipedia.org.

With controlled prevention, the risk of imitation is minimized, while with excessive media coverage of the problem, the risk of imitation increases. According to the Czech Radio and Television Broadcasting Council and other relevant expert panels, children have a strong tendency to imitate media-mediated behaviour, because children cannot be expected to have an adequate ability to estimate risk (based on experience) as adults have. That is why media content is regulated. Unfortunately, much of the content in the online world is not regulated at all.

The legitimacy of fears of imitation has been proven many times in the past. It is worth mentioning perhaps the best-known case, when Saddam Hussein was executed in 2006 and footage of the execution has travelled the world. The tragic consequence of this media coverage was six dead children. In various parts of the world, these children died imitating Hussein's execution.[16]

The risk of imitation is also manifested for example in various types of adrenaline challenges inspiring children to imitate and follow them. Typical examples are planking (LDG), but also risk challenges like choking game, salt and ice game, snorting game, eyeball challenge and other similar activities.[17]

Imitation of course also appears in the field of pornography – children naturally crave information about sex and look for pornography on the Internet. However, watching pornographic material arouses premature interest in sexuality and can lead to a distorted image of sex. Watching pornography increases the likelihood of anorexia and other eating disorders in girls, can affect unplanned parenthood, adopting unwanted behaviours (violence), pornography also increases children's tolerance of normal but also deviant sexual practices, etc.[18]

3. Primary prevention of risky behaviour should take place in limited groups (ideally 20–30 people)

If the preventive action takes place in a small group, the children get enough space to ask questions and the preventionist can pay more attention to them. He is also able to actively involve them as much as possible in preventive activities, he can effectively discuss, communicate, answer their questions, etc. All this minimizes the occurrence of panic and imitation – analysing the situation and clarifying the facts is crucial.

16 Kids Imitate Saddam's Televised Hanging Death. ABC News. 8th January 2007. 17 Dangerous Internet Challenges – Understanding Their Appeal to Teens. HealthyChildren.org. 25th September 2020. 18 How Pornography Harms Children. ProtectKids.com.

As the audience grows, efficiency decreases, so it is necessary to change the preventive method of reaching clients in the case of large groups. Some organizations therefore choose a combination of prevention-oriented video, followed by a discussion in which the target group first watches a prevention video informing about the risk phenomenon based on specific stories, followed by a discussion in which children can express, ask, react and possible discrepancies can be clarified. All this reduces possible panic and hysteria and increases the impact of the activity. However, the role of the parent in prevention is absolutely crucial, as it is the parent who influences the child from an early age, and from whom the child seeks help and support in critical situations.

4. Primary prevention must influence the attitudes of the target group

The basis of prevention is to influence the attitude of the target group – in a positive direction. When we communicate with children about social networks, we change their attitudes, for example towards interpersonal communication, verifying who they are having fun with, the importance of their own personal data, respect for themselves (self-esteem) and for others, etc. The attitude must be formed by the child himself or herself, the task of the preventionist is to bring the child to this attitude in a natural way. Influencing attitudes significantly increase children's resilience to risky behaviour. In the school environment, prevention focuses primarily on strengthening good relations between children (and also teachers) and on improving the quality of the school climate.

5. The information we present to a child must always be proportionate to their age

Any information we present to a child must be proportionate to his or her age. It will be difficult for six-year-olds to deal with what sex is and for 15-year-olds how to set a secure password. Each age has its own specifics, which must be respected and adapted to them. It is certainly not appropriate and desirable to discuss planking with young children for example, because it is likely that they will try out the presented situations. Likewise, we will not discuss various sexual practices with a first-class child because they simply will not understand. In addition, there is a risk of premature sexualization.

On the other hand, we can have a debate with them on how to protect yourself on the Internet, how to verify information, how to secure a profile, how to check your Internet friends, etc. The range of topics will gradually expand with regard to the physical and mental development of the child.

KEY FACTORS IN EDUCATION

In previous chapters, we focused on what education aimed at preventing risky behaviour in the online environment should look like, what it should focus on, and how it should be implemented to be as effective as possible. However, we must not forget that the prevention of risky behaviour in the online environment does not only concern the pupils themselves, but also their parents and teachers, who can have a significant influence on their children/wards.

In 2018, the research team of the Centre for the Prevention of Risky Virtual Communication, in cooperation with O2 Czech Republic, conducted a research called Parent and Parenthood in the Digital Era.[19] Among other things, the research mapped how parents themselves approach the prevention of risky behaviour, how they implement prevention in the home environment and which topics are dominant for them. According to this research, the most important topics from the parents' point of view related to the prevention of risky behaviour include communication with strangers, protection of personal data and privacy on the Internet, aggression on the Internet, online dating, YouTube and youtubers, false information in the online world, sexuality, illegal content

19 Parent and Parenthood in the Digital Era (in Czech). E-bezpeci.cz. 2018

on the Internet, etc. Unfortunately, a large proportion of parents (and teachers) are not educated or trained in these topics and often work only with information from the mass media, which is often distorted and may not correspond to reality. However, the role of the parent is absolutely crucial and critical in prevention, it is the parent who can influence the child from an early age, and it is with the parent that a large part of the children seek help and support in critical situations.

Education focused on the risk phenomena associated with communication in the online environment is, of course, also very important for educators who are in daily contact with their students and can purposefully influence their behaviour.

EXAMPLES OF GOOD PRACTICE

The Czech Republic is at a very high level in the field of general primary prevention focused on the issue of risky behaviour in the online world. Both state organizations and authorities (e.g. the Ministry of Education, Youth and Sports of the Czech Republic, the Ministry of the Interior of the Czech Republic, the National Cyber and Information Security Agency, the Police of the Czech Republic, etc.) and universities (especially Palacký University in Olomouc through the eSafety project) are involved in preventive activities, companies (NIC.CZ and its project Safe on the Net, O2 Czech Republic and its project O2 Smart School, Avast and its project Be Safe Online) as well as non-profit organizations (e.g. Don't Be a Victim, Safe on the Internet, etc.).

In the area of prevention, it is also worth mentioning a number of films and series that focus on prevention – in recent years we can mention for example the films To the Mountains, the series Marty Is Dead (awarded the international Emmy Award) and the feature-length social experiment Caught in the Net. What is very important – there are sophisticated methodologies for the above-mentioned films that schools can use effectively when working with them.

Yana Humen
Expert on Cybersecurity Policy, EU Affairs and Digital Economy and Society, Member of the Friedrich Naumann Foundation for Freedom Expert Network

EU POLICIES AND ACTIONS PROMOTING SAFER INTERNET FOR CHILDREN

Growing digitalisation has certainly brought a number of positive changes, such as better access to information, more effective communication as well as enhanced economic growth. Nevertheless, many issues that societies are facing all over the world – discrimination, violence or crime – have also been catalysed through digital tools. In particular, online child abuse is considered to be one of the key action areas for combating online crime in Europe.[20] Over the past decade, the reports of child sexual abuse online in the EU has rapidly increased; from 23 000 in 2010 to over 725 000 in 2019.[21] Moreover, according to Internet Watch Foundation report, 89 percent of known URLs containing child sexual abuse material were registered in Europe.[22]

As online presence of children has intensified during the COVID-19 pandemic, this issue has been exacerbated, as stated in the IOCTA 2020 report.[23] EUROPOL further examined the way lockdown life influenced the approaches of sex offenders and outlined policy recommendations to fight the new surge in its June 2020 report.[24]

There are several aspects that should be considered in the context of risks that children and minors face online: harmful content or content featuring sexual exploitation, and harmful conduct such as cyberbullying as well as harmful contact which may lead to sexual extortion.[25] Recently, the EU has been taking a number of actions to protect children online. The EU developed a legislative framework defining unlawful actions related to child abuse as well as law enforcement mechanisms and enhanced cooperation between public, private and civil society actors allowing detection, mitigation of harmful actions and content directed against children: on the national, EU, and international levels. This Chapter will explore the recent examples of EU – and some global – policies addressing child sexual abuse material (CSAM), child sexual exploitation (CSE) as well as harmful content children are exposed to via the Internet. As a cross-cutting action area, it is important to address technological developments and challenges as well as importance of fostering cooperation with industry in this context.

CURRENT EU LEGAL FRAMEWORK

The EU actions for protection of children online are focused on two main areas:

1) Fighting child sexual exploitation and dissemination of child sexual abuse material, and
2) Raising awareness about children as Internet users and limiting harmful content online.

The milestone of the current legislative framework to protect children from sexual abuse online is the Child Sexual Abuse Directive[26] adopted in 2011. The Directive set out a minimum baseline for a comprehensive approach to prevent, detect and prosecute sexual abuse and exploitation of children. In addition, the E-commerce Directive allows[27] for the limited liability of the Internet intermediary providing services. However, there is a number of challenges that show the need for reviewing the current framework. In 2016, the Commission issued two reports assessing the state of implementation of the 2011 Directive by the Member States (MS),[28] as well as a specific assessment of implementation of measures laid down in Article 25 on measures against websites containing or disseminating child pornography.[29] First, although some progress was made in the national transposition of the 2011 Directive, the Commission had to start the infringement procedures against 23 MS that failed to achieve its proper implementation.[30] Moreover, the legislation does not appear to reflect the current debate around online child abuse – for instance, by using outdated definitions. Thus, there are numerous calls for the Commission to bring more legal certainty by introducing a harmonised system with clear, up-to-date definitions as well as to provide incentives for cooperation against it. Last but not least, the legislation needs a revision in the context of technological development and the emergence of new threats that children face online.

20 Internet Organised Crime Threat Assessment (IOCTA). Europol. 2020. 21 EU strategy for a more effective fight against child sexual abuse. European Commission. July 2020. 22 Europe Internet Watch Foundation 2019 report. IWF 23 Internet Organised Crime Threat Assessment (IOCTA). Europol. 2020. p.36. 24 EUROPOL report "Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic". Europol. June 2020. 25 Alliance to better protect minors online. European Commission. 26 Directive 2011/93/EU. EUR-Lex. 27 Directive 2000/31/EC. EUR-Lex. 28 2016 Report on the assessment of the Directive 2011/93/EU. EUR-Lex. 29 2016 Report on Article 25 of the Directive 2011/93/EU. EUR-Lex. 30 EU strategy for a more effective fight against child sexual abuse. European Commission. July 2020.

Apart from the sexual exploitation of children, which constitutes a large part of illegal content online, one of the other challenges is the harmful content that children and minors have access to when using the Internet. Therefore, in 2018, the revised Audiovisual Media Services Directive (AMSD) was adopted, introducing rules for protecting children and minors from the content, "which may impair the physical, mental or moral development."[31] This also applies to online services, such as video-on-demand services and video-sharing platforms.

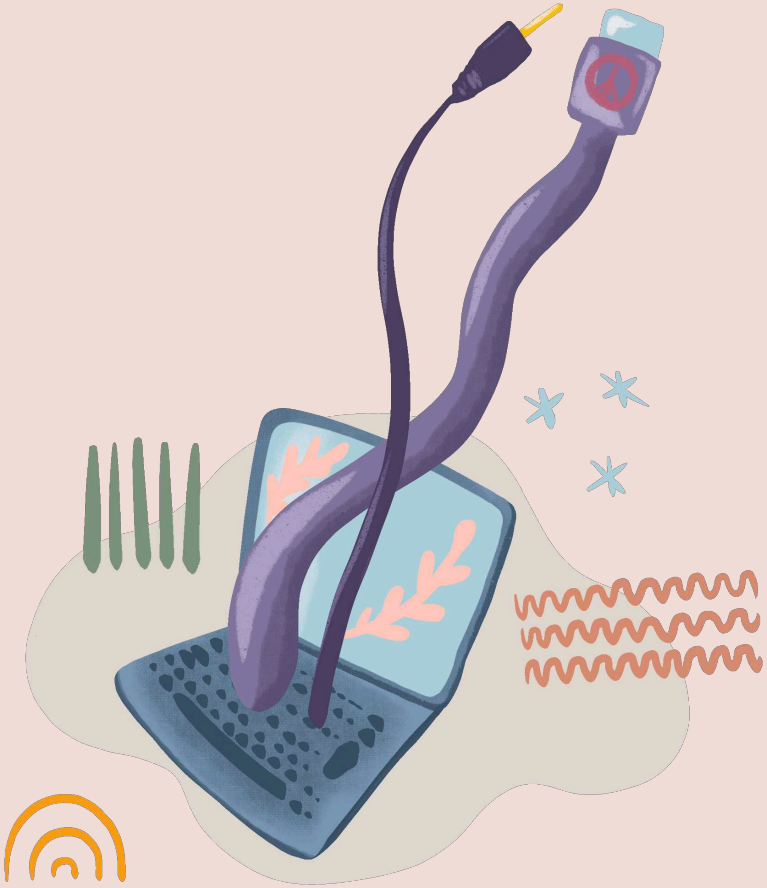
In addition to the relevant legislation, the European institutions have issued guidance and recommendations aiming to address the issue of illegal content online as well as the protection of children in digital space. In 2017, The Council adopted the EU Guidelines for the Promotion and Protection of the Rights of the Child called "Leave No Child Behind,"[32] a revision of 2007 guidance. The document sets out a list of actions promoting the implementation of the UN Convention on the Rights of the Child – among others, the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

The 2018 Commission recommendation on measures to effectively tackle illegal content online calls hosting service providers to take proactive measures to detect and prevent the dissemination of CSAM referring to the commitments undertaken in the context of the Global Alliance against Child Sexual Abuse Online.[33] This underpins the important role the industry plays in this area.

31 Article 6a, Directive (EU) 2018/1808. EUR-Lex. 32 Revision of the EU Guidelines for the Promotion and Protection of the Rights of the Child – Leave No Child Behind. Council of the European Union. March 2017. 33 Commission recommendation on measures to effectively tackle illegal content online. EUR-Lex. March 2018. Recital 25. 34 The European Strategy for a Better Internet for Children. EUR-Lex. March 2012.

STRATEGIES AND OFFICIAL COMMUNICATIONS

It is important to emphasise the European Strategy for a Better Internet for Children adopted in May 2012 which laid ground for most of the initiatives and projects supporting multi-stakeholder cooperation to promote child safety online.[34]



Despite growing cooperation and funding of initiatives aimed at protecting children online, the global statistics in terms of CSE and abuse have been rising (which is also partly but not exclusively explained by better detection mechanisms). Therefore, in November 2019, European Parliament called the European Commission (EC) to take appropriate action to tackle this issue in its Resolution on children's rights which was adopted on the occasion of the 30th anniversary of the UN Convention on the Rights of the Child.[35]

Subsequently, the Commission adopted the EU Security Union Strategy[36] from July 2020 in which highlighted that online tools enhance CSE and set out the following priorities: support of research and prevention activities. The Strategy came along with the EU strategy for a more effective fight against child sexual abuse[37] that laid down eight specific initiatives targeting legal framework, law enforcement capabilities as well as multi-stakeholder actions in prevention, investigation and assistance to victims for the period of 2020–2025. It emphasises the need to keep up with the new technological developments and presages revision of the existing legislation as well as announces future sector-specific legislation in tackling CSE online, which is to be proposed in 2021.

Moreover, tackling child sexual abuse and CSE, including the production and dissemination of child abuse material, is among the Council's priorities in the 2018–2021 policy cycle (European Multidisciplinary Platform Against Criminal Threats – EMPACT) to fight against serious and organised crime,[38] which are based on Internet Organised Crime Threat Assessment (IOCTA) 2020 report.[39]

Last but not least, the recently announced Commission's 2030 Digital Compass aimed at a "human-centred, secure and open digital environment"[40] also seeks to develop principles to protect and empower children in online space. Focused on digital skills development, the Digital Decade communication seeks to provide children the opportunity to "learn how to understand and navigate through the myriad of information they are exposed to online"[41] – thus targeting another important side of child protection online.

35 Children rights in occasion of the 30th anniversary of the Convention on the Rights of the Child. European Parliament. November 2019. 36 EU Security Union Strategy. European Commission. July 2020. 37 The EU strategy for a more effective fight against child sexual abuse. European Commission. July 2020. 38 Draft Council conclusions on setting the EU's priorities for the fight against organised and serious international crime between 2018 and 2021. Council of the European Union. May 2017. 39 Internet Organised Crime Threat Assessment (IOCTA). Europol. 2020. 40 2030 Digital Compass: the European way for the Digital Decade. European Commission. March 2021. p.12. 41 2030 Digital Compass: the European way for the Digital Decade. European Commission. March 2021. p.4. 42 The US National Centre for Missing and Exploited Children. Missingkids.org. 43 International Child Sexual Exploitation database. Interpol. 44 Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. International Labour Organization. January 2016.

COOPERATION FRAMEWORKS AND INITIATIVES

Cybercrime is a cross-border issue. It is important to emphasise that the EU largely relies on its international partners and their policies on protecting children online. One of the key EU partners is the US National Centre for Missing and Exploited Children (NCMEC).[42] Since many online platform providers are operated by US-based companies, NCMEC receives a large part of the CSE and CSAM reports through its CyberTipline. Therefore, it serves as an important source for analysis of evolving trends in this area and allows better targeting of policies implemented worldwide. Similarly, International Child Sexual Exploitation (ICSE) image and video database run by Interpol [43] allows for more efficient investigation of criminals around the world. The Canadian Centre for Child Protection and the Australian Center to Counter Child Exploitation are also important partners in terms of information sharing.

Another important partner is End Child Prostitution and Trafficking (ECPAT) International, a global network of organisations supporting the fight against CSE (including online exploitation). ECPAT assists abuse survivors and provides research and policy recommendations. In 2016, in collaboration with The United Nations Children's Fund (UNICEF) and other organisations ECPAT published the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.[44] It is an important step forward for policymaking, since the relevant legislation in many cases fails to use up-to-date, harmonised definitions.

Within the EU, Europol and its European Cybercrime Centre (EC3) play a key role in fighting CSE. Together with Eurojust, the EU Agency for Criminal Justice Cooperation, Europol coordinates implementation on the EU policy cycle (EMPACT) actions, including those related to tackling CSE online. It has also been gathering valuable information for the Serious and Organised Crime Threat Assessment (SOCTA) and Internet Organised Crime Threat Assessment (IOCTA) reports that address CSE and abuse online. Furthermore, Europol published special guidelines for parents and care-givers on online safety as a response to the surge in CSE and CSAM during the COVID-19 pandemic.[45]

The EU also promotes the protection of children through "Better Internet for Kids", an EC-funded initiative. In addition, there are Safer Internet Centres (SICs) operating across the EU Member States as national awareness centres or/and a helpline (organised in a network called Insafe) as well as hotlines (organised in a network called International Association of Internet Hotlines, INHOPE). In its strategy for a more effective fight against child sexual abuse, the EC announced an intent to create a European Centre to prevent and counter child sexual abuse that will work in the area of improving law enforcement (supported by Europol), prevention and assistance to victims.[46]

According to NCMEC data, 21.4 million out of the 21.7 million reports were made by electronic service providers in 2020.[47] Therefore, active cooperation with the industry – internet and service providers, content and video-sharing platforms, electronic communication services and others – is crucial for detection and investigation of CSE and abuse which, in most cases, are shared through these services, often with for-profit purposes. This said, the inclusion of academia and civil society in such cooperation is essential.

A good example of a public-private partnership is the biggest multistakeholder platform operating globally, WePROTECT Global Alliance. The EU also intends to cooperate with the industry through the EU Internet Forum. Some stakeholders also formed coalitions promoting safer internet for children, taking the self-regulatory approach, such as CEO Coalition (2011), ICT Coalition for Children Online (2012), or Alliance to Better Protect Minors Online (2017).

In an awareness-raising effort, the EC along with other stakeholders from industry and civil society promote a Safer Internet Day (SID). Over the last two years, up to 61 million people across the EU were reached by SID activities, and SID is celebrated in over 170 countries today.[48]

In addition, the EU also prioritises preventive actions tackling CSE and abuse, through the Child Sexual Abuse Prevention Network (CSAPN)[49] which is managed by the EC and serves as a platform for dialogue and research between academics and practitioners.

FUNDING

The EU has also been contributing to the protection of children online through targeted funding of relevant projects under Horizon 2020 program (and Horizon Europe framework programme in future) as well as the Internal Security Fund. Through Connecting Europe Facility, it funds SICs across the MS. The EU also provides financial support to the INHOPE network and the global Interpol database, International Child Sexual Exploitation (ICSE).[50]

In addition, the EC is funding other relevant projects that stimulate innovation in forensics and automatic identification of illegal content to improve operational cooperation and provide training to law enforcement, public administration, judges and academics on prevention and intervention actions.[51] In future, funding for such projects will also be provided via Digital Europe Programme.[52]

CURRENT LEGISLATIVE PROPOSALS AND GENERAL DEBATE

Considering the current debate and the potential developments, the EC will consider review of the Child Sexual Abuse Directive. The current legal framework was believed by many to disincentivise online platforms to report illegal content. Therefore, through introducing the "good Samaritan" principle in the Digital Services Act proposal[53] announced in December 2020, the Commission aimed to clarify the liability safeguards for hosting intermediaries that were originally laid out in the e-Commerce Directive for online intermediaries. The goal is to bring better legal certainty for digital service providers and allow – and even oblige – them to take relevant precautions in relation to illegal content. The obligatory approach as compared to the current voluntary framework was not met with big endorsement from the industry and brought about a debate on which approach is practically efficient and legally appropriate.

Under the new European Electronic Communications Code (EECC)[54] that entered into force in December 2020, the "number-independent interpersonal communications services" (NI-ICS) had to comply with ePrivacy Directive[55] and thus were not allowed to process data for the purpose of detecting online child abuse as ECSs did before. To remedy this, in September 2020 the EC proposed an interim Regulation[56] allowing NI-ICS such as webmail, messaging platforms and internet telephony to be exempted from the ePrivacy rules and thus allowed further detecting child sexual abuse in digital space, on a voluntary basis.[57] With this mechanism being positioned as a temporary solution (effective until 31 December 2025), it is expected to be repealed by the permanent derogation that could be laid down in future legislation to tackle child sexual abuse online.

Apart from this, the e-Evidence proposals[58] published in April 2018 are key to enabling access to electronic evidence held by digital service providers. Moreover, as outlined in the 2020 strategy, the EC seeks to strengthen Europol's mandate, especially when it comes to data access. However, this brought up uneasy questions of jurisdiction and sovereignty as well as the impact on technologies like cloud and encryption, which by nature do not allow service providers to have access to the content on the platforms they operate. This has created a conflict between maintaining a technology and providing the possibility for lawful access to data for investigation purposes. It is not an easy task to solve this bifurcation, especially for providers using encryption technology – as any access to the encrypted data automatically deems it not encrypted.

In December 2020, the Council adopted a Resolution on Encryption "Security through encryption and security despite encryption,"[59] which communicates the EU willingness to establish a multistakeholder debate including representatives of industry holding encryption technology, academics, and civil society on how to tackle the encryption dilemma.

45 COVID-19 Global online safety advice for parents and carers. Europol. April 2020. 46 EU strategy for a more effective fight against child sexual abuse. European Commission. July 2020. p.13. 47 2020 reports by electronic service providers (ESPs). Missingkids.org. 48 A European Strategy to deliver a Better Internet for our Children. European Commission. March 2012. 49 Child Sexual Abuse Prevention Network (CSAPN). European Commission. 50 International Child Sexual Exploitation database. Interpol. 51 Fight against child sexual abuse. European Commission. 52 A European Strategy to deliver a Better Internet for our Children. European Commission. March 2012 53 Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act). European Commission. December 2020. 54 Directive (EU) 2018/1972. EUR-Lex. December 2018. 55 Directive 2002/58/EC. EUR-Lex. July 2002. 56 Interim Regulation on the processing of personal and other data for the purpose of combatting child sexual abuse. European Commission. 57 Proposal for a Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament [...]. Council of the European Union. October 2020. 58 COM/2018/225. EUR-Lex. 59 Council adopts resolution on security through encryption and security despite encryption. Council of the European Union. December 2020. 60 Conclusions of the Council of the EU on Retention of Data for the Purpose of Fighting Crime. Council of the European Union.

Earlier, in May 2019, the Council adopted Conclusions on Retention of Data for the Purpose of Fighting Crime.[60] The Council called the EC to further explore the possibilities to establish the data retention in the EU, allowing the telecommunication services to retain and share certain data with public administrations for the purposes of criminal investigations without violating privacy and protection of personal data principles. The results of the study could lay the groundwork for the prospective legislation. As discussed above, in June 2020 the EC announced its intention to propose relevant legislation to tackle child sexual abuse online in Q2 2021. The future act is expected to lay down requirements for online and communication service providers in terms of detection and reporting of child sexual abuse materials to the public authorities.

EUROPEAN LIBERAL FORUM

The European Liberal Forum (ELF) is the foundation of the European Liberal Democrats, the ALDE Party. A core aspect of our work consists in issuing publications on Liberalism and European public policy issues. The foundation also provides a space for the discussion of European politics, and offer training for liberal-minded citizens. The aim is to promote active citizenship in all of this. The foundation is made up of a number of European think tanks, political foundations and institutes. The diversity of membership provides a wealth of knowledge and is a constant source of innovation. In turn, we provide our members with the opportunity to cooperate on European projects under the ELF umbrella. ELF works throughout Europe as well as in the EU Neighbourhood countries. The youthful and dynamic nature of ELF allows us to be at the forefront in promoting active citizenship, getting the citizen involved with European issues and building an open, Liberal Europe.

www.liberalforum.eu

INSTITUTE FOR POLITICS AND SOCIETY

The Institute for Politics and Society is a Czech think-tank founded in October 2014. The mission of the Institute is to cultivate the Czech political and public sphere through an in-depth and open discussion and to create a living platform which terms problems and offers recipes for their solutions through international conferences, seminars, public discussions and political and social analyses available to the whole Czech society. We believe that an open discussion is a prerequisite for any successful solution to political and social problems. Our main themes are foreign and security policy, defence, European matters, as well as schooling, digitization, power industry, urbanism, city life and in the public space, values in politics and human rights in our country and abroad.

www.politikaspolecnost.cz

FRIEDRICH NAUMANN FOUNDATION FOR FREEDOM

Friedrich Naumann Foundation for Freedom is a German liberal political foundation with over 60 years of tradition. It aims to promote values of liberal democracy, freedom and human rights in more than 60 countries all over the world. With safeguarding and development of its statutory projects the Friedrich Naumann Foundation for Freedom wants to contribute to shaping the future. Furthermore, it assists the development of democratic and constitutional structures by supporting liberal parties, NGOs as well as talented individuals. The foundation's central idea is the realization of freedom and responsibility.

www.freiheit.org

ISBN 978-2-39067-003-2