# European Crime Prevention Network

## Thematic Paper

# Youth Internet Safety: risks and prevention

*In the framework of the project 'The further implementation of the Multiannual Strategy of the EUCPN and the Informal network on the Administrative Approach'- EUCPN Secretariat, May 2018, Brussels*

With the financial support of the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

*Abstract*

This thematic paper is published by the EUCPN Secretariat in connection with one of the EU priorities, more specifically cybercrime. It focusses on the prevention of risks children encounter online. A brief overview is given of several forms of cybercrime considering youth and what motives and facilitating factors enhance them. The last part of the paper focusses on prevention tips with existing examples.

*Citation*

EUCPN (2018). *Youth Internet Safety: Risks and Prevention*. In: EUCPN Secretariat (eds.), *EUCPN Theoretical Paper Series*, European Crime Prevention Network: Brussels.



*Authors*

Orchana De Corte, Intern, EUCPN Secretariat

Jorne Vanhee, Research Officer, EUCPN Secretariat

Cindy Verleysen, Senior Research Officer, EUCPN Secretariat

Febe Liagre, Strategic Policy Officer, EUCPN Secretariat

# Table of contents

# 1. Introduction

In the Best Practice Conference (hereafter BPC) of 2015, organised by the presidency of Luxembourg, was decided to focus on Cybercrime in general. However most Member States submitted projects targeting children and adolescents. Therefore the Secretariat concluded that the Member States consider Cybercrime and Cyber Safety concerning youth an important topic in relation to prevention and a toolbox was written with this focus in mind (EUCPN, 2015). This paper will discuss the risks children encounter online more detailed, what motivates and facilitates offenders and give some prevention tips. Finally, a list with prevention projects will be given.

Nowadays children grow up in a media centred environment (European Commission, 2012). They come more and more in contact with the internet and start using it at an increasingly younger age, as it is possible to access the internet via multiple devices and with high-speed connectivity. This results in ICT becoming embedded in their lives, because the internet creates a lot of possibilities and opportunities, being a treasure of information and the ideal way to relax or communicate with friends. According to the Eurobarometer *"Europeans' attitudes towards cyber security"* 96% of the 15-24 years old Europeans use internet on a daily base and only 1% never uses it (European Commission, 2017).

**D62R** Use of the Internet
**(% - EU)**

| | Everyday | Often/ Sometimes | Never | No Internet access (SPONTANEOUS) |
|---|---|---|---|---|
| EU28 | 70 | 9 | 19 | 2 |
| Age | | | | |
| 15-24 | 96 | 3 | 1 | 0 |
| 25-39 | 92 | 6 | 2 | 0 |
| 40-54 | 81 | 11 | 7 | 1 |
| 55 + | 40 | 13 | 42 | 5 |

**Source: Special Eurobarometer 464a, 2017, p18**

Because social network sites and chatrooms are becoming more accessible for youth, it is easier for online offenders to find and contact potential victims. Different social media or dating sites/apps are used by the perpetrators to reach the children (EC3 Europol, 2017). Frequently children do not think about the consequences, for themselves or for others, when putting something on the internet. They often do not know the risks of being online and engage without any concerns. This environment makes children an easy target for all sorts of online offending. So when focusing on the prevention of cybercrime, children are an important target group, if not the most important one.

Some studies show that the North East European Member States (MS) have the highest rate of online risks experienced by children whereas Western and Southern European Member States have the lowest online risks (Dalla Pozza, Di Pietro, Morel, & Psaila, 2016). However this should be considered with great caution as not all the Member

States systematically collect data in this area and the definitions of these phenomena are not always commonly agreed upon.

The European institutions and organisations know that there is a need to protect youth against potential criminal activities in cyberspace. Many projects aiming to do so are funded by the European Commission. In 1999 they launched the Safer Internet Programme, which is referred to as the "*Better Internet for Kids*" since the adoption in 2012 of the European Strategy to Make the Internet a Better Place for Children. The strategy proposes a series of actions by the Commission, Member States and the whole industry value chain (European Commission, 2012).

> *"The strategy is articulated around four main 'pillars' that mutually reinforce each other*
> *(1) Stimulating quality content online for young people;*
> *(2) Stepping up awareness and empowerment;*
>
> *(3) Creating a safe environment for children online; and*
> *(4) Fighting against child sexual abuse and child sexual exploitation."*
> (European Commission, 2012, p. 2)

The European Commission's *"Better Internet for Kids"* programme funds two important projects concerning the online behaviour of children: EU Kids Online and Net Children Go Mobile.

The *"EU Kids Online"* network exists to provide empirical results to get an insight on the online activities, skills and experiences of children and their parents. Twenty-five MS took part in the study. Every MS delivered the needed analysis and reports and had to make sure that the recommendations made by the *"EU Kids Online"*- research team get passed on to the national and regional policy makers and agencies who inform the parents and teachers. The network is active since 2006 and consisted of three phases of which the last phase ended in 2015. Today a follow-up survey is being prepared with additional topics such as cyberhate, discrimination and violent extremism, cyber-bystanders, digital citizenship, e-health and the internet of things. The data collection window is open until summer 2018. The cross-country analysis will start fall 2018 (EU Kids Online, 2017).

The "*Net Children Go Mobile*" project focuses on the access and use of smartphones and tablets by European children and the risks or opportunities when using these devices to go online. It started in 2012 and ended on December 2014, but the website remains online as a reference archive (Net Children Go Mobile, 2013).

A joint report comparing the *"EU Kids online"* results of 2010 and *"Net Children Go Mobile"* results of 2014, stated that 22% of 9-10 year olds and 53% of 11-12 year olds have an account on one or more social network sites. Despite the fact that most social network sites do not allow children below the age of 13. Nonetheless, children did become better at protecting themselves online, unfortunately this does not mean that children are safer now. Cyberbullying increased over the years and more children report that they have been bothered online (Livingstone, Mascheroni, & Ólafsson, 2014).

The European General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was created to harmonise the rules and regulations to protect EU citizens' data privacy. The GDPR will enter into force on the 25th of May 2018. All organisations, EU and non-EU, that offer services or goods processing or holding personal data of EU subjects are obligated to follow this regulation. Below the age of 16, parental

consent is required.[1] MS may regulate a younger age of consent, but never below the age of 13. How the social network sites will anticipate on this rule is still unclear and the rule's effect should be assessed. At this moment Facebook, Instagram, … are changing their regulations and ask their users to agree with several privacy related topics. The University of Ghent keeps track on the age of consent in the Member States, below the current provisional indications of the age of parental consent across the EU are mapped.


**Source: Milkaite & Lievens, 2018**

## 2. International legislation:

Cybercriminal offences involving youth are getting a lot of attention. International organisations trying to prevent children from becoming an online victim were sprouting up. The national policies became a patchwork of laws which led to the need to create international measures and regulations. Now there are many international and European initiatives, legislations and conventions in the fight against cybercrime, but the MS are still required to implement measures into their own legislation and policies to be effective. More detailed information can be found in the EUCPN's toolboxes on Cybercrime (EUCPN, 2015) and on Cyber Safety (EUCPN, 2017).

[1] Art. 8, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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). Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

The Convention on the protection of Children against Sexual Exploitation and Sexual Abuse, 25 October 2007 in Lanzarote (Spain), was the first instrument to establish various forms of sexual abuse of children as criminal offences. This convention is a multilateral treaty of the Council of Europe whereby MS, which ratified the treaty, agreed to criminalise certain forms of sexual abuse against children and to criminalise sexual activities with children below the legal age of consent, regardless of the context in which such behaviours occurs. It also contains the criminalisation of child prostitution and pornography even when the act was committed abroad. This Convention imposed several preventive measures including the screening, recruitment and training of people working in contact with children, making children aware of the risks and teaching them to protect themselves, as well as monitoring measures for offenders and potential offenders (Council of Europe, 2007).

In 2011 the European Union adopted a directive on 'Combatting the sexual exploitation of children and child pornography' replacing the Council Framework Decision 2004/68/JHA. The directive aimed to harmonise European criminal offences in regard of child sexual abuse and exploitation, and child sexual exploitation material (CSEM). It also aimed to prevent child sex convicts from exercising a profession involving contact with children. This directive expanded on the online solicitation of children and other online risks and set out minimum sanctions for offenders (European Parliament & The Council, 2011). On 16 December 2016, the Commission adopted a report on the measures taken by the MS to combat the sexual abuse and sexual exploitation of children, and CSEM. It presented an overview of the measures taken by the Member States to transpose the Directive into national law. It showed that although they were progressing, there was still some room for improvement. Especially for the prevention and intervention programmes for offenders; the assistance, support and protection of child victims; removal of CSEM (European Commission, 2018).

The Digital Single Market Strategy of the European Commission aimed to have every European citizen digital, considering that children have specific needs and vulnerabilities on the internet. Therefore we need to address the risks of internet usage for children, so they can use the opportunity to access knowledge, to communicate, to develop their skills and to improve their job perspectives and employability. Online safety for children needs to be guaranteed. The EU tries to protect children from cybercrime, hence the EU has created several legislative measures for the Member States to implement or follow (European Commission, 2012). Nevertheless the MS each have their own approach in addressing the issues concerning cybercrime.

Most MS believe that what is considered illegal offline, should be illegal online. This way a lot of online criminal offences are penalised through the laws of the offline offences, except for child pornography which is penalised in all the MS. However it is not always easy to find the right law or penalty and some MS began the introduction of some new criminal laws concerning online criminal offences. Some examples:

- **Sweden** introduced a new criminal offense "*unlawful privacy violation*" which makes it illegal to infringe on someone else's privacy by spreading privacy-sensitive information and visuals, such as revenge pictures, nudes or other offending records. In addition, Sweden modernized the criminal provisions on threats and insults. They extended the definition of threat so that they can punish offences such as threating to spread nudes of someone.

- **Cyprus** has a "*law on the prevention and combating of sexual abuse and sexual exploitation*" (law 91(I)/2014).
- **Austria** applied the following legislation into their criminal law: "*Sexual offenses against infants*" (§§ 206 and 207 Criminal Code), "*sexual abuse of young people*" ("207b StGB) and "*promotion of prostitution and pornographic representations of minors*" (§ 215a StGB).
- **Poland** implemented the offense "*seducing a minor under the age of 15 with the use of an ICT system or a telecommunications network"* (Article 200a of the Penal Code). The Polish police collects statistical data on this crime. The table below shows that this phenomenon is becoming a bigger challenge for the police.

| | Number of initiated proceedings | Number of identified crimes |
|---|---|---|
| 2016 | 529 | 339 |
| 2015 | 281 | 275 |
| 2014 | 154 | 129 |
| 2013 | 129 | 132 |
| 2012 | 84 | 74 |
| 2011 | 64 | 62 |
| 2010 | 34 | 6 |

## 3. Dangers on the internet

The internet is a wonderful place full of opportunities. However, all kinds of dangers lurk around the corner. A classification of all sorts of risks and opportunities was made by Staksrud et al. (2009). (See figure below)

| | | Content: Child as recipient | Contact: Child as participant | Conduct: Child as actor |
|---|---|---|---|---|
| Opportunities | **Education learning and digital literacy** | Educational resources | Contact with others who share one's interests | Self-initiated or collaborative learning |
| | **Participation and civic engagement** | Global information | Exchange among interest groups | Concrete forms of civic engagement |
| | **Creativity and selfexpression** | Diversity of resources | Being invited/inspired to create or participate | User-generated content creation |
| | **Identity and social connection** | Advice (personal/ health/sexual etc.) | Social networking, shared experiences with others | Expression of identity |
| Risks | **Commercial** | Advertising, spam, sponsorship | Tracking/harvesting personal info | Gambling, illegal downloads, hacking |
| | **Aggressive** | Violent/ gruesome/ hateful content | Being bullied, harassed or stalked | Bullying or harassing another |
| | **Sexual** | Pornographic/ harmful sexual content | Meeting strangers, being groomed | Creating/ uploading pornographic material |
| | **Values** | Racist, biased info/ advice (e.g. drugs) | Self-harm, unwelcome persuasion | Providing advice (e.g. suicide, pro-anorexia) |

**Source: Staksrud, Livingstone, Haddon, & Ólafsson, 2009**

It is important to be aware of these risks, to recognize them when they occur and to not walk right into the trap. Cybercriminal offences consists of new types of crimes or cyber-dependent crimes (e.g. phishing, social engineering…) and new methods of old criminal activities or cyber-enabled crimes (e.g. online sexual exploitation, cyberbullying…) (Norden, 2013). The difference between offline crimes and the cyber-enabled crimes lies in the use of a virtual cyber medium (EUCPN, 2015). Hereafter an enumeration of the most common phenomena is given. Nonetheless this list is non-exhaustive. For more information on cybercrime risks, the reader can consult the EUCPN's toolboxes and theoretical papers on Cybercrime and Cyber Safety[2]. As the internet and everything connected with the internet is evolving quickly, updates every now and then will be needed.

## 3.1.Common phenomena

### *3.1.1. Cyberbullying*

The EU does not have one standard definition of cyberbullying. However a lot of organisations, institutions and academia already tried to provide one. A lack of uniformity makes it more difficult to adopt measures concerning this phenomenon and generalising or comparing data from reports is fairly impossible.

Cyberbullying is every form of bullying through the use of new information- and communication technologies to irritate, threaten, humiliate or offend victims (BeSafe, 2018). Cyberbullying and bullying have a lot of similarities, however cyberbullying has unique characteristics that imply important corollaries for its approach. For example cyberbullying can occur 24/7 at any place (even the children's bedroom[3]), the cyberbully can act anonymously and often there are more witnesses online than in real life bullying (Mediawijs, s.d.). Additionally, the consequences of cyberbullying proof to be worse, because of a greater audience and bystanders and the fact that something on the internet can be found even after being deleted. However cyberbullying is less frequent than real life bullying (Erreygers, 2016).

Nevertheless, cyberbullying and bullying should not be seen as two different phenomena. Sometimes real life bullying continues on the internet or in some cases the bullied one even becomes the cyberbully.

There are three criteria needed to define actions as (cyber)bullying (Bastiaensens, s.d.):

- The bully intends to **harm** the victim physically or psychologically.
- There is an **imbalance of power**. The bully dominates the victim. This can be created by the anonymity of the perpetrator, the victim does not always know whom he is up against. In this way it is possible that a 'weaker' person in real life, is the 'stronger' person on the internet.
- The bullying actions are **repeated**.

[2] Cybercrime was the topic under the presidency of Luxemburg in 2015 and Cyber Safety was the topic of the Estonian presidency in 2017.
[3] Many children have at least one device with internet connection in their bedroom. This implies that there is no supervision and that children are not even safe for online risks such as cyberbullying in their own bedroom, what should be a safe place. The amount of children having internet access in their room increases every year (Erreygers, 2016).

The manner of bullying in cyberspace changed over times due to quick developments. The arrival of new social media and different devices created a lot of new opportunities for bullies to operate. Therefore, preventing and fighting cyberbullying is not an easy task and being up to date with the latest developments is very important. Victims of cyberbullying and bullying can suffer severe mental problems and even suicidal thoughts as a consequence of the offences. Therefore it should be taken seriously and not only sensitising programmes about (cyber)bullying at school, but also suicide prevention should be implemented in classes (Hinduja & Patchin, Bullying, Cyberbullying, and Suicide, 2010).

Cyberbullying is more prominent amongst children aged 10-15 years according to several studies. Some adults also engage in cyberbullying or are a victim of this phenomenon, however this is less common. Almost all studies claimed that boys are more likely to be the bully than girls. Moreover, there is a big overlap of being the victim of cyberbullying and being a cyberbully at the same time. Bullying is induced by stressors and negative experiences. It is thus important for children to learn how to cope with these feelings (Erreygers, 2016).

In order to prevent cyberbullying, it is important to include all the engaging parties. However, the most important ones are the bully/bullies, the victim(s) and bystanders. Especially the bystanders have a significant role in the bullying. They can choose to help the bully, to intervene in the bullying or ignore it (Cantone, et al., 2015). In some cases the bully cannot be found, e.g. the offender uses a fake profile or is anonymous, which is very distressing for the victim. Another difficulty is the 'cockpit'-effect, where a bully believes that he did not cause the victim any pain, because he did not see the victim getting harmed by him (Heirman & Walrave, 2008).

Most MS lack data on cyberbullying. They do however believe that prevention is the best way to tackle cyberbullying. Therefore, none of them has introduced this phenomenon in their national criminal law. In addition, cyberbullying is being criminalised through other criminal offences in a broad range of areas such as violence, cyber-related crimes and anti-discrimination (Dalla Pozza, Di Pietro, Morel, & Psaila, 2016). In a lot of cases cyberbullying is connected with (cyber)stalking: the harassment of a targeted individual by repeatedly sending intimidating messages threatening to harm them or to scare them (Senker, 2017).

Although cyberbullying is mostly the online version of bullying, there are some specific cyberbully forms that are completely new due to the possibilities created by the internet:

- *Fraping*: Logging into someone's social network page (e.g. Facebook) without their consent and altering their status or info (Moncur, Orzech, & Neville, 2016). The reformed content can be embarrassing, inappropriate or even cruel (Urban Dictionary, 2011).
- *Trolling*: Posting provocative or offensive messages on the internet to get an emotional reaction out of the target for a humorous purpose (Bishop, 2013).
- *Doxing/outing*: Researching and outing an anonymous poster's real identity or broadcasting personal details of someone on the internet, often with the intention to humiliate, threaten, intimidate or punish the identified individual (e.g. forwarding personal text messages, "name and shame"…) (Douglas, 2016).
- *Happy slapping*: Attacking an unsuspecting passenger and film it with a mobile phone in order to disseminate it afterwards for the amusement of others (VICE, 2018).

### *3.1.2. Sexting*

Sexting, the portmanteau of sex and texting, is sending, receiving or forwarding sexually explicit or suggestive texts, images and videos, using mobile devices (NSPCC, 2018). The phenomenon 'sexting' is widely talked about, as it is a hot topic in the media, press, judicial and academic world. Many assumptions concerning youth sexting influence prevention programmes. One of the assumptions is that most teenagers sext. In reality only a minority engage in sexting even though the numbers are increasing slowly over the years. Research reports are all giving other outcomes and therefore it is not possible to know exactly how many teenagers are involved. The main reason is that the researchers use different definitions of sexting and different age groups, which makes comparing them difficult (Mitchell K. J., Finkelhor, Jones, & Wolak, 2012). A meta-analysis of multiple researches learned that adolescents receive more sexts (27,4%), than send them (14,8%) (Madigan, Ly, Rash, Van Ouytsel, & Temple, 2018).

> *"Dominant understandings view sexting as a troubling teenage trend created through the combination of camera phones and adolescent hormones and impulsivity, but this view often conflates consensual sexting between partners with the malicious distribution of a person's private image as essentially equivalent behaviors."*
> Amy Adele Hasinoff, 2011, abstract

The media and even a lot of researchers conclude that sexting is harmful or has horrible consequences, such as reputational damage, and is associated with risk-taking behaviour, substance abuse, risky sexual behaviour and cyberbullying (Van Ouytsel, Walrave, & Ponnet, 2018). The risks and victimisation are stressed and often a gender distinction is made: boys are more likely the receiver or manipulate girls for sexts, girls are more likely the victim of unwanted pictures and the sender (Korkmazer, De Ridder, & Van Bauwel, 2018). There might be found some truth in these prepositions – for example there are some known incidents with children committing suicide due to a leaked nude picture – however more research should be conducted to known the real extent of sexting.

Sexting between minors is a debatable topic with many different perspectives, some blame the children for sending self-generated sexualised material, others portray them as victims and some believe it is a natural process in their experimental phase (Hasinoff, 2011). In most countries sexting as a minor or with a minor is prohibited because it is seen as distributing child sexual exploitation/abuse material (Hinduja & Patchin, 2012). Even if the child willingly generated the images or videos himself and sent it to a peer. At times they even are put on the sex offenders list (Wolak & Finkelhor, 2016).

Sometimes it is hard to see the difference between normal sexual behaviour and deviant sexual behaviour. Sexting is considered suitable when (De Bie & Day, s.d.):

- There is an explicit affirmative consent between the receiver and the sender
- There is no form of coercion or threat
- The engaging parties are at the same level (e.g. age, mentality…)
- Their behaviour corresponds to their development and the situation
- Their behaviour is not harmful

An often used argument of the opponents of sexting is the "Lolita"-effect: the sexualisation/pornification of prepubescents and teenagers perpetrated by the media that subtlety fosters sex crimes. Named after the roman "Lolita" by Vladimir Nabokov (Durham, 2008). An example of this effect is young girls and boys, between the ages of 12 and 16, selling sexy photos and videos on social network sites. In 2017 the Russian newspaper "Meduza" did some research and found hundreds of profiles of teenagers selling their self-generated indecent material on VKontakte, a Russian social network site. Lovers of child pornography can find these profiles in groups or with the search terms "central processors" (child pornography) or "CP in DMs" (child pornography in direct messages). Most teenagers create fake profiles to maintain some anonymity. However some of the existing fake profiles are people buying and then reselling the material or crusaders pursuing paedophiles (Merzlikin, 2017).

Sexting or producing sexualised material can thus be the innocent and normal sexual behaviour of a teenager exploring their boundaries, but it can have serious repercussions for the creator, the sender or distributor and the receiver.

### *3.1.3. Grooming*

Grooming is the process in which a 'groomer' contacts children online with the intention of maintaining sexual contact, mostly through the use of fake profiles ("catfishing") representing a minor or a celebrity. Often offenders have multiple profiles on a variety of social media platforms or chatrooms to reach different potential victims. The groomer can have multiple motives for tricking the children: to exploit them and get some money out of their pictures, for their own sexual pleasure or to gain some power over them (EC3 Europol, 2017).

Groomers work with a very manipulative strategy. They start by being nice and attentive. This way they gain their trust and make a real connection. They become a friend where the child can turn to, they listen to their troubles and give them compliments (Child Focus, s.d.). They create a relationship of trust without parental supervision or the environment knowing about it. Vulnerable children around the age of 13-14 years are the perfect victims. Victims of grooming are more likely to have a low self-esteem or do not have close relationships with their parents, experience depressive or homosexual feelings, have a lot of (social) troubles, have been abused before… The perpetrator gives them the feeling that they are special.

After a while the 'groomer' begins to ask some questions about their love life and sexuality. Slowly these conversations evolve in demanding sexual actions for the web cam, exchanging explicit material or talking about sexual encounters and fantasies (EXPOO, s.d.). Most of the offenders just want some child sexual material, but some hands-on perpetrators also use this technique to meet up with children offline. Others coerce, extort or threaten the child (e.g. to show their pictures or videos to their family or peers) for receiving new material or doing other sexual things. In a few cases a child is asked to financially pay the perpetrator for silencing or deleting the material. Once the victim accepts the offender's demands, the victim is more likely to continue conceding in other demands. Some children do not even realise that they were victims of a crime or are too ashamed to report the crime (EC3 Europol, 2017).

In most cases the groomer is an adult. In some cases the perpetrator is an acquaintance, a professional or family member is the offender. However peers can be grooming too.

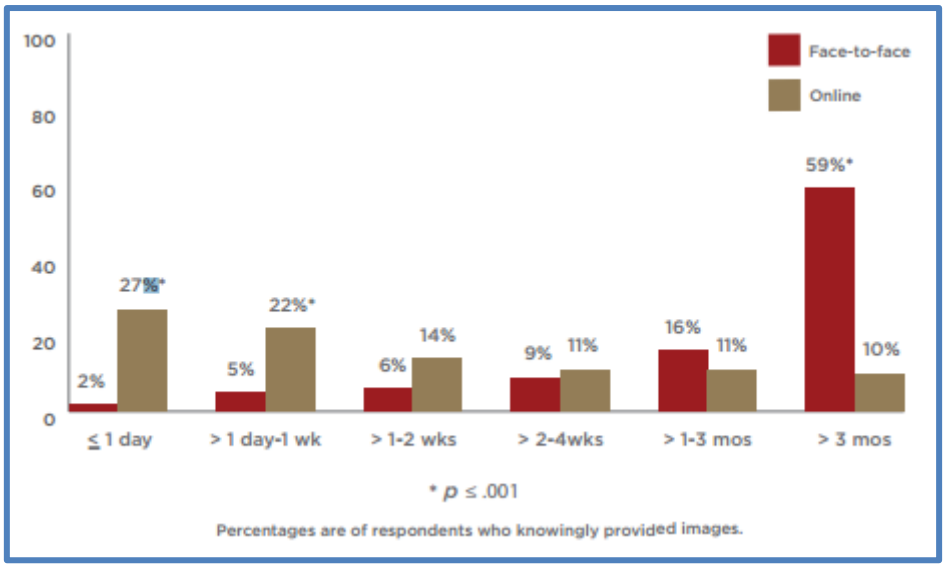
### *3.1.4. Sexual exploitation and abuse of minors online*

Online child sexual exploitation and online child sexual abuse are frequently mixed up with each other by different studies and even institutions or organisations. Both phenomena comprise sexual activities with children online, notwithstanding that the motives for the crimes are different. For online child sexual exploitation the motive is to gain something, for example money, services or goods. The offender wants to receive money out of the produced material, which can be produced by the child or another person with or without force (UNODC, 2015). On the other hand online child sexual abuse happens for a sexual preferential reason or power motive. Nevertheless one does not necessarily preclude the other. Thirty percent of offenders in possession of child sexual exploitation material (CSEM) are involved in both online as offline child sexual exploitation (EUROPOL, 2017).

CSEM is more and more produced for financial gain. One of the newest threats is *Live Distant Child Abuse* (LDCA), where an offender pays to watch the live abuse of a child and this through the use of various video sharing platforms (EUROPOL, 2017). The viewers remain anonymous and make payments by wire transfer. Often they downplay the live abuse by thinking that the child acts in consensus; they need the money or other excuses. This relativism happens when the offender does not want to accept that he is complicit in the crime. However, by watching CSEM or CSAM the child is re-victimised over and over again.

Sexual extortion or "sextortion" is a form of sexual exploitation that occurs primarily online, whereby non-physical forms of coercion are used, such as blackmail, to extort the victim for money or to meet to engage in sexual activities (NCMEC, 2018). Most sextortion targets are women and adolescent girls harassed by men and adolescent boys. Although sometimes the tables are turned (Wolak & Finkelhor, 2016). In a research conducted by Wolak and Finkelhor about sextortion (see figure below), a survey of 1.631 victims, more than half of the respondents (629 victims) who had a face-to-face relationship[4] with the perpetrator, waited at least three months to knowingly share an image. While 49% of the respondents (497 victims) in an online relationship with the perpetrator provided an image within one week of the first contact. These results show how quick a (romantic) relationship evolves online and how important it is to educate young people about the risks of online relationships. It is contradictory that we sooner trust someone we never met, except online, than someone we know in real life.

[4] The face-to-face or online relationship with the perpetrator is not necessarily a romantic or sexual relationship.




**Source: Wolak & Finkelhor, 2016, p18**

Child sexual abuse is mostly not documented as it takes place in private settings such as the home and thus is invisible for investigators. However, sometimes the offender captures the abuse to have some material for later sexual satisfaction or for distribution. In this case there is evidence of the crime and the perpetrator can be penalised (INTERPOL, 2018).

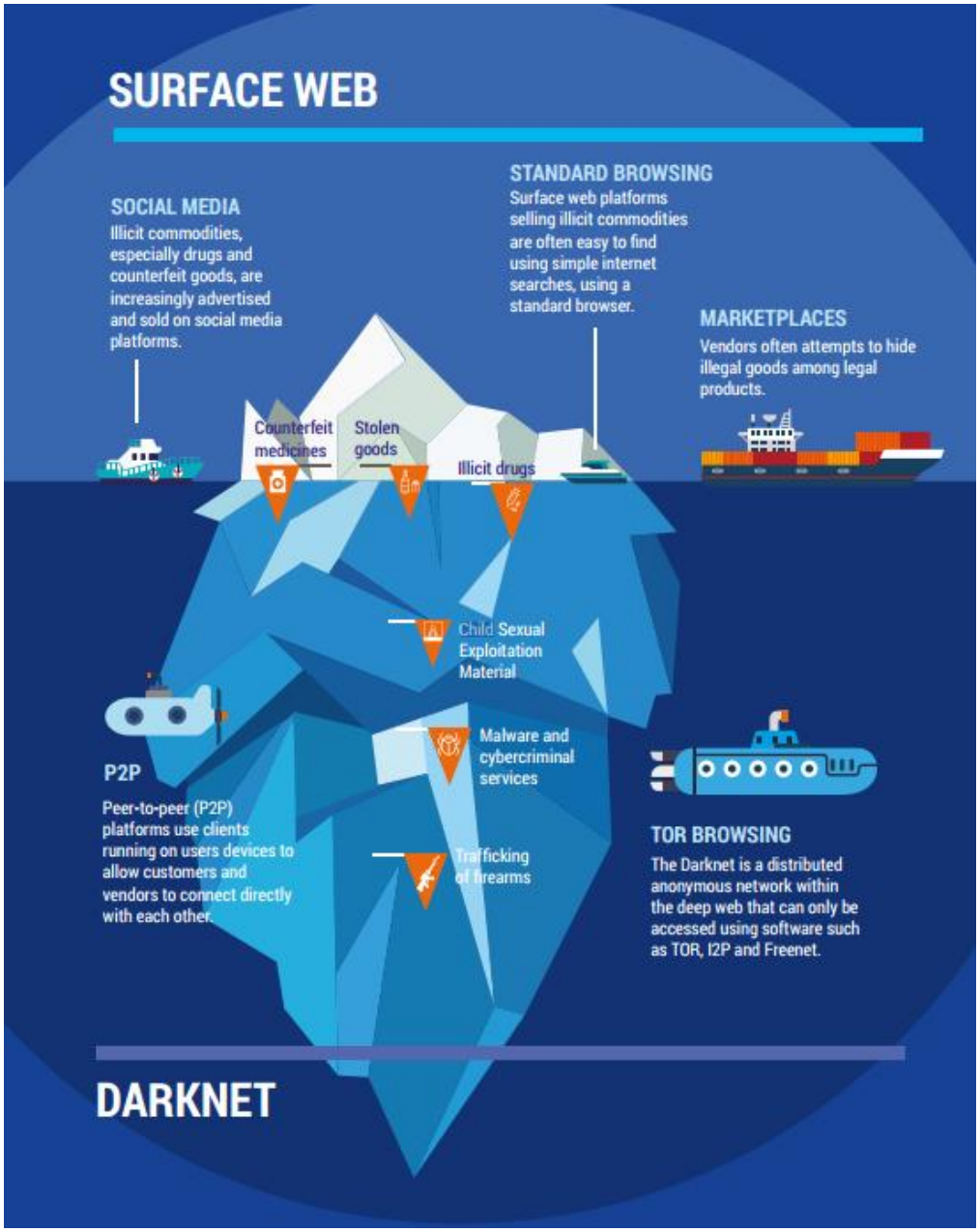
Sometimes CSEM/CSAM can be found on obvious internet websites. YouTube was recently under fire because of an article of The Times. They found out that some profiles on You Tube were used to distribute child abusive or exploitative material. The profiles contained seemingly innocent videos of children (coming out of a shower with a towel, licking their lips,...) with an e-mail address in the title. When sending a mail to that address, the user could receive thousands of child pornographic videos (The Times, 2017).

There are two types of offenders: the ones directly abusing or exploiting a child and the ones buying material, thus indirectly abusing or exploiting a child. The first type of offender is most often a person known to the child, such as a parent or guardian, family member, neighbour or childcare professional (INTERPOL, 2018). This indicates that prevention should focus on the adults the closest to the children, the ones who should protect them from getting harmed. First of all, they should be informed about warning signs and they should learn to speak up when knowing or suspecting that a child is being abused or exploited. Secondly, adults should offer sexuality education to children on time. Finally, all sex offenders should be provided with a specialised treatment programme (Stop It Now , 2018). Nevertheless this should not mean that prevention of potential child sex offenders should be a manhunt on paedophiles[5]. Only 1-2% of the population have paedophilic feelings (BBC News, 2014) and certainly not all paedophiles act upon their sexual interest. The first step for a potential offender is to accept that they have sexual feelings for children. The second step is to work on their self-control or inhibition. Self-control in the real world is easier than online where no one is watching

[5] According to the DSM-5 (American Psychiatric Association, 2013) a criteria for paedophilia is "Over a period of at least 6 months, recurrent, intense sexually arousing fantasies, sexual urges, or behaviors involving sexual activity with a prepubescent child or children (generally age 13 years or younger)." Whereas the DSM V leaves out the adolescents, paedophilia in this paper is seen as having sexual interest in all children.

over our shoulders. Research indicates that paedophiles experienced more childhood trauma's and child sexual abuse themselves than the average population, though it is still not known why certain people experience sexual feelings towards children. Prevention programmes should be offered for paedophiles who fear to lose their self-control (Vanhoeck, 2015).

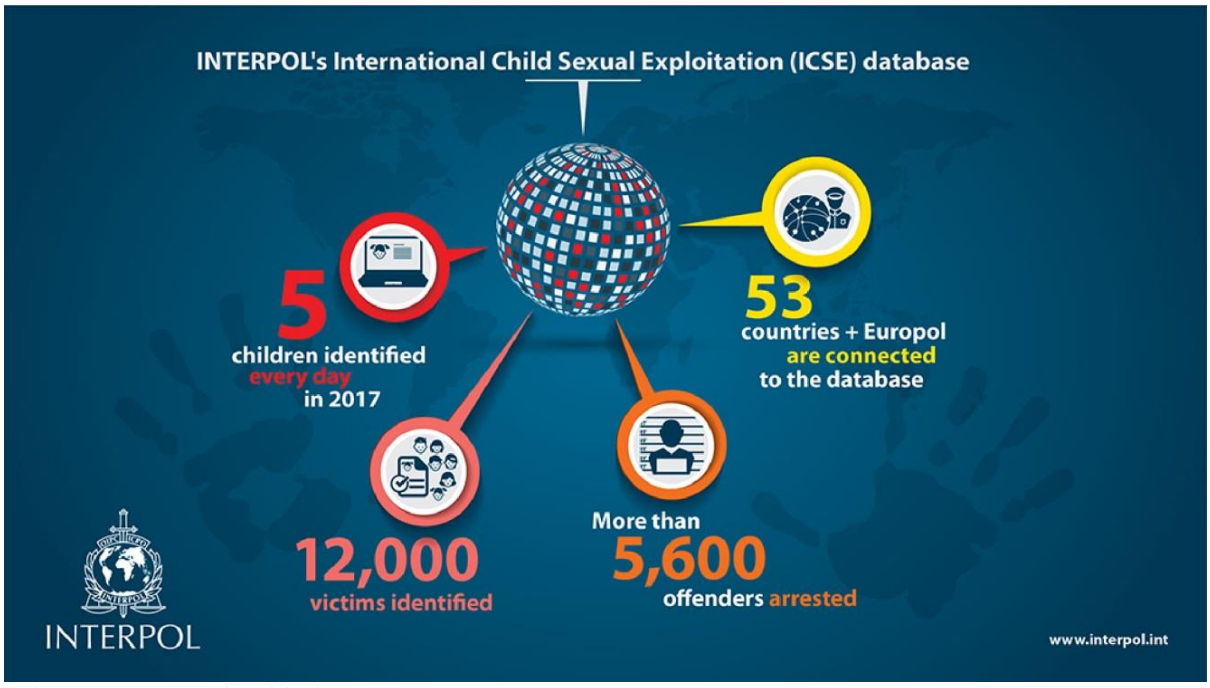
The increasing global availability of internet and internet-enabled devices encourages (potential) offenders to interact with potential victims and other offenders in an allegedly safe and anonymous environment. The number of fora and services on the Darknet, dedicated to the production and distribution of CSEM, increases, with the peer-to-peer (P2P) networks as the most used platform for sharing material (EUROPOL, 2017). The figure below illustrates the difficulties of the web:




**Source: EUROPOL, 2017**

As these phenomena are European priorities, the Member States, many institutions, organisations, other countries and other stakeholders work together to tackle them.

- **ECPAT** is a global network of 101 civil society organizations in 92 countries working to research and better understand the global exploitation of children in all its forms. They especially focus on tackling the online sexual exploitation of children, trafficking of children for sexual purposes, forced and early marriage of children and the sexual exploitation of children through the travel and tourism industry (ECPAT, 2016).
- **OAP EMPACT** The SOCTA of EUROPOL (2017) identified Cybercrime as one of the eight priority threats to the EU, with online sexual exploitation of children as main concern. The European Commission released on the 12th of April 2017 a statement with their views on the SOCTA and the new Policy Cycle and agreed upon putting online child sexual exploitation as a priority (European Commission, 2017). Resulting in an operational action plan of EMPACT.
- **The WePROTECT Global Alliance** to End Child Sexual Exploitation Online is an international movement dedicated to national and global action to end the sexual exploitation of children online. They aim to identify victims and ensure support, to investigate cases of exploitation and prosecute the offenders, to increase public awareness and to reduce the availability of CSAM online (WePROTECT Global Alliance, 2015).
- **ICSE** is an International Child Sexual Exploitation image database managed by INTERPOL. It is an investigative tool which allows specialized investigators to share data with colleagues across the world. The database uses image comparison software to connect pictures and videos with victims, abusers and places. However Child Abuse Material is more likely to show the face of the victims rather than the face of the abuser causing image analysts to focus more on the victims (INTERPOL, 2018).




Source: INTERPOL, 2018

ECPAT and INTERPOL conducted a research together between 2016 and 2018. The researchers draw data from the ICSE database to analyse. They discovered that 64,8% of the unidentified victims in the database were girls and 31,1% were boys. When boys were depicted in abusive material, it was more likely to be severe or involve paraphilic themes. Also the younger the victim the more severe the abuse. 56,2 % of the unidentified victims were prepubescent, 4,3% were infants or toddlers and in 14% of the cases the images contained children of multiple ages. Offenders could not be determined in more than half of the cases. 92,7% of the determined offenders were male and 7,5% were female. Young adult or late adolescent females are more likely to operate alone while older females mostly cooperate with a male offender (ECPAT; INTERPOL, 2018).

### *3.1.5. Social media challenges*

"Life is a game which ends with death", the hype of the "Blue Whale" - game, an online suicide game, started in 2015 in Russia on VKontakte (a social network platform such as Facebook) causing teenagers to take their lives. A child becomes member of a group and is instructed by the group administrator, the curator, to complete one challenge a day. The 50$^{th}$ challenge ends with suicide of the child and posting a blue whale on their social network page. The tasks can easily be found on the internet and comprise auto-mutilation, facing fears, standing on high buildings, creating relationships with other "whales", watching psychedelic and horror movies, waking up at 4.20 a.m.,… (Bureau Jeud en Media, 2017).

The game grew bigger, probably because of the media attention and the teenagers' fascination. New groups and new curators arose on different social network sites or apps around the world. Some social networks, such as Instagram and Facebook, show a warning when searching for the game: *"Posts with words or tags you're searching for often encourage behaviour that can cause harm and even lead to death. If you're going through something difficult, we'd like to help"* (Instagram, 2018). This also counts for other terms like "suicide" or "self-harm". Not only the networks, but also peers and adults try to prevent children from committing suicide or playing the game by writing advice or leaving their phone numbers on their status and comments on social media. Even some counter movements were established. For example: "Baleia Rosa" (Pink Whale), in Brazil, containing positive tasks to learn to value life and combat depression.

After the "Blue Whale" - game some other harmful challenges came to the surface. The "salt and ice" - challenge and the "deodorant" - challenge which causes burns, the "drinking bleach" - challenge, "Fire" - challenge, etc. These challenges are without a curator who manipulates them to act the way he/she wants. This implies that the only reasons teenagers start doing this challenges is media attention and peer pressure or extreme thrill-seeking behaviour (McKenzie, 2008). The curiosity of these teenagers can lead to their death without even realising it. Perhaps it could help to have some kind of clause in the law talking about these games to put some boundaries and maybe even criminalise them and the persons who encourages teenagers to conduct them. A similar game that got a lot of attention, but did not include social media was the "Choking"-game. Based on a survey on this phenomenon pre-adolescents see their parents (43%), as the most respected source of a preventive education message and for older adolescents a victim or the victim's family (36%) (Macnab, Deevska, Gagnon, Cannon, & Andrew, 2009). It is shown that informing the care takers, parents, schools and children also works. It is thus important to have an open communication and good sensitising

programmes and combine forces with social media. Because of these morbid social media games being recent, there is a need to conduct more research on the topic and prevention. This would help to create a legal framework and to set up some good prevention programmes.

A lot of organisations, companies… nowadays use the challenges for advertising or reaching a bigger public. The hype regarding these challenges is sometimes used to raise awareness (e.g. the ALS ice bucket challenge). These challenges are innocent and harmless, but where do we draw the line between a good and a bad challenge?

In most MS the police monitors these challenges. When a challenge with negative consequences occurs in their country, they try to raise awareness by using (social) media and give lectures in schools. Other MS believe that talking about the challenge only feeds the hype. In Germany search engine Google works with the Network Against Abuse and Sexual Exploitation of Children – No Grey Areas on the Internet. As part of this cooperation, Google launched measures to display warnings above its search results when there is reasonable suspicion that a user is searching for child sexual abuse imagery. Furthermore, users are shown details of related hotlines, helplines and prevention networks.

#### *3.1.6. Other risks*

- ✓ Malware

Children and even adults can download malware by accident. This can entail severe consequences, not only for themselves but also for their families: cybercriminals can access someone's bank account or other sensitive information. In this case, it is important to make children aware of how malware enters a computer or other device. Cybersecurity software can counteract some threats, but definitely not all of them. The most important measure is to communicate with your child (Kaspersky Lab, 2018).

- ✓ Phishing

The cybercriminal pretends to be a trustworthy entity to obtain sensitive information (e.g., passwords, credit card details) through deception of the victim. Mostly e-mails or advertisements are used to deceive the target. These "notify" the user that an occurring problem only can be solved with the confirmation of some personal information or promise a tempting offer that one cannot refuse. Typically a link redirects the victim to an official looking site (De Kimpe & et al., 2018). Minors are more susceptible for phishing than adults. Interactive games and online trainings are proven to be the best prevention methods (Sheng, Holbrook, Kumaraguru, Cranor, & Downs, 2010).

- ✓ Unwanted exposure to sexual or harmful material

Approximately one fourth of the children between 10-17 years are exposed to (un)wanted online sexual or violent material at least once. The older they get, the more chance of exposure, because of more excessive internet use and/or risky behaviour. The more time spend on the internet, the more frequent a child will be exposed. Filtering and blocking software reduces some unwanted material, but it does not guarantee to block all material (Mitchell, Finkelhor, & Wolak, 2003). More boys are exposed to unwanted as well as wanted sexual material online. It is important to make the distinction between whether the child looked it up or accidentally stumbled upon it. Some children experience

distress after seeing this kind of material, nevertheless the risks for children are perceived as a bigger issue than they actually are. Children still see more unwanted sexual material on television or advertisements than they do online. There is still too little known about the potential harm, to create prevention measures (Byrne, Kardefelt-Winther, Livingstone, & Stoilova, 2016).

- ✓ Privacy

> Article 16 of the *"UN Convention on the Rights of the Child"* (UNCRC)
> 1. *"No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."*
> 2. *"The child has the right to the protection of the law against such interference or attacks."*
>
> United Nations, 1989, p. 5

Children do not always understand the consequences of posting a picture or personal details online. Even adults make the mistake of placing too much personal information online. The posted material affects not only themselves, but also others, for example, by giving their home address or posting a group picture.

A lot of parents engage in this risk by posting content about their parenting on Facebook, Instagram, Snapchat, WhatsApp, blogs… It seems innocent, but online shared information can be seen by many and even gets spread all over the internet. This phenomenon called "sharenting" can cause serious risks for their children. Online information might haunt a child for years and even harm them (Steinberg, 2017; Commission for the Protection of Privacy, 2018). Just like anyone else, parents should ask permission to their children to share material, if possible, or at least consider the possible consequences for them in respect of article 16 of the UNCRC (United Nations, 1989).

Also businesses and companies violate children's privacy by creating business models targeting them. On the internet a user leaves traces by accepting cookies, buying online, clicking on a link… This data is collected by a company, who can sell this information to another company or can use it to create personal advertising, named profiling (eNACSO, 2015). The European NGO Alliance for Child Safety Online (eNACSO) stimulates the debate and actions to protect children from online businesses that have a negative impact on their rights as set out in the UNCRC (eNACSO, 2016).

- ✓ In-app purchases

In-app purchases are extra content, subscriptions or services that one can buy within an app (Google Play, 2018; Apple, 2018). App providers should inform users in advance when they have in-app purchases, this way the users know that the currency in the game is real money (eNACSO, 2015). Nevertheless, this does not guarantee that children are protected against in-app purchases. Often the providers are not transparent enough or misleading and some children are just vulnerable for this kind of commerce. Regulations for app providers are thus necessary (eNACSO, 2016).

## 3.2.Motives and facilitating factors

In the above mentioned phenomena some of the reasons or motives to commit these kinds of crimes are already pointed out. In this part a little more explanation is given, since prevention starts with knowing why somebody does what he/she does.

### *3.2.1. Anonymity*

Although guaranteed anonymity on the internet provides privacy, it can also bring a lot of problems. A person's behaviour can change completely while being online. They can become extremely kind or emotional and share everything with anyone or they can become very rude and brutal due to anonymity and invisibility. Online offenders have the perception of being untouchable and unpunishable; this is called the 'online disinhibition effect'. Additionally, it is easier to turn a blind eye to the suffering of people you do not know. Some people watching child abusive or exploitation material differentiate themselves from the perpetrator, because they did not abuse or exploit the child (Suler, 2004). As already mentioned, another effect of anonymity on someone's behaviour is 'the cockpit'-effect. The offender does not realise that he/she harms a person on the other side of the screen, because he/she cannot see the victim (Heirman & Walrave, 2008).

An internet user can easily hide behind this anonymity by creating a pseudonym or steal someone else's identity, encrypt traffic through numerous nodes, conceal the original IP-address or using a hacked computer (EC3 Europol, s.d.). Anonymity on the internet thus bears an opportunity for the offender to approach a potential victim, without the victim knowing their real identity. Furthermore, the Darknet makes it possible to share, buy and sell child sexual exploitation or abuse material to one another without giving any personal data, mostly purchased with hard-to-trace virtual currencies such as Bitcoin. To safeguard communications and stores with this material, encryption is widely used (EC3 Europol, 2017).

### *3.2.2. Peer/Media Pressure*

Teenagers and children have a great influence on each other. With the rise of the internet, their world broadened alongside their interactions with others. As Livingstone, Mascheroni, and Staksrud (2015) argued, social norms and values on young people's social media use cannot be separated from media representations. Mass media, including printed media often emphasises the already existing image and constructs norms and values on 'childhood', 'good parenting', 'the nature of risk', and 'sexuality' (Korkmazer, De Ridder, & Van Bauwel, 2018). These constructions and images created by the media and peers pressures someone to live up to standards.

MYMOVEZ is a project testing the peer pressure and social media influence by tracking youth (8-15 years) with a watch connected to the "Wearable Lab" application. The project aims to develop a method for effective campaign implementation by targeting young people's social networks via social media. Social forces (i.e., important classmates and friends that influence youth's health behaviours) are used to enhance campaign effects on physical activity, snacking and drinking behaviour (CORDIS, 2017). If this project is successful the peer and media pressure can be used for stimulating positive behaviour on the internet. However, privacy concerns should be respected at all times.

#### 3.2.3. Money

Money is a motive for anyone who makes a financial profit out of the crime. It is one of the main incentives for the online distributors of CSEM. It is possible to buy, sell and resell anonymously sexual images of children. Distributors sometimes get paid to abuse or exploit children via livestreaming devices by the watchers. Likewise, some children use their self-generated sexual material to sell on social network sites. Furthermore, there are a lot of other cybercrimes or risks where the motive is gaining money, such as online blackmailing, phishing, hacking, etc.

#### 3.2.4. Feeling powerful

To feel powerful over someone an inequality between the interactors is needed. The perpetrators desire to control a child is linked to child sexual abuse. The offender commits the crime to gain some feelings of power over a helpless child or to assert his authority. In cyberbullying the feeling of imbalance is also an important factor to start with it. The bullied child is unable to come against the bully's force.

#### 3.2.5. Sexual preferences

The internet created a space to be permanent connected online and made it easier and cheaper for paedophiles and child sex offenders to act on their desires and to come in contact with potential victims. Child sex offenders mostly operate alone, but they also communicate among each other within like-minded groups in cyberspace. The most common tool for exchanging child abuse material is the peer-to-peer platforms. Some youngsters use self-generated sexual material to act on the desires of others or themselves. Not only adults, but also minor can get aroused by creating, sending or receiving sexually suggestive or explicit material.

#### 3.2.6. Own entertainment

This applies to teenagers and others who have no malicious intent or financial benefit, but simply do it because they can. Mostly they commit these crimes out of boredom, to try out their skills, to have a great laugh or just because they are curious.

## 4. Safe internetting: prevention

As said in most researches and reports: the conclusion on how to keep a child safe on the internet, is communication. Talk about the risks, the opportunities and mainly listen to which experiences the child has or which problems he/she encounters. This advice is not only applicable for the parents or guardians of the child, also the teachers, educators, policy makers, researchers, etc. can learn from paying attention to what children already know or still need to discover.

Already a lot of sensitising programmes exist at schools for youth and internet use. It could be helpful to bring them together and look for the things that really work. Nevertheless, evaluating these programmes on their impact is not an easy task. At this moment we do not really know which programmes are useful. Protecting children from cybercriminal offences is hard. Children are human beings and they have their rights and freedoms, which should not be restricted when preventing these crimes.

## 4.1.Tips

### *4.1.1. Multi perspective and transnational approach*

> *"Successful campaigns against child pornography require shared responsibility and effort by parents, Internet Service Providers (ISPs), legal enforcement and the international community at large"*
> Raphael Cohen-Almagor, 2013, p.1

Internet users should feel safe and secure when going online. Nor in the physical world, nor in the digital world should criminal activities be accepted. To reduce the risks and enhance the security of the digital environment, individuals and private and public institutions should take responsibility in their own environment and globally. Industries should also be involved, in particular in the protection of minors using their devices (European Commission, 2010). The prevention of online crimes against and committed by children needs a multi perspective approach. The most common actors are children and youth, parents or guardians and educators. Nonetheless, there are more key actors in this problem. For instance: perpetrators, social workers, website moderators, policy makers… (UNODC, 2015).

Childnet is a British charity to help make the internet a safe place for children and youngsters. They made some good proposals for providers of social media and apps to safeguard the children's privacy and to keep them from harmful material (Childnet, 2017):

- Providers should guarantee that privacy settings are default on regardless someone's age
- Providers should always inform users, which reported content, about the outcome of the report and indicate some sites for potential further help. This ensures trust and transparency
- A lot of popular social media apps have an age requirement; however, they do not always control the age when signing in, nor is it always clear what the age limit is. This should be more strict and checked more
- The Terms and Conditions and Community Standards should be easy to understand and child-friendly. Also this should be visible on the website and users should be reminded of them at a regular basis. The Youth Parliament of Belgium made a recommendation for providers of social networking sites to have informative banners with a daily tip on how social networks should be used and what rights and duties pertain (Jongerenparlement, 2016)
- All the prohibited contents and behaviours should be easy to report

In addition to the list, it could be an idea for the providers to create their own ratification system for distributors to use when uploading material. In that case a user posting a video with for example sexual references, can indicate that the content of the video is age restricted. YouTube already allows this in the advanced settings of a video (YouTube, 2018). Providers of interactive internet services, such as social media, should be required to delete messages that obviously constitute threats or privacy violations.

Slowly the cooperation between the different stakeholders grows, but it is still in its early days. It is important to include social network sites and media as partners in the preventing of cybercrime, hence 88% of the European 16-19 year olds participate in them. Prevention should not only be having a profile on a social network site to reach raise awareness; it should be using them as a partner in prevention projects and policies as well.

| GEO/TIME | 2011 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|
| Austria | 92 | 89 | 92 | 91 | 93 | 93 |
| Belgium | 80 | 84 | 86 | 96 | 96 | 95 |
| Bulgaria | 70 | 73 | 77 | 78 | 81 | 82 |
| Cyprus | 90 | 93 | 97 | 92 | 96 | 93 |
| Czech Republic | 70 | 85 | 93 | 91 | 90 | 94 |
| Germany | 92 | 92 | 90 | 93 | 88 | 87 |
| Denmark | 94 | 96 | 95 | 94 | 98 | 99 |
| Estonia | 80 | 91 | 95 | 95 | 96 | 97 |
| Greece | 80 | 83 | 87 | 88 | 88 | 90 |
| Spain | 88 | 94 | 90 | 89 | 89 | 88 |
| Finland | 89 | 89 | 94 | 92 | 91 | 98 |
| France | 79 | 82 | 77 | 73 | 73 | 78 |
| Croatia | 83 | 84 | 78 | 97 | 93 | 98 |
| Hungary | 86 | 89 | 97 | 94 | 96 | 94 |
| Ireland | 87 | 91 | 90 | 85 | 89 | 95 |
| Italy | 71 | 76 | 79 | 76 | 77 | 76 |
| Lithuania | 84 | 94 | 97 | 92 | 92 | 92 |
| Luxembourg | 86 | 94 | 93 | 89 | 97 | 94 |
| Latvia | 95 | 96 | 95 | 96 | 93 | 91 |
| Malta | 85 | 94 | 93 | 98 | 97 | 97 |
| Netherlands | 90 | 96 | 94 | 87 | 85 | 90 |
| Poland | 79 | 85 | 86 | 93 | 88 | 92 |
| Portugal | 77 | 94 | 96 | 88 | 97 | 95 |
| Romania | 59 | 71 | 73 | 82 | 76 | 82 |
| Sweden | 96 | 90 | 95 | 92 | 80 | 88 |
| Slovenia | 89 | 89 | 95 | 92 | 86 | 85 |
| Slovakia | 94 | 93 | 88 | 92 | 92 | 95 |
| United Kingdom | 91 | 97 | 91 | 100 | 89 | 98 |
| European Union | 84 | 88 | 87 | 87 | 85 | 88 |

**Source: Eurostat, 2018**

Offender-oriented prevention is more difficult, less researched, and thus fewer projects are focusing on the (potential) perpetrator (Vanhoeck, 2015) (EUCPN, 2017). Mostly the offender-oriented prevention considers a variety of crimes, not one in particular and to prevent recidivism instead of prevention for committing a crime in the first place (Peeters, Elffers, van der Kemp, & Beijers, 2011).

### 4.1.2. Focus on the target group

Prevention for children should be in their language. The usage of computer games and popular social media or YouTube channels are thus effective to reach them (European Commission, s.d.). Gamification is the use of game-like or fun elements in non-game environments to promote learning and engagement, for example a watch that tracks your steps motivates a person to exercise more (Kapp, 2012). The game-like elements are motivational affordances to provoke a positive psychological and behavioural outcome (Hamari, Koivisto, & Sarsa, 2014). This could work effective as a prevention method for children. Providers could also use this for informing children about their rules and conditions instead of a dry text nobody reads.

### 4.1.3. Investment in primary prevention

Raising public awareness on the possible online risks is one of the first things to do. The Safer Internet Programme, now Better Internet for Kids, helps the EU and the Member States to provide information and education for children, parents and teachers on online safety. The programme organises several international events each year, for instance Safer Internet Day and Safer Internet Forum[6], to raise more awareness and share information. The Safer Internet Centres, represented in 30 European countries, are an important part of the programme. They advise the children, carers and teachers in their country, organise youth panels on online safety and lead campaigns (European Commission, 2018). They work together with the hotlines, INHOPE, and the helplines, INSAFE (European Commission, 2017). The hotlines allow people to report illegal content anonymously so they can pass it on to the competent bodies. The helplines provide information, advice and assistance to youth and parents on how to deal with online harmful content, conduct and contact. They can be reached via telephone, e-mail, web forms, Skype and online chat services (Better Internet for Kids, s.d.). It is important to further develop this network so they will become more known and will reach more children and different stakeholders. The Better Internet For Kids also made a guide (https://www.betterinternetforkids.eu/web/portal/onlineservices) about online services to provide some key information about some of the most popular apps, social networking sites and other platforms which are commonly being used by children and young people (and adults) today. This way parents, caretakers and children can learn about the different services and possible opportunities or risks (Better Internet for Kids, s.d.).

Giving (correct) information to the public, especially youth, can change their behaviour. However, only raising awareness and educating children is not enough to stop them from risky online behaviour. According to research from the National Foundation for Educational Research (NFER) children are generally aware of how they should behave online to safeguard themselves, but do not always (know how to) use these strategies. Because of this awareness-raising is not enough, but also reflexes in how to react on the internet should be generated (National Foundation for Educational Research, 2010). Some projects aim to achieve this through the use of games that reflect the real life. An example is the Re:Pest game. This was developed to teach children all kinds of behaviours in bullying and the consequences of these behaviours (HOWEST, s.d.).

[6] The Safer Internet Forum is an annual conference in Europe where policy makers, researchers, law enforcement bodies, youth, parents and carers, teachers, NGOs, industry representatives, experts and other relevant actors come together to discuss the latest trends, risks and solutions related to child online safety ( Safer Internet Forum Secretariat, 2018).

In Belgium a school created a fake profile of a young girl and befriended their students to gain some control on cyberbullying. Soon they discovered that a lot of groomers tried to get in contact with this profile. The school was worried about their pupils and reached out to a popular human interest programme "Koppen" to help them with an experiment. They created a new fake profile on Facebook, this time of a young handsome boy, and befriended all their students of the 1st and 2nd year high school. Two third affirmed the friend request and 29 students started a conversation, after a week of chatting ten students agreed to meet up. They choose five students and three of them actually showed up (always with friends), although they had had classes in online behaviour. This experiment creates an opening to discuss the online risks. This kind of prevention will stick longer because of the shock effect and first-hand experience than sensitising alone (Koppen, 2015).

Protecting our own identities more carefully and using social control to discourage unacceptable behaviour could prove to be more effective, than criminalising all forms of this behaviour. Someone can protect him-/herself by using a nickname, enhancing their privacy settings and avoiding to put certain pictures public, because everything put on the internet can haunt someone for the rest of their life. This way strangers are less motivated to get in touch (Senker, 2017).

#### *4.1.4. Parental control*

In the research done by Livingstone, Mascheroni, & Ólafsson (2014), it was found that parents use less restrictive forms of parental mediation (banning social network sites, using parental control or filters) than active forms (encouraging, suggesting, helping, talking to their child about the use of internet). It is better for parents to inform their children about the benefits and risks of the internet, to support exploration of the internet and enhance their opportunities, coping skills and resilience to potential harm. They can set some clear rules relating to online behaviour and communicate with the child about what they do on the internet. Parental control or filters are not the only way, nowadays children come in contact with the internet everywhere and other devices are not always provided with parental control. It is important to discuss with the children what kind of parental mediation can be done, if a parent works from a top-down restriction, internal family issues can occur causing the child to lose their trust or even lie about their internet behaviour (Zaman & Nouwen, 2016).

An example of parental control is the "SafeToNet" app. It was created by a concerned father and controls a child's device. It detects behavioural changes in the texts and messages your child sends and informs children and parents in real-time when risks arise. One of the features is the sexting filter. When installing "SafeToNet", the device is scanned for images of a sexual nature. Should an inappropriate image be detected in a child's photo library, it is quarantined, thumb-nailed and degraded. When the app detects that the child is sexting, than it blocks the camera for several minutes and informs the child on the risks. When the child attempts to sext three times within 24 hours, their parent will be notified who can block the device. The parent can choose how much they want to control the child's device (SafeToNet, 2018).

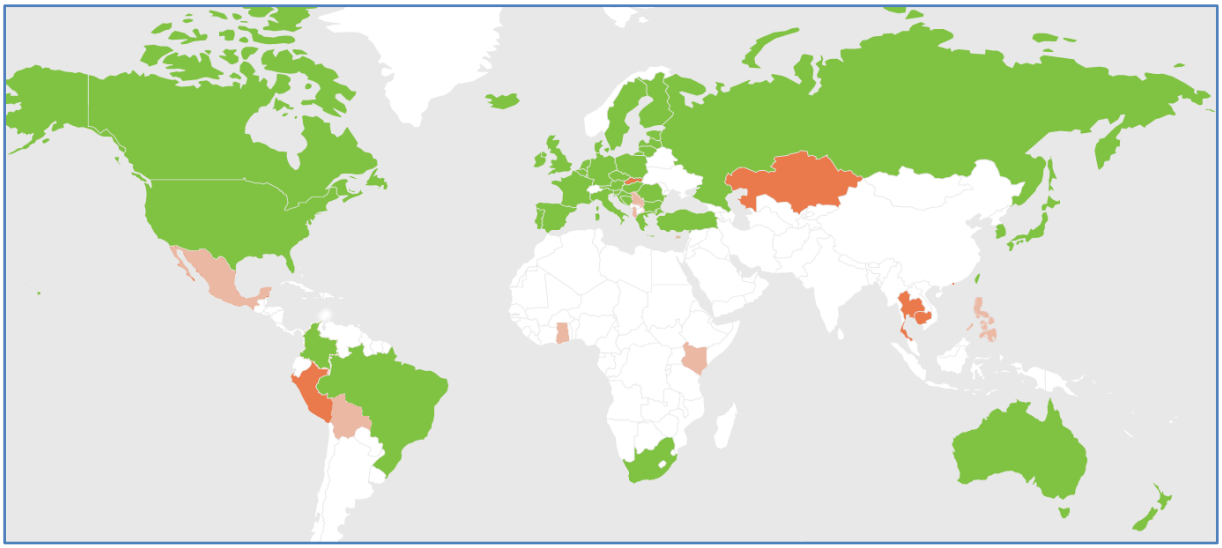
### 4.1.5. Focus on affirmative consent

The legal age to engage in sexual activities as a child varies depending on the country and the opinions are divided. A question that one should ask is: "When is it illegal and punishable for a child to have sex or sext, if the child willingly and knowingly engages?" (Hasinoff, 2016). Something to keep in mind for sex related offences, is to focus on affirmative consent in prevention programmes. A lack of acknowledged consent of the victim is the trigger for criminalising the acts. Therefore children should be well aware of the intention of the other and dare to refuse. Building resilience can help them stand up for themselves (Lievens, 2017).

There should a focus on affirmative consent in offender-oriented prevention. When there is affirmative consent essentially it is alright to engage with the (other) child, so the engaging parties know what will happen and no one will be forced or exploited. Most law systems contain restraints for getting involved with children. Tools should be given to control the urge of the offender. A good project doing so, is "Stop it now". The project deals with sexual abuse of children by awareness-raising and being a helpline for paedophiles and their relatives. The project exists in the USA, UK, Ireland, The Netherlands and the Flemish part of Belgium (Stop it Now, s.d.). Other offender-oriented prevention programmes can be found on the link "https://helplinks.eu". This site was created by a joint police cooperation Police2Peer and sums up online and offline help by country.

### 4.1.6. Hotlines

Hotlines, where citizens can report illegal content, are seen as an important prevention strategy by the Member States. The INHOPE Foundation is the biggest network of hotlines across the world and all MS are affiliated. The map below represents the members of the INHOPE Association (green), members of the INHOPE Foundation (orange) and members of the INHOPE Foundation focus countries (light orange). The INHOPE Foundation helps new hotlines with funding and start-up activities (INHOPE, s.d.).



**Source: INHOPE Foundation , 2017**

Austria provided some numbers of their hotline. They stated that the number of advertisements reported for child pornography of minors[7] went from 465 in 2015 to 681 in 2016. The number of ads for grooming[8] went from 52 ads to 80 ads in 2016. The number of references in the registration office Child Pornography and Child Sex Tourism decreased (2015: 2,742 thereof 310 with reference to Austria; 2016: 1,530 indications, of which 347 relating to Austria). This does not mean that child pornography and child sex tourism cases decreased, but that CSAM or CSEM online is more found in closed forums or in peer-to-peer Range (P2P).

### 4.2.Update on prevention projects and programmes

Offender oriented prevention:

| Project/ programme | MS or other countries | Description |
|---|---|---|
| Stop It Now! | the USA, Great-Britain, Ireland, The Netherlands and Belgium | A project that raises awareness on child abuse and has a helpline for people with paedophilic feelings or relatives of the paedophiles. https://www.stopitnow.org |
| Re:Pest De pest aan pesten! | Belgium | A game created with the aim to reduce bullying behaviour. In this game children learn different ways to react on bullying. http://repest.howest.be/ |
| **Otanvastuun.fi (I take responsibility)** | Finland | A self-help program for adolescents and adults who are concerned about their sexual interest in children. The program was established in January 2018 and can be used anonymously and free of charge. https://www.mielenterveystalo.fi/aikuiset/itsehoito-ja-oppaat/itsehoito/seksuaalinen-kiinnostus-lapsiin/Pages/default.aspx |

Child/victim oriented prevention:

| Project/ programme | MS or other countries | Description |
|---|---|---|
| **Help.some** Help. some | Finland | A mobile app launched in 2016 that provides information and advice for children and young people concerning their worries and problems. The app offers reliable information and support from trained professionals and volunteers. It enables users to get help with such things as bullying and harassment, matters concerning sexual harassment and abuse, as well as other criminal acts. Discussions are staffed by experts from Save the Children, the Helsinki Virtual Police and Victim Support Finland. |

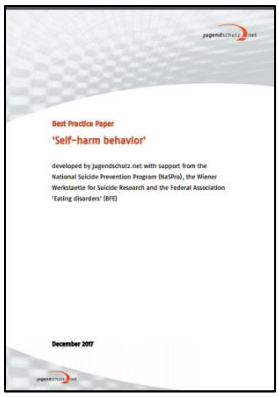
[7] § 207a StGB (StGB = Strafgesetzbuch or the Austrian criminal code)
[8] § 208a StGB

| | | |
|---|---|---|
| **Verklickt!**<br>  | Germany | Verklickt! is a 50-minute feature film aimed at children and young people aged 12 and older, and was created to teach them safety and security awareness in their digital day-to-day lives. An educational booklet is included in the media package for teachers and educators. It focusses on cyberbullying, illegal downloads, cost traps, rights of personality and copyright. Additional topics include e.g. behaviour on social networks, content that is harmful to young people and password security. https://www.polizei-beratung.de/startseite-und-aktionen/verklickt/?L=0 |
|  | Germany | ProPK has issued a lealeft for victims, entitled "Opfer, Schlampe, Hurensohn – gegen Mobbing". This brochure, designed as a comic strip, shows how cyberbullying takes shape. It explains the functions included in smartphones, and shows how mobile devices connected to social networks can be used as a tool for cyberbullying. However, its main message is that bullying should not be tolerated. Victims of cyberbullying can and should seek help from third parties. The brochure is aimed at children and teens. |
|  | Germany | ProPK has also developed a child-friendly comic book entitled "Hallo – jetzt reicht's" which deals with children's experiences of violence, bullying, blackmail, property damage and chatting on the internet, and teaches children how to behave in these situations. The comic is aimed at primary school children. |
|  | Germany | The program “Medienhelden” (Media Heroes”) is a universal, modularized, theory based and carefully evaluated preventive intervention for use in schools (7th-9th graders). The programme's objectives include: prevention of cyberbullying/victimisation and teaching children and young people to protect themselves online. “Medienhelden” aims to change attitudes and beliefs through the transfer of knowledge by providing students with definitions, teaching them the legal implications of cyberbullying, providing information on how cyberbullying impacts the victim and promoting empathy with the victims of cyberbullying. |
| **Cybermobbing guide**<br>  | Luxembourg | The Guide "Cybermobbing" is the result of an intense collaboration between the Police and BEE SECURE. It provides practical advice on how to proceed in the case of cyber-harassment for police officers and victims. The flyer also points out the necessity of an appropriate psychological support of victims and who to contact in order to request such help. https://police.public.lu/fr/publications/2018/20180220-cybermobbing.html |

| | | |
|---|---|---|
| **http://www.childprotection.lu** | Luxembourg | ECPAT Luxembourg, together with the Police and BEE SECURE initiative launched a website via which victims or witnesses of sexual exploitation or abuse of children can report such incidents. |
| **"Mana drošība" (Eng: "My safety")** | Latvia | The State Police Mobile App "Mana drošība" is for anyone who cares about their safety on the road every day. It is an easily accessible and easy-to-use tool that enables the user to get information on current and important security issues, test or supplement his knowledge by completing an interactive safety test, and find out what the right action after an incident. Additionally, this app provides an opportunity to communicate with the State Police in a convenient way when reporting on such incidents. |
| **http://www.vp.gov.lv/pasaka/** | Latvia | State Police of Latvia takes actions on online safety for children starting from an early age. There has been a development and distribution of a board game for children (age 5-9), which also includes various aspects of internet safety. In addition, the State Police of Latvia has developed a storybook for children (age 5-9) and their parents, which includes educational aspects on cyberbullying and internet pornography. The interactive version of the material in Latvian is available on this website: http://www.vp.gov.lv/pasaka/ |
| **Juvenile inspectors of the State Police of Latvia** | Latvia | In 2017 they organised 162 interventions about online safety, indicating possible threats in the virtual environment (the amount of personal information provided, correspondence with unknown persons, potential offensive features, etc.). Juvenile inspectors conducted lectures on communication on the Internet and the topics "Internet Security", "About the Internet", "Your Internet Security", and lectures on the challenge game "Blue Whale". |
| **"The White Dot Tolerance"-project** | Romania | It was implemented in Deva City during the period 1st of May – 19th June 2015 and it addressed to teenagers aged 15-17, teachers and parents. The aim of the project was to prevent the serious effects of cyber bullying in the physical and psychological development of young people/adolescents. It's activities were: a debate, an intensive training course for 25 pupils, a meeting with 27 parents, a human street exhibition (human chain) and six information activities in schools to raise awareness. |

Awareness and primary prevention:

| Project/ programme | MS or other countries | Description |
|---|---|---|
| **Saferinternet.at** | Austria | Saferinternet.at is the information and coordination centre for safer internet use and media competence in Austria. Saferinternet.at supports internet users, with a special focus on children, youth, parents and educators, in safer use of digital media. The rich portfolio of ongoing activities includes the website www.saferinternet.at, free school resources and booklets, workshops and helpline services throughout Austria, as well as networking with relevant players and being a contact point for journalists. |
| | Austria | The topics of violence and addiction prevention are summarized in the overall concept "UNDER18" and are subdivided into the programmes "All Right - Everything is right!", "Click & Check" and "Look@your.Life". Each of these programs meets criteria that are essential for proper implementation and sustainability. The violence prevention program "Click & Check" deals with the promotion of responsible use of digital media. In addition, special attention is paid to preventive legal information in particular with the youth protection regulations, as young people in their most varied life worlds are confronted with various legal provisions. http://www.bundeskriminalamt.at/205/start.aspx |
| | Austria | The Austrian helpline for children need of support regarding sexual exploitation as well as other questions. https://www.rataufdraht.at/ |
| | Belgium | Child Focus is the Belgian Safer Internet Centre. On their website is information given on safe internet usage. http://www.childfocus.be/fr/prevention/clicksafe-tout-sur-la-securite-en-ligne |
| **Cyberscout Training Programme**  | Bulgaria | For 12-15 year olds. This training programme aims to educate students about the most common online threats and the ways to prevent them, as well as to teach them how to share the skills they have learned with their peers. During a parallel session, their teachers are also introduced to the programme and the ways in which they can cooperate with the students and help them organise different events for raising awareness among other students about the online threats and the ways to address them. The programme is financed by Telenor Bulgaria and is realised with the help of the Ministry of Interior. https://www.safenet.bg/en/initiatives/173-cyberscouts-teams |

| | | |
|---|---|---|
| **An awareness raising video on child pornography** | Cyprus | In cooperation with the Cyprus Police Press Office, the Office for Combating Cybercrime (OCC) has prepared a short video related to cyber bullying and child sexual exploitation. which is accessible via the Internet and is frequently presented on TV. http://www.cypruspolicenews.com/ArticleSideGallery/ArticleID=7026 |
| **Schau hin!** | Germany | On its website, the initiative provides information on media and media use with the aim of empowering parents and families to play a greater role in media education, ensuring that children have access to the opportunities media can offer, while at the same time minimising the risks. https://www.schau-hin.info/ |
| **Medienscouts** | Germany | Works with a peer-education approach, such as the Bulgarian Cyberscout Training Programme. http://www.medienscouts-nrw.de/ |
| **Guide "Im Netz der Neuen Medien"** | Germany | the "ProPK" programme (joint police crime prevention programme of the German federal authorities and federal states) published a guide on new media. This publication provides readers with comprehensive knowledge for promoting media literacy among children and young people. It allows readers to develop a fundamental understanding of key new-media related issues, including cyberbullying. https://www.polizei.sachsen.de/de/dokumente/Landesportal/ImNetzderNeuenMedien-Web1.pdf |
| **Best Practice Paper "Self-harm behavior"**   | Germany | jugendschutz.net has published guidelines for social media platform operators on self-harming behavior in a best practice paper with support from the National Suicide Prevention Programme, the Wiener Werkstätte for Suicide Research and the Federal Eating Disorders Association. They provide guidelines for evaluating content promoting self-harm, contains recommendations for proactive measures and includes a list of counselling services. The guidelines are available in German: http://www.jugendschutz.net/fileadmin/download/pdf/Best_Practice_Paper_Selbstgefaehrdung.pdf and English:(https://www.jugendschutz.net/fileadmin/download/pdf/Best_Practice_Paper_Self_harm_behavior.pdf). |
| **Factsheet "Blue Whale"**  | Germany | jugendschutz.net has also published a fact sheet about the "Blue Whale Challenge" for press enquiries. Available in German: https://www.suizidprophylaxe.de/aktuelles/ansicht/news/detail/News/fact-sheet-zum-thema-blue-whale-challenge-15/ |

| | | |
|---|---|---|
| **Cyber Crime Division of the Hellenic Police HQ** | Greece | The Cyber Crime Division of the Hellenic Police HQ, is responsible for Internet issues that involve minors. They implemented some innovative acts: informative lectures and workshops for students, parents and teachers, teleconferences with schools, educational visits from schools and other entities, informative leaflets and TV spots (cyberbullying was introduced in 2014). Additionally, they have two websites regarding cyber safety: www.cyberkid.gr , www.cyberalert.gr |
| | Luxembourg | BEE SECURE is a joint initiative of the Ministry of the Economy, the Ministry of Family, Integration and the Greater Region and the Ministry of National Education, Childhood and Youth. The BEE SECURE initiative includes actions to raise awareness of safer use of new information and communication technologies. BEE SECURE is also a project funded in part by the European Commission, which acts as a Luxembourgish awareness center within the pan-European Insafe network. https://www.bee-secure.lu/de |
| **Cyber-Mobbing Erste-Hilfe App** | Germany, Luxembourg | In short video clips the guides, a boy and a girl, give concrete behaviour tips, talk about courage and accompany a child in their first steps to combat cyberbullying. Apart from the legal background information and links to counselling centres there are tutorials to report, block or delete insulting comments on social media platforms. The app was designed and programmed by the young people of "klicksafe youth panel" for other youngsters. The Luxembourgian app was adapted BEE SECURE and the BEE SECURE Youth Panel. www.klicksafe.de/youthpanel |
| **TAM – Together Against Mobbing** | Luxembourg | TAM was a project led by the Luxembourgian Police together with a high school and other partners. Three awareness raising videos were produced, one of these videos was dealing with cyberbullying. https://police.public.lu/fr/prevention/programmes/20171026-tam-prev.html |
| **"Child on-line" campaign** | Poland | An important part of this campaign, apart from media activities, is the wide range of educational material offered. This was prepared by the Nobody's Children Foundation and is aimed at children, adolescents, their parents and the professionals. In this campaign an innovative course called "Child on-line" was created. It shows various aspects of the sexual abuse of children on the Internet and other forms of threat to young Internet users (www.dzieckowsieci.pl). The current version of the campaign, titled "Protect your child in the network", concerns the protection of children against harmful Internet content. |

| | | |
|---|---|---|
| **The Project Prevention and Investigation of Child Pornography Cases on the Internet** | Romania | It focused on two major guidelines: enabling children to recognize abusive behaviour online and report it and enabling children to become aware of the fact that images displayed online are permanent and can be harmful. The project included an awareness campaign. |
| **Ora de Net (Eng: The Internet Class)** | Romania | It promotes Internet safety for children and adolescents. The project is focused on the virtual environment, having a central website (www.oradenet.ro) and a Facebook profile (https://www.facebook.com/SigurPeNet). It provides services such as: **awareness** building, **hotline** (for reporting illegal and harmful content online), **helpline** (a counselling line that is meant to offer guidance and advice to children, parents, teachers in cases referring to Internet related issues). More info may be found on the EUCPN webpage, Romania's good practice section. |
| stopline.sk | Slovakia | An online form for reporting illegal content or activities on the Internet and plays a key role in spreading the awareness of this type of crime. This project has the function of a national centre for reporting illegal content or activities on the Internet. As a result of the cooperation of all parties involved in this project, the regular publication of statistical information on illegal content and activities on the Slovak Internet and the identification of new trends in cybercrime will also result in a more effective fight against child abuse and other illegal phenomena on the Internet. |
| https://www.kybersikanovanie.sk/ | Slovakia | An online cyber-preventive program under the auspices of the civic association "eSlovensko". It discusses in detail what cyberbullying is and how to recognize it, what are the principles of protection against cyber-bullying, and also illustrates examples from Slovak schools and the world. The interpretation of the issue is complemented by educational films. |
| **deSHAME** PROJECT deSHAME | Hungary, Denmark and UK | It aims to increase reporting of online sexual harassment among minors and improve multi-sector cooperation in preventing and responding to this behaviour. In close consultation with young people, professionals, industry and policymakers, Project deSHAME will improve understanding and raise awareness of online sexual harassment. This project will develop a range of education, training and awareness materials as well as practical tools for multi-sector prevention and response strategies. The project will transfer this learning to other European countries and partners worldwide in order to promote young people's digital rights. http://www.childnet.com/our-projects/project-deshame/about-project-deshame |

| | | |
|---|---|---|
| **"Say no!" - campaign** | Europol | A campaign of Europol to raise public awareness and prevent online sexual coercion and extortion of children. https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime |
| **T.A.B.B.Y. (Threat Assessment of Bullying Behavior in Youth)** | EU | It addresses negative challenges faced by teachers, school counselors, instructors, chief directors, parents and students related to youths' use of digital media, the Internet and cell phones and other interactive device: mainly cyberbullying, cyber threats and sexting. The project aims to increase knowledge, skills to protect young people when using internet, mobile, social networks, school but also off-campus from victimisation by peers or other youngsters or adults by setting up a system for school officials and students themselves for the identification of risk factors and assessment of cyberbullying, cyberthreats and sexting and take adequate preventive actions to protect themselves and victims from such noxious behaviours. They created a game and several guidelines. http://ing.tabby.eu/ |
| **Positive Online Content Campaign** | Better Internet for Kids | Content can help kids learn and develop skills, explore the internet, and motivate them to take part as active citizens in our digital society. At the same time, it is important that they are protected from potentially harmful content and learn what appropriate content is, and how they can find and access it. https://www.betterinternetforkids.eu/web/positiveonlinecontent |
| **Let's talk about sexting** | USA | The intent of these presentations is to provide a starting place or a template for your program when responding to requests, typically from schools, for basic information or awareness raising presentations. They have included the key points and best practice approaches to discussing the topic and expect you may customize some aspects of the slides to meet your community's needs, experiences, and resources. The slides contain detailed notes and considerations for the trainer. http://www.wcsap.org/lets-talk-about-sexting |
| **NetSmartz® online educator training program** | National Center for Missing & Exploited Children, Disney | NetSmartz® Workshop and Disney have teamed up to offer a self-paced, online training program to help you teach Internet safety and prepare kids to be better digital citizens. This training will cover the issues of: Digital literacy & Ethics, Inappropriate Content, Online Sexual Solicitation, Online Privacy, Sexting, Cyberbullying and Practical Cybersecurity. https://www.netsmartz.org/Training |

| | | |
|---|---|---|
| **ThinkUKnow** | UK | This website provides information and educational material for different age groups. |
| **https://getsafeonline.org/** | UK | Get Safe Online is the UK's leading source of unbiased, factual and easy-to-understand information on online safety. The website provides practical advice on how to protect yourself, your computers and mobiles device and your business against fraud, identity theft, viruses and many other problems encountered online. |

### 4.3.Challenges for the projects

- ✓ Lack of evaluation: More projects should be evidence based. Evaluations are necessary to know if the measures work effective, efficient, what impact they have and how it was processed.
- ✓ Lack of knowledge: Prevention projects deal with complex problems. Partnerships should be made with the scientific and academic world to gain more knowledge on the new forms of cybercrime and new procedures and research methods can be established. Also interacting with other existing projects to share experiences and information.
- ✓ Persistency: They have to persevere in their projects; a lot of them are not updated or just end after some time. Short term projects are proving to have lesser effects.

## 5. Conclusion

For the prevention of online criminal acts regarding children, it is necessary for all to be on the same page, as cybercrime is a global problem. Children are extra vulnerable on the internet and specific needs should be kept in mind. The measures taken by the international agencies should serve as an overall structure for the national policies to accomplish an effective instrument in the fight and prevention against online crimes. It is required to operate a uniform definition for these types of cybercrime, especially child sexual exploitation and abuse, and cyberbullying. Only if the Member States and Europe maintain the same mind-set, measures and recommendations can be made.

The best way to prevent children from these crimes is to be transparent in every way. Information should be clear and objective so that children know what the dangers are as well as the opportunities. They do not need to be scared off. Important stakeholders should be hold accountable for preventing these crimes: online providers, policy makers, parents or guardians, educators, media, etc. Therefore it is essential for them to know what is going in cyberspace and how they can affect a child's behaviour.

The big scare created by the media is that an adult will approach a child online and sexually abuse or exploit them or coerce them into doing sexual activities with them. Research proved that children deal more with other risks, such as privacy violations, cyberbullying, in-app purchases … and perpetrators are more likely to be their peers. Internet education in schools should thus not only deal with the child as victim, but also as an offender.

**Recommendations**:

- In a number of studies it is stated to emphasise the opportunities instead of the risks on the internet. Nevertheless, most studies focus on these risks.
- In general more research is needed on these topics and the latest developments. The social media, internet and devices evolve so quickly that researchers and law agencies cannot keep up.
- Nevertheless, perhaps the most important recommendation is for the stakeholders to all work together on this issue to build a safe online environment for children

Finally, the Secretariat would like to thank all the Member States (AT, BE, BG, CY, FI, DE, EL, LT, LU, PL, RO, SK and SE) that filled in the questionnaire concerning this topic. With your help the paper could give some more insight in the different policies and the prevention projects.

## 6. Bibliography


Safer Internet Forum Secretariat. (2018). *Safer Internet Forum*. Retrieved April 5, 2018, from Better Internet for Kids: https://www.betterinternetforkids.eu/web/portal/policy/safer-internet-forum

American Psychiatric Association. (2013). *The Diagnostic and Statistical Manual of Mental Disorders , Fifth Edition.* Washinton DC.

Apple. (2018). *About in-app purchases*. Retrieved April 5, 2018, from Apple: https://support.apple.com/en-us/HT202023

Bastiaensens, S. (s.d.). *Dossier: Wat is cyberpesten?* Retrieved February 21, 2018, from Mediawijs: https://mediawijs.be/dossiers/dossier-cyberpesten/wat-cyberpesten

BBC News. (2014, July 30). How many men are paedophiles? *BBC News magazine*.

BeSafe. (2018). *Cyberpesten.* Retrieved March 1, 2018, from BeSafe: https://www.besafe.be/sites/besafe.localhost/files/u16/cyberpesten.pdf

Better Internet for Kids. (s.d.). *GUIDE TO ONLINE SERVICES*. Opgehaald van Better Internet for Kids: https://www.betterinternetforkids.eu/web/portal/onlineservices

Better Internet for Kids. (s.d.). *INSAFE AND INHOPE*. Retrieved April 5, 2018, from Better Internet for Kids: https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope

Bishop, J. (2013). *Examining the Concepts, Issues, and Implications of Internet Trolling.* Hershey, Pennsylvania, USA: IGI Global.

Bureau Jeud en Media. (2017, May 18). *Wat je moet weten over de 'blue whale'-challenge*. Retrieved February 16, 2018, from Bureau Jeugd en Media: https://www.bureaujeugdenmedia.nl/blue-whale-challenge/

Byrne, J., Kardefelt-Winther, D., Livingstone, S., & Stoilova, M. (2016). *Global Kids Online: Research Synthesis 2015 - 2016.* UNICEF Office of Research–Innocenti and London School of Economics and Political Science.

Cantone, E., Piras, A. P., Vellante, M., Preti, A., Daníelsdóttir, S., D'Aloja, E., . . . Bhugra, D. (2015). Interventions on Bullying and Cyberbullying in Schools: A Systematic Review. *Clinical Practice & Epidemiology in Mental Health* (11), 58–76.

Child Focus. (s.d.). *Grooming*. Retrieved February 21, 2018, from Child Focus: http://www.childfocus.be/nl/seksuele-uitbuiting/grooming

Childnet. (2017). *Childnet Response to the DCMS Internet Safety Strategy Green Paper.* United Kingdom: Childnet.

Cohen-Almagor, R. (2013, March 21). Online Child Sex Offenders: Challenges and Counter-Measures. *The Howard Journal of Criminal Justice, 52*(2), 190-215.

Commission for the Protection of Privacy. (2018). *Sharenting*. Retrieved March 13, 2018, from Ik Beslis: https://www.ikbeslis.be/ouders-leerkrachten/sharenting

CORDIS. (2017). *MYMOVEZ Report Summary: Periodic Report Summary 2 - SNIHCY (Social Network Implementation of Health Campaigns Among Youth).* European Commission.

Council of Europe. (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse . *CETS No.201*. Lanzarote.

Dalla Pozza, V., Di Pietro, A., Morel, S., & Psaila, E. (2016, July). Directorate General for Internal Policies. Policy Department C: Citizen's rights and constitutional affairs. Cyberbullying among young people. (Study). Brussels, Belgium: European Parliament: Policy Department for Citizen's Rights and Constitutional Affairs.

De Bie, E., & Day, J. (s.d.). *Sexting... Oké of niet oké?* Retrieved February 28, 2018, from sexting.be: https://sextingopschool.mediawijs.be/okeofnietoke

De Kimpe, L., & et al. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics*.

Douglas, D. M. (2016). Doxing: a conceptual analysis. *Ethics and Information Technology, 18*(3), 199-210.

Durham, M. G. (2008). *The Lolita-effect: The Media Sexualization of Young Girls and What We Can Do About It.* The Overlook Press.

EC3 Europol. (2017). *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2017.*

EC3 Europol. (s.d.). *First Year Report.*

ECPAT. (2016). *About ECPAT.* Retrieved from ECPAT: http://www.ecpat.org/about-ecpat/

ECPAT; INTERPOL. (2018). *Towards a global indicator on unidentified victims in child sexual exploitation: Summary Report.* Bangkok.

eNACSO. (2015, September 29). Your Right to Choose online.

eNACSO. (2016, May 25). Recommendations from When "free" isn't.

eNACSO. (2016). *When "free" isn't: Business, Children and the Internet.* Rome: eNACSO.

Erreygers, S. (2016). *Cyber-Shoc: Eindrapport schoolonderzoek.* Antwerp: Universiteit Antwerpen - Departement Communicatiewetenschappen.

EU Kids Online. (2017). *EU Kids Online*. Retrieved February 20, 2018, from LSE Media and Communications: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

EUCPN. (2015). Cybercrime: a theoretical overview of the growing digital threat . *EUCPN Theoretical Paper Series*. (EUCPN Secretariat, Ed.) Brussels: European Crime Prevention Network.

EUCPN. (2015). Preventing Cybercrime: policies & practices. *EUCPN Toolbox Series n°8*. (EUCPN Secretariat, Ed.) Brussels: European Crime Prevention Network.

EUCPN. (2017). Cyber Safety: A theoretical Insight. *EUCPN Theoretical Paper Series*. (EUCPN Secretariat, Ed.) Brussels: European Crime Prevention Network.

EUCPN. (2017). Cybersecurity and Safety: Policy and best practices. *EUCPN Toolbox series n°12*. (EUCPN Secretariat, Ed.) Brussels: European Crime Prevention Network.

European Commission. (2010). *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A digital agenda for Europe.* Brussels: European Commission.

European Commission. (2012, May 2). Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *European Strategy for a Better Internet for Children, COM(2012) 196 final*, 2. Brussels.

European Commission. (2012, May 2). Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *European Strategy for a Better Internet for Children, COM(2012) 196 final*. Brussels.

European Commission. (2017). *Europeans' attitudes towards cyber security.*

European Commission. (2017, April 12). Report from the Commission to the European Parliament, the European Council and the Council:Sixth progress report towards an effective and genuine Security Union. *COM (2017) 213 final*. Brussels: European Commission.

European Commission. (2017, May 9). *Safer Internet Centres*. Retrieved April 5, 2018, from https://ec.europa.eu/digital-single-market/en/safer-internet-centres

European Commission. (2018). *Child sexual abuse*. Retrieved from Migration an home affairs: https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/child-sexual-abuse_en

European Commission. (2018, March 22). *From a Safer Internet to a Better Internet for Kids*. Retrieved April 5, 2018, from https://ec.europa.eu/digital-single-market/en/content/safer-internet-better-internet-kids

European Commission. (s.d.). *Can personal data about children be collected?* Retrieved from European Commission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/how-my-personal-data-protected/can-personal-data-about-children-be-collected_en

European Parliament & The Council. (2011, December 13). DIRECTIVE 2011/92/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Strasbourg.

EUROPOL. (2017). *The EU Serious and Organised Crime Threat Assessment: Crime in the age of technology.* EUROPOL.

Eurostat. (2018, March 15). Internet use: participating in social networks (creating user profile, posting messages or other contributions to facebook, twitter, etc.) .

EXPOO. (s.d.). *Grooming*. Retrieved February 21, 2018, from Expertisecentrum Opvoedingsondersteuning van de Vlaamse overheid: https://www.expoo.be/grooming

Google Play. (2018). *Make in-app purchases in Android apps*. Retrieved April 5, 2018, from Google Play Help: https://support.google.com/googleplay/answer/1061913?hl=en

Hamari, J., Koivisto, J., & Sarsa, H. (2014). Does Gamification Work? -- A Literature Review of Empirical Studies on Gamification. *2014 47th Hawaii International Conference on System Sciences*, (pp. 3025 - 3034). Waikoloa, Hawaii.

Hasinoff, A. A. (2011, January). *No right to sext? A critical examination of media and legal debates about teenage girls' sexual agency in the digital age.*

Hasinoff, A. A. (2016). How to have great sext: consent advice in online sexting tips. *Communication and Critical/Cultural Studies, 13*(1), 58-74.

Heirman, W., & Walrave, M. (2008). Assessing Concerns and Issues about the Mediation of Technology in Cyberbullying. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*(2), article 1.

Hinduja, S., & Patchin, J. W. (2010). Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research, 14*(3), 206-221.

Hinduja, S., & Patchin, J. W. (2012). *School Climate 2.0: Preventing Cyberbullying and Sexting One Classroom at a Time.* United States of America: Corwin.

HOWEST. (s.d.). Retrieved from Re:Pest: http://repest.howest.be/

INHOPE Foundation . (2017, October). *Our Participants*. Retrieved April 19, 2018, from INHOPE Foundation: http://www.inhopefoundation.org/network/members

INHOPE. (s.d.). *At a glance*. Retrieved April 19, 2018, from INHOPE: http://inhope.org/gns/who-we-are/at-a-glance.aspx

Instagram. (2018).

INTERPOL. (2018). *Crimes against children: Victim identification*. Retrieved April 24, 2018, from INTERPOL: https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

INTERPOL. (2018). INTERPOL's International Child Sexual Exploitation (ICSE) database.

INTERPOL. (2018). *Victim Identification*. Retrieved April 27, 2018, from INTERPOL: https://www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification

Jongerenparlement. (2016, January 29). AANBEVELINGEN. Jongerenparlement: recht op afbeelding. *Commissie: Beeldmateriaal op sociale media. Aanbeveling 3*. Kamer van volksvertegenwoordigers, Halfrond, Brussels, Belgium.

Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-based Methods and Strategies for Training and Education.* San Francisco: John Wiley & sons.

Kaspersky Lab. (2018). *Top Seven Dangers Children Face Online: How to Keep Them Safe*. Retrieved March 13, 2018, from https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online

Koppen. (2015, December 2). Mag ik je vriend worden? (VRT, Ed.)

Korkmazer, B., De Ridder, S., & Van Bauwel, S. (2018). *Who does not dare, is a pussy : a textual analysis of media panics, youth, and sexting in print media in Northern Belgium.* Presented at the 68th Annual ICA Conference.

Lievens, E. (2017, March 30). Consent, awareness and harm – analysing sexual images. (INHOPE, Interviewer) Better Internet for Kids.

Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). *EU Kids Online: Final Report 2011.* London: EU Kids Online Network.

Livingstone, S., Mascheroni, G., & Ólafsson, K. (2014). *Children's online risks and opportunities: Comparative findings from EU Kids Online and Net Children Go Mobile.*

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe.* London: EU Kids Online Network.

Livingstone, S., Mascheroni, G., & Staksrud, E. (2015). *Developing a framework for researching children's online risks and opportunities in Europe.* EU Kids Online.

Macnab, A. J., Deevska, M., Gagnon, F., Cannon, W. G., & Andrew, T. (2009). Asphyxial games or "the choking game": a potentially fatal risk behaviour. *Injury Prevention*(15), 45-49.

Madigan, S., Ly, A., Rash, C. L., Van Ouytsel, J., & Temple, J. R. (2018). Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics*.

McKenzie, R. N. (2008). *The Path to Addiction...: "And Other Troubles We Are Born to Know.".* Bloomingdale, Indiana: AuthorHouse.

Mediawijs. (s.d.). *Cyber-Scan om je school een anti-cyberpestbeleid te geven*. Retrieved March 1, 2018, from Mediawijs.

Merzlikin, P. (2017, July 27). The kids aren't alright Why Russian adolescents are selling self-created pornography online. *Meduza*.

Milkaite, I., & Lievens, E. (2018, April 16). *Mapping the GDPR age of consent across the EU: April 2018 update*. Retrieved April 17, 2018, from Better Internet For Kids:

https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3017751

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2003, March). The Exposure of Youth to Unwanted Sexual Material on the Internet. *Youth & Society, 34*(3), 330-358.

Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2012, January). Prevalence and Characteristics of Youth Sexting: A National Study. *Pediatrics, 129*(1).

Moncur, W., Orzech, K. R., & Neville, F. G. (2016). Fraping, social norms and online representations of self. *Computers in Human Behavior, 63*, 125-131.

National Foundation for Educational Research. (2010). *Children's online risks and safety: A review of the available evidence.* UK Council for Child Internet Safety.

NCMEC. (2018). *Sextortion*. ( National Center for Missing & Exploited Children) Retrieved April 25, 2018, from Missing Kids: http://www.missingkids.com/theissues/onlineexploitation/sextortion

Net Children Go Mobile. (2013). Retrieved February 14, 2018, from http://netchildrengomobile.eu/

Norden, S. (2013). How the Internet has Changed the Face of Crime. Florida Gulf Coast University.

NSPCC. (2018). *Sexting*. Retrieved April 3, 2018, from NSPCC: https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/sexting/

Peeters, M. P., Elffers, H., van der Kemp, J., & Beijers, W. M. (2011). *Evidence- based aanpak van woninginbraak: Enkele voorstellen voor een intensievere aanpak van woniçnginbraak, op basis van een inventarisatie van de criminologische literatuur.* Amsterdam: Vrije Universiteit Amsterdam.

SafeToNet. (2018). Retrieved April 5, 2018, from SafeToNet: https://www.safetonet.com/

Senker, C. (2017). *Cybercrime and the darknet: Revealing the hidden underworld of the internet.* London: Arcturus Publishing.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). *Who Falls for Phish? A Demographic Analysis of Phishing: Susceptibility and Effectiveness of Interventions*. Atlanta, Georgia, USA: ACM.

Staksrud, E., Livingstone, S., Haddon, L., & Ólafsson, K. (2009). *What do we know about children's use of online technologies?: a report on data availability and research gaps in Europe [2nd edition].* London: EU Kids Online Network.

Steinberg, S. B. (2017). Sharenting: Children's Privacy in the Age of Social Media. *EMORY LAW JOURNAL* (66).

Stop It Now . (2018). *About us*. Retrieved April 25, 2018, from Stop It Now: https://www.stopitnow.org/our-work/about-us

Stop it Now. (s.d.). Retrieved March 7, 2018, from Stop it Now: https://stopitnow.be/

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology & Behavior: the impact of the Internet, multimedia and virtual reality on behavior and society.*(7), 321-326.

The Times. (2017, December 27). Call for crackdown after claims YouTube is shop window for child abuse. *The Times*.

United Nations. (1989, November 20). *Convention on the Rights of the Child; Art. 16 §1.* Retrieved March 13, 2018, from http://www.refworld.org/docid/3ae6b38f0.html

UNODC. (2015). *Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children.* New York: United Nations.

Urban Dictionary. (2011, May 25). Retrieved March 23, 2018, from Urban Dictionary: https://www.urbandictionary.com/define.php?term=Fraping

Van Ouytsel, J., Walrave, M., & Ponnet, K. (2018, May). Adolescent Sexting Research: The challenges ahead. *JAMA Pediatrics, 172*(5).

Vanhoeck, K. (2015, July - September). Preventieve hulp voor mensen met pedofiele gevoelens. *Tijdschrift Klinische Psychologie, 45*(3).

VICE. (2018, February 26). *A Complete History of Happy-Slapping*. Retrieved May 7, 2018, from https://www.vice.com/en_uk/article/437b9d/a-complete-history-of-happy-slapping

WePROTECT Global Alliance. (2015). *Our Mission and Strategy*. Retrieved from WePROTECT Global Alliance to End Child Sexual Exploitation Online: https://www.weprotect.org/our-mission-and-strategy/

Wolak, J., & Finkelhor, D. (2016). *Sextortion: Findings from a survey of 1,631 victims.* Crimes against Children Research Center.

YouTube. (2018). *YouTube Help*. Retrieved April 20, 2018, from YouTube: https://support.google.com/youtube/answer/2950063?hl=en

Zaman, B., & Nouwen, M. (2016). *Parental controls: advice for parents, researchers and industry.* EU Kids Online.