



Foreword



Christoph HilligenBoard Member, World Vision
Deutschland e.V.

The digital revolution has created entirely new living conditions and risks for children, which differ from those experienced by older generations. Even today's generation of parents, some of whom might see themselves as "digital natives", are quickly being left behind by the ever-evolving

developments, especially in the area of social media and online gaming. Globally, one in three users of the Internet is a child and it is precisely children who are constantly exploring new digital frontiers. In doing so, they swiftly move across national borders, just like the Internet itself. The dangers they face are global in nature and can only be solved through cross-border research and international cooperation.

This is why, for the purposes of this research, we worked in collaboration with our partner offices in India, the Philippines and Thailand. Through their programme work in the area of sexual violence online, they have developed a high level of expertise and are thus ideal partners for harnessing the opportunities of postcolonial development cooperation: learning from and with each other on an equal footing.

Conversations with experts and affected individuals paint a picture of highly complex challenges. Not only does the Internet make it possible to exploit children from a distance with its ever-expanding digital worlds transcending national borders (e.g., through intermediaries via livestreaming), it also provides perpetrators with the possibility of making numerous attempts (effortlessly reaching out to hundreds of children through what is known as cybergrooming, via social media or gaming platforms).

In a world altered by the COVID-19 pandemic, the opportunities for such acts have increased even further. Through the long months of distance learning, even younger children were spending more and more time on the Internet. If they did not have it previously, now even children from low-income households have access to a smartphone as a result of the pandemic. However, in some cases, especially in global South countries, families may be so severely affected by poverty in other aspects of their lives that they will knowingly accept or even facilitate the online abuse of their children for monetary gain. In Germany, too, incidents continue to come to light in which children create sexual content and distribute it over the Internet in exchange for money.

The interviewed experts emphasise that solutions can only be found if there is more effective cooperation between the various areas, including prevention, assistance, education, and law enforcement. Not only politicians, but also technology companies, should be held to account. This study aims to illustrate how these complex challenges can be faced through coordinated, transnational efforts in prevention, assistance, and law enforcement.

Best wishes,

Silog Filling

Legal information

Publisher: World Vision Deutschland e.V.

Authors: Dr Ekkardt Sonntag, Prof. Dr Caterina Rohde-Abuba, Kristina Kreuzer

Data services: Human8, Happy Thinking People

Design and consultation: Wortballon, Klaus Schickor, Uwe Kobler

This work and its parts are protected by copyright. Any use in cases other than those permitted by law shall require the prior written consent of the World Vision Institute: www.worldvision.de/informieren/institut

Printed on 100% recycled paper

Last updated: September 2023

Content

	Foreword	3
1.	Introduction	6
2.	Theoretical and methodological concept of the study	12
2.1	Digital lifeworlds of young people today	13
2.2	Theoretical and legal foundations concerning sexual violence in the digital space	13
2.3	Study methodology	14
2.4	Incidence and limitations	15
3.	Findings from the interviews	16
3.1	Forms of violence and threats	17
3.2	Factors behind sexual violence in the digital space	23
3.3	Assistance and prevention	28
4.	Conclusions	38
5.	Political demands	42
6.	Appendix: Overview of interviews	44
7.	Bibliography	46

01.Introduction

From a global perspective, roughly one in three individuals who use the Internet today is under the age of 18 (Wright and Rotino 2020, 6). The Internet is an expanding virtual space in which sexual violence¹ against children has taken on new forms and manifestations (ECPAT Deutschland 2023). The Internet and its future developments, such as artificial intelligence and augmented reality, are continually creating new spaces with innovative ways of communication and, thus, new opportunities for perpetrators. Consequently, the stakeholders involved, including policymakers, law enforcement, platform providers, and researchers, are being faced with a significant challenge to ensuring the protection of children and safeguarding their rights.

Digitisation has led to an increase in the observed severity of cases of sexual violence. An analysis of depictions of sexual abuse of children (Salter and Whitten 2022) compares the current situation with the time before the widespread use of the Internet by the general public in the mid-1990s. The study is based on a randomly selected set of 1,004 instances of abuse material from various countries, retrieved from a Canadian archive and dating exclusively from before 1995. When the material is compared to depictions from the 2008–2015 period, it is clear that the more recent depictions tend to be more extreme. Salter and Whitten speculate that this is related to a dynamic of child abuse known in the analogue realm: when acts are committed in groups in the analogue world, the offences tend to be more severe. The existence of relevant forums makes it much easier to create a group setting. Digital networking allows perpetrators to feel part of a like-minded group.

Accessing and consuming abuse material has been significantly simplified by digitisation, thereby intensifying abuse in the analogue realm in at least two ways. Not only is there analogue abuse behind all new digital abuse material, but there are also indications that increased consumption of abuse material is likely to result in the consumer eventually arranging an analogue meeting (Insoll et al. 2022, 14).

Since the late 2000s, social media has attracted an increasingly broad range of Internet users. At around the same time, smartphones and chat services entered the mass market. These developments have fundamentally changed the way in which abuse material is distributed

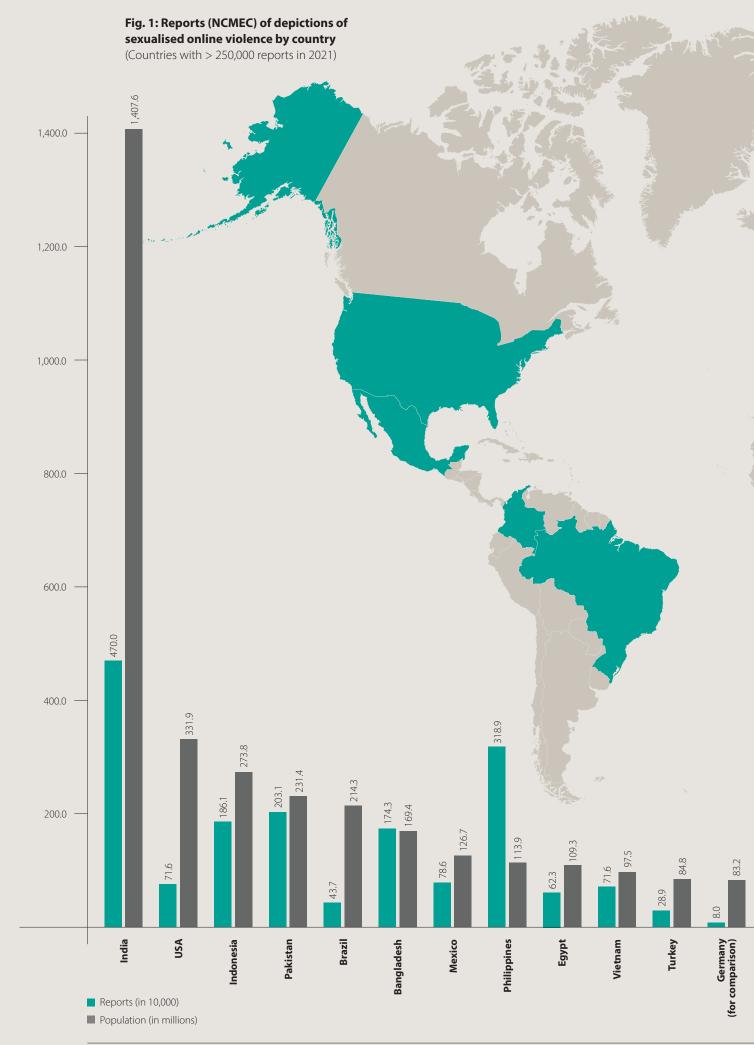
and dramatically increased its incidence. While studies on search engine queries before 2010 provided almost reassuring results (Steel 2009, 58), a representative study by the State Media Authority of North Rhine-Westphalia (Nennstiel and Isenbarg 2021) of 2,163 children and adolescents aged 8 to 18 has found that, nowadays, over one-quarter of the respondents have been asked online by an unknown adult to meet them in the analogue world. This change can be attributed to the multitude of social media and online gaming platforms that have gained widespread popularity in recent years, incorporating multimedia functions and encryption, which facilitate many forms of online abuse that is prevalent nowadays.

While abuse material is increasingly exchanged and traded on the so-called darknet (the unregulated part of the Internet accessible through special browsers), a significant portion of abusive activities also occur on the clearnet (the part of the Internet used by the general public). The Canadian Center for Child Protection estimates that only about three percent of photos and videos containing abuse material is stored on the darknet; often, links shown there redirect to addresses on the clearnet (Bongen and Moßbrucker 2022). The solicitation of children also takes place on the clearnet, especially on social media and gaming platforms.

The Internet transcends national borders and the boundaries of time zones. Perpetrators and their victims can reside in different time zones and on different continents. This is particularly evident in the case of so-called livestreaming. In this case, offenders, who tend to be from the global North, connect with children in the global South via a local intermediary. These transnational structures of abuse can therefore involve different jurisdictions, posing significant challenges in the area of prevention and intervention.

In order to examine national and transnational dynamics of sexual violence against children on the Internet, along-side data collected in Germany, we included data from three additional countries which are part of the international World Vision Partnership: India, Thailand, and the Philippines. The selection of these country contexts is based on a combination of reported cases of abuse material in absolute numbers and per capita (see Fig. 1 and 2) as well as the practicality of data collection in the respective country contexts whilst ensuring uniform standards.

¹ In this study, the term "sexual violence" is used as an umbrella term that encompasses abuse and exploitation involving sexual content or for the satisfaction of the sexual needs of the perpetrator or consumer (cf. ECPAT International 2016, 14).



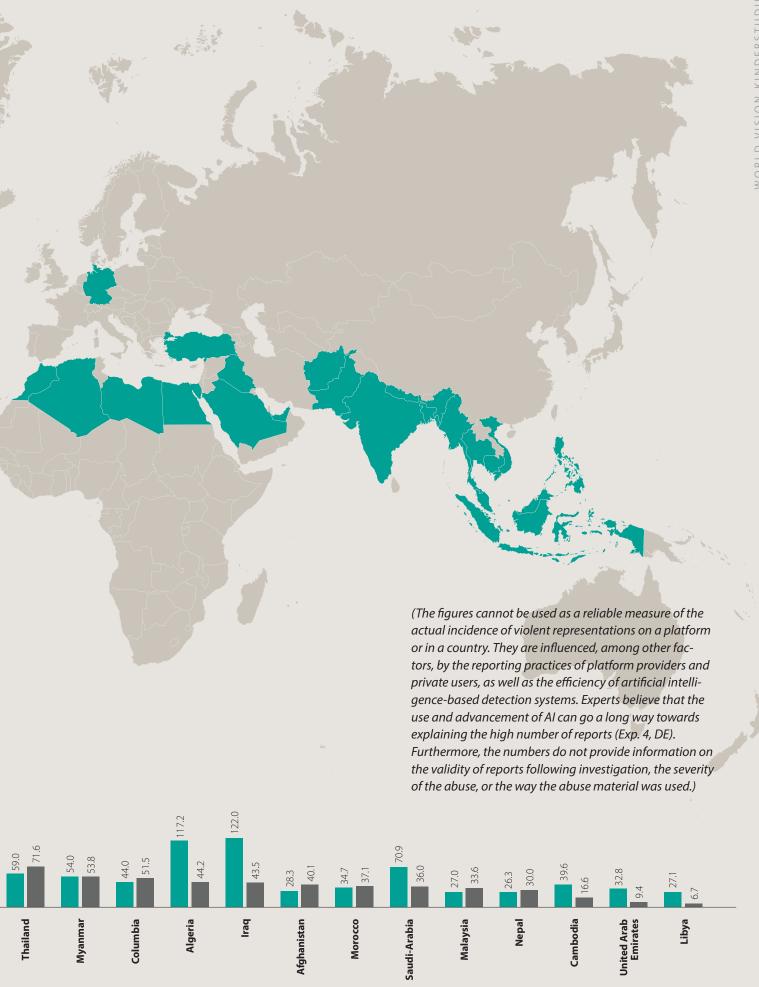
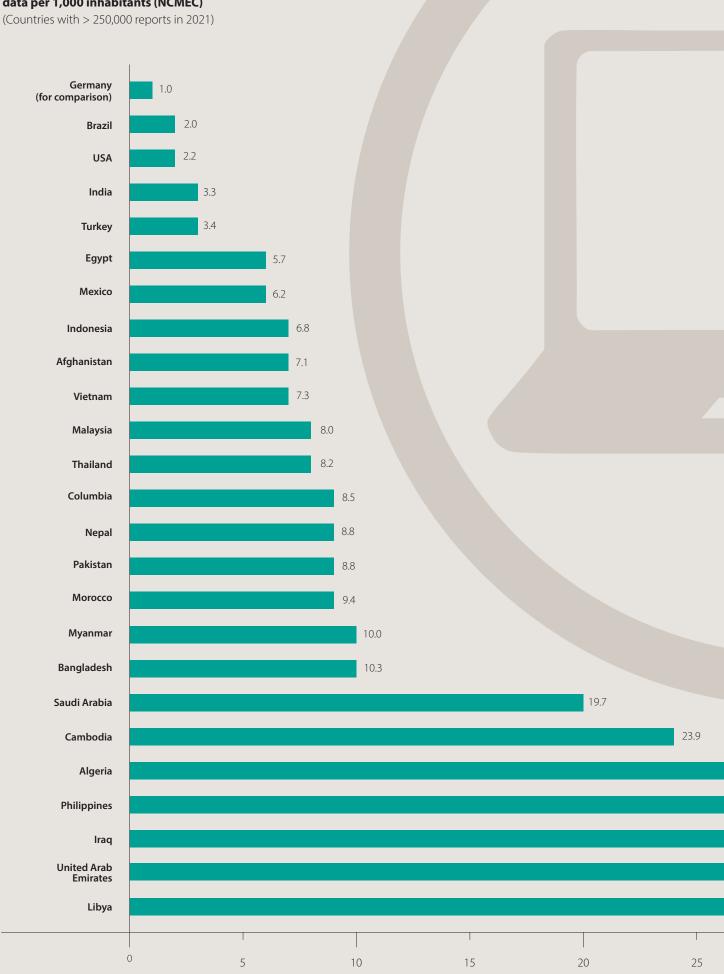


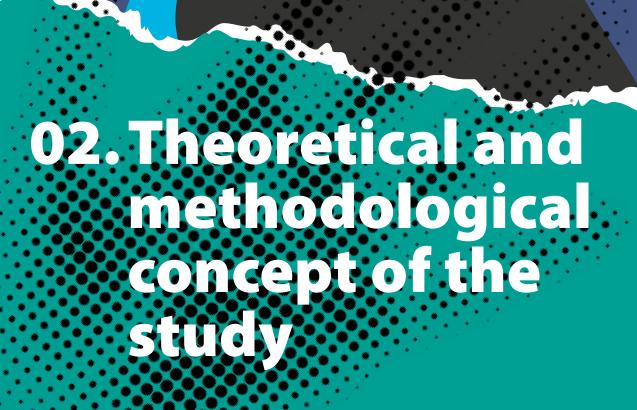
Fig. 2: Reports of depictions of sexualised online violence, data per 1,000 inhabitants (NCMEC)



28.0 28.0 40.2 30 35 40

Based on qualitative expert interviews and interviews with affected children, the study initially attempts to identify and explore various forms of sexual violence against children online as well as the contexts in which it occurs. As part of this, the study also explores the influence of the pandemic, as a result of which children's daily lives have shifted more towards the digital realm. Finally, the study examines what needs-based prevention and assistance for affected children might look like, and what roles politicians, law enforcement agencies, the children themselves, their social environment, and internet platform providers can play.

(The figures cannot be used as a reliable measure of the actual incidence of violent representations on a platform or in a country. They are influenced, among other factors, by the reporting practices of platform providers and private users, as well as the efficiency of artificial intelligence-based detection systems. Experts believe that the use and advancement of AI can go a long way towards explaining the high number of reports (Exp. 4, DE). Furthermore, the numbers do not provide information on the validity of reports following investigation, the severity of the abuse, or the way the abuse material was used.)



Research projects of the World Vision Institute are anchored in childhood research approaches that view children as social actors in their environment. Our fundamental premise is that children are full-fledged members of society and we reject the proposal that they do not become these until after becoming adults (following Hengst and Zeiher 2005). Our research perspective focuses on how children themselves influence their lives and "express their own interests and needs in their decisions and actions" (Wihstutz 2019, 28). Particularly when it comes to safety in digital lifeworlds, in which adults participate far less than children, we must rely on their knowledge and experiences to develop needs-based protection concepts. Given the relatively weak development of digitisation (and digital competence) in Germany and the transnational structures of digital lifeworlds, albeit with their local specificities (Hosny et al. 2020, 3522), it is necessary to adopt a decolonised research approach that actively involves children from different parts of the world (Liebel 2017, 71).

2.1 Digital lifeworlds of young people today

In the countries studied, almost all² young people have access to the Internet, including those from socio-economically disadvantaged backgrounds. Their lifeworlds are strongly media-driven, many of their games and leisure activities are digital, for example, on TikTok and You-Tube (Fleer 2016), and their profiles on social networks, like Instagram, play a vital role in shaping their personalities. Digital lifeworlds offer diverse learning resources that are independent of adults (e.g., also covering taboo topics like sexuality or queer gender identities), while also enabling young people to self-organise, such as through WhatsApp groups (DeFelice 2017; Levine et al. 2021, 3; Zumbrängel 2020). In a highly polarised world marked by social inequality, digitisation appears to offer young people many opportunities for participation and networking beyond socio-economic classes and national borders. However, this also means that all young people are exposed to the risks posed by the Internet, as international and national norms and protective measures are significantly lagging behind technological advancements (Levine et al. 2021, 3).

Older generations struggle to keep pace with the rapid development of digitisation, leaving parents, educators, and youth workers alike with insufficient knowledge and skills to prepare young people to navigate the risks of digital lifeworlds. What exacerbates the situation is that Western parenting, in particular, tends to strongly emphasise

labelling safety risks for one's own children outside of their household as "stranger danger". Over the past 30 years, this has led to a significant reduction in children's freedom of movement and increased parental monitoring in the analogue world outside the household (DeFelice 2017, 577–78). This trend, which increasingly restricts children's freedoms to the privacy of their households (DeFelice 2017, 578), which are considered "safe", goes hand in hand with young people creating new freedoms for themselves on the Internet, with risks that adults are hardly aware of. Parents and professionals often feel overwhelmed by the issue and are sometimes resistant to addressing it (cf. Zumbrängel 2020, 37), without realising that for many young people a complete withdrawal from digital lifeworlds is no longer a real possibility (Levine et al. 2021).

2.2 Theoretical and legal foundations concerning sexual violence in the digital space

Sexual violence in the digital space poses serious threats to the safety of children, which is why it must be incorporated into national and international child protection legislation. In particular, within the context of international child protection, in which this study is anchored, the "human security approach" provides a suitable theoretical foundation. This approach, which originates from development cooperation in the 1990s, no longer places the security of states at the centre of political work, but instead examines the consequences of state policies for human security (Akgul, Gurer, and Aydin 2021, 61; Boracetti 2017). This new understanding of security puts a strong emphasis on the assertion that human security must be universal and applicable everywhere (Haq 1995, 115; Salminen and Hossain 2018, 111; Kjaerulf and Barahona 2010, 382–83). In addition to clear human rights obligations (e.g., the right to physical and mental health, Article 12 of the International Covenant on Economic, Social, and Cultural Rights) for contracting states, Article 19 of the 1992 UN Convention on the Rights of the Child demands the protection of all children from physical and mental abuse, explicitly including sexual abuse of children and the requirement for effective procedures for the identification, reporting, referral, investigation, treatment and follow-up of instances of child maltreatment. Article 34 of the Convention on the Rights of the Child expressly obliges contracting states to protect children from sexual exploitation by taking appropriate measures to prevent children's involvement in unlawful sexual activity and the exploitative use of children in prostitution and pornography.

² According to data from the International Telecommunication Union (2023a), as of 2021, the following percentages of the general population had 3G access on at least one device: 99% in India, 96% in the Philippines, and 99% in Thailand.

These requirements arising from human rights and children's rights must also be applied to digital lifeworlds, and states must be held responsible for the actions that they take in respect of safeguarding the rights of young people. Therefore, the UN Committee on the Rights of the Child, which is responsible for monitoring the implementation of the Convention on the Rights of the Child in contracting states, published an addendum to the Convention on the Rights of the Child (known as General Comment No. 25) in 2021 concerning the implementation of children's rights in the digital space, with explicit recommendations for action to be taken by states.

In addition to security risks related to data protection, privacy, and personal rights, digital lifeworlds can also give rise to forms of physical abuse (e.g., analogue physical abuse which is then filmed and uploaded online) and psychological abuse, such as sharing offensive content, abusive interactions between users through degradation, humiliation, or blackmail (cyberbullying), as well as the incitement, persuasion, or coercion to engage in offensive acts in the digital space or the analogue world. Experiences of violence on the Internet are therefore not limited to sexual content or activity3, but the high degree of societal taboo surrounding sexuality can facilitate and exacerbate the dynamics of power and exploitation in the digital realm. Since there are hardly any functioning age-specific protection structures on the Internet, young people of various ages and levels of maturity can interact with one another or with adults. On many apps or platforms, interactions are not moderated or monitored, resulting in the absence of safeguards (cf. Ali and Paash 2022; Durkin and DeLong 2012).

A special vulnerability factor for children and young people is the fact that they can be confronted with issues of sexuality in the digital space at a young age, when they are not yet at a developmental stage at which they could understand and deal with them.

At the same time, it must be recognised that digital lifeworlds can serve as places of learning for young people, where they can acquire knowledge about their sexuality that is not available or is taboo in their analogue lifeworlds and, moreover, they allow young people to express it. Therefore, the digitised sexuality of young people must also be viewed as a developmental opportunity, though

one that is fraught with the risks of the Internet and which requires appropriate sensitisation, for instance, regarding the possible dissemination of images or videos depicting sexual acts.

Adults who use the Internet have an advantage over children in terms of knowledge and experience, enabling them to use sexual content and actions for their own gratification and to manipulate children for this purpose. Children whose emotional needs are not satisfied in their life contexts can also be vulnerable, seeking affection and validation through online interactions, which can propel them into a spiral of sexual violence (Engfer 2006, 801). In the context of (mostly illegal and systematic) dissemination and marketing of sexual content and acts on the Internet, young people face strategically acting perpetrators with a certain level of organisation. This creates a strong power imbalance, which reaches its extreme form in organised crime through the enslavement of children for sexual exploitation online, which combines various components of violence.

2.3 Study methodology

The data for the study was collected between autumn 2022 and spring 2023. During this period, 27 problem-based, structured, qualitative interviews of 60–90 minutes in length were conducted. Experts from around the world were invited, among others, from the fields of social work, media, advocacy, science and law enforcement. They came from governmental, non-governmental and multilateral organisations. In the countries where World Vision is systematically addressing the issue of sexual violence online (India, the Philippines, and Thailand), interviews were conducted with affected individuals who were willing to share their experiences with sexual violence online in their childhood or adolescence. During the interviews, utmost care was taken to protect the interviewees against possible retraumatisation.

The interviews were transcribed and those which were not conducted in either German or English were translated into English. They were then analysed using the qualitative content analysis method (Mayring 2022). The affected individuals are quoted using self-selected pseudonyms. All quotations in this version have been translated to English.

³ For example, offensive content can also include (simulated) acts of torture or murder. Degradation and humiliation can target different physical or mental characteristics or social affiliations (for example, it can take on the form of racism), while the incitement to offensive acts can include, for example, incitement to various forms of self-harm, such as excessive exercise or restricting food intake.

2.4 Incidence and limitations

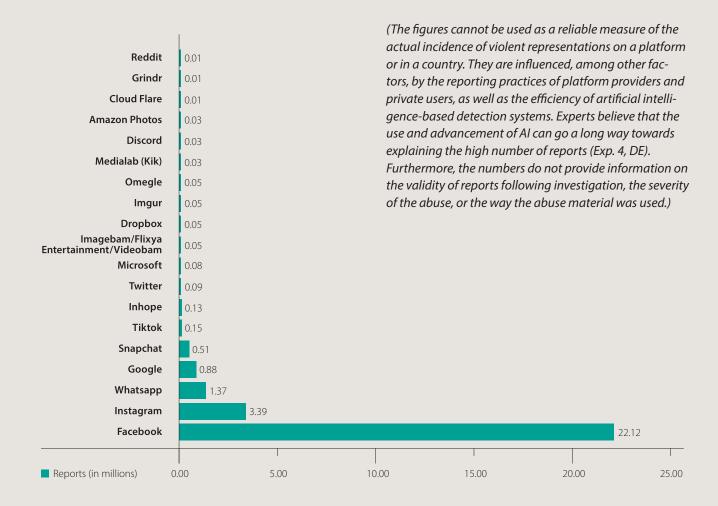
Online violence is an extremely multifaceted phenomenon, which makes it a challenge to describe it in quantitative and qualitative terms. For instance, there is no recognised measure of the prevalence and severity of online violence (International Justice Mission and Inter-Agency Council against Trafficking 2020). When describing country-specific contexts, it is difficult to assess whether higher incidence rates truly reflect a relatively higher frequency of cases or whether they are a result of better reporting practices of authorities, the population, and of automated reporting systems, such as those using artificial intelligence. Various aspects of online violence intertwine – victims sometimes become intermediaries or perpetrators themselves, while acts committed offline can also involve a digital aspect. However, taking into account the perspectives of practical work and advocacy, incomplete and

ambivalent data also deserves attention because child protection cannot wait for academic precision. What remains crucial nonetheless is that data should be interpreted strictly within the context from which it originates.

On an international level, the National Center for Missing and Exploited Children (NCMEC) in the USA serves as a central hub for reporting abuse material found on the Internet. The reports originate from various digital platforms, and are made both manually and through automated systems, with the latter being significantly more prevalent. The graphics (Fig. 1 and 2) show the country contexts as well as platforms with the highest number of reports received in 2021, and the per capita incidence of reports based on the population size. A report is defined as an Internet address that refers to a medium (image or video).

Fig. 3: Reports (NCMEC) of depictions of sexualised online violence by platform

(Platforms with > 10,000 reports in 2021)



03. Findings from the interviews

3.1 Forms of violence and threats

Experts describe various forms of online violence against children. Following Levy and Robinson 2022b, these can be categorised into four different, albeit often interconnected, forms of threat: 1) trading and disseminating abuse material; 2) exploitation through livestreaming; 3) cybergrooming; 4) sextortion and cyberbullying. As evidenced by the interviews with the affected individuals, these different types of violence entail different consequences and, therefore, warrant a differentiated analysis. Such an approach is also necessary for targeted prevention strategies. In this regard, the digital space should no longer be seen as separate from the analogue world. Online and offline abuse can intertwine, for instance, when acts of abuse are filmed or photographed and then shared online following abuse occurring in the analogue world.

1) Trading and disseminating abuse material

Distribution between perpetrators represents the lion's share of this form of crime. A significant proportion of such activities takes place on the darknet, where there are relevant forums with high numbers of members and large volumes of data. Experts often cite data from the NCMEC (National Center for Missing & Exploited Children 2023), according to which 29 million images and videos were posted throughout the year 2021, of which 22 million was reposted material, while 7 million represented new material being shared for the first time. This figure, however, fails to reflect the true incidence of the crime, which is extremely difficult to measure. This is because the users of such material make a point of having it in their possession. While conventional (adult) pornography often remains on servers and is streamed from there, child sexual abuse material is usually stored locally on digital devices and is only registered by law enforcement following successful physical house searches.

Experts report that material is also stored simply on the clearnet, often on cloud storage services (for examples, see Fig. 3 on page 15). The files are distributed by sharing links to them in encrypted communication (on the darknet or through common messenger services that have been offering end-to-end encryption as a standard for several years now). Due to encryption being used, these messages circumvent technical protective measures. Cloud storage services are only obliged to investigate and remove material when there is a specific suspicion.

Case study 01

Ming, female, aged 18, Thailand

Ming wanted to improve her English and was looking for native speakers when she found out about the "Omegle. com" video chat service on Tiktok. Tiktok videos showed how other people her age easily connected with people from all over the world on Omegle and practised speaking English. No registration is necessary, users are not required to create profiles and, as such, they know very little about the people they chat to. To take better advantage of the video feature, Ming chose to use a tablet with a larger screen rather than her phone. First, she met two people her age and had brief conversations. She then skipped two more people ("skipping" is made very easy) and on the fifth attempt was connected to a native English speaker whose age she had difficulty estimating. After a brief introduction, the user asked Ming if she wanted to play a game. On Tiktok, she saw that Omegle was used for word games via the chat function and therefore agreed. The participant only typed the words "boobs" and "ass". Ming says that she was very frightened and noticed how the man's pose straightened and she could see movement at the bottom of the screen. The user then adjusted the camera so that the video showed his genitals while he was masturbating. Ming says she felt caught off guard and had difficulty finding the "skip" button. After this experience, she was confused and unable to think clearly for a couple of hours. Confident that it was certainly just an isolated incident, she made another attempt the following day. After a short time, she was again connected to a user who, this time without further ado, showed his genitals.

Ming says she has stayed away from Omegle and similar services since that second incident. She actively warns her friends against using them and has posted her comments on Tiktok when videos about Omegle appear. She describes the experience as traumatising: "Whenever I open up something, I'm scared, thinking that it's going to happen to me. [...] I'm paranoid. I'm always paranoid, like, I'm scared."

However, Ming did not tell her family about the incidents for fear of burdening them with her own trauma. Before this experience, Ming said she had never heard of sexual violence online. Ming would like to see more education in schools and families about the risks posed by platforms such as Omegle. She criticises the platform for not requiring any proof of identity or age. She also believes that it would be useful for certain security measures, such as a report button for cases of abuse, to be required by law.

The distribution of material between perpetrators can also take on a commercial or semi-commercial form, whereby material is either sold directly, or it acquires cashlike significance. The latter occurs when abuse material is required in order to register on a relevant forum. On these forums, new members must prove that they are not acting on behalf of law enforcement by uploading material and, in doing so, they further expand the data pool.

Distribution from victims to perpetrators represents another significant part of this form of violence and it covers a spectrum that often begins with consensual sharing of intimate images. One or more of the participants later abuses trust and shares the material without the consent of the depicted person. Where the abuser acts with intent and feigns an intimate relationship, it is referred to as "cybergrooming" (see page 20). When extortion (either for money or further material) becomes part of the exchange, experts often refer to it as "sextortion" (see page 21).

Random "viral" dissemination describes the sharing of material without any of the aforementioned motives. In this case, abuse material is shared, among other reasons, out of outrage, personal interest, misguided humour or mockery, or when adults discover material depicting children in their care and seek help from other adults. This type of dissemination also significantly contributes to the circulation of such material. Levy and Robinson estimate that up to 3 million of the 29.4 million reports to the NCMEC in 2021 can be attributed to this kind of dissemination (Levy and Robinson 2022b, 16). Since the possession of child sexual abuse material itself is a criminal offence in Germany, distributing it, even out of outrage or while seeking help, also falls under the category of criminal activity, leading to unintentional incrimination. In the criminal law reform of 2021, when the possession of child sexual abuse material was elevated from a petty offence to a serious crime, this effect further intensified. Experts view this critically, as it obstructs law enforcement efforts elsewhere. One interviewed expert illustrates this as follows:

"This criminal law reform was a really bad move. [...] If, let's imagine, I discovered that, for example, my niece had this sort of 'child pornography" on her phone, and I took a photo of her phone screen with my mobile and then took it to the police to ask for advice on how to deal with it, the police would say: 'Oh my goodness! You are in possession

of child pornography!' This would then mean that, well, I wouldn't go to jail for one picture, [...] but I'd still have a suspended sentence hanging over me, and the judges would have no way [...] of simply dropping it, because it's a serious crime." (Exp. 3, DE)

Thus, in certain situations, the criminal law reform actually achieves the opposite of its intended purpose. Police forces are now required to also investigate offences committed unintentionally, diverting capacity away from dealing with the overwhelming number of NCMEC reports and with "actual" cases of child abuse, as well as proactively pursuing perpetrators.

2) Exploitation through livestreaming:

Exploitation through livestreaming typically involves at least three parties. There is frequently an intermediary who introduces the victim to a perpetrator, who then pays for and consumes a livestream of sexual acts, sometimes interactively directing the acts according to their personal preferences. Experts report a wide range of abuse severity, from posing in revealing clothing or undressing slowly, all the way to engaging in penetrative acts with objects or sexual intercourse involving third parties (who may also be minors – siblings of the victims, for example), the use of violence, and paraphilic acts, including urine and other bodily excretions. The age of the victims spans from infants to young adults. As far as is known, livestreaming frequently occurs transnationally, with victims and intermediaries located in countries in the global South and offenders in Northern countries or in economically privileged Southern countries. In the global South, a high level of English proficiency, fast and widespread Internet access, and low household incomes are identified by experts as risk factors. The amounts paid increase with the severity of the abuse, with the payment itself facilitated through international money transfer companies like Western Union or MoneyGram, as well as other channels like GCash, PayPal, or so-called cyber wallets and cryptocurrencies. In these situations, relatively small amounts are transferred – according to our respondents, often in the low two-to-three-digit range in dollars, occasionally also for severe abuse. However, the fact they can sometimes represent a month's salary in the high prevalence countries makes this form of exploitation lucrative for the intermediaries involved. Banks and money transfer services often do not raise suspicion regarding these small amounts, and in many contexts, bank secrecy

⁴ What is meant here are depictions of child pornography that originate from misguided humour or are created as a dare.

⁵ For example, by police officers creating children profiles ("fake child patrols") with the aim of tracing criminals online.

and data protection regulations hinder law enforcement. In addition, livestreaming occurs in real time and is therefore difficult to trace.

Besides instances of organised crime, close acquaintances and immediate family members often act as intermediaries, and it is not uncommon for the parents of the victims to be involved. Experts attribute this to the poverty of the victims' households. During the COVID-19 pandemic, travelling offenders may have shifted to livestreaming when faced with travel restrictions, and some took long flights, as in the case of Jaika (see below), to engage in acts in the analogue world during periods of relaxation.

According to our interviews, livestreaming is a crime that often takes place in local communities. Data from law enforcement suggests that arrests can lead to further arrests being made in the same neighbourhood. Some of the individuals involved are aware of other instances of

exploitation occurring in the same area. Where similar risk and vulnerability factors are present, it can be assumed that some families will work together by following each other's example, thus creating a sense of legitimacy. The former is supported by the fact that victims often report initially noticing a sudden improvement in the living standards of their acquaintances, which aroused their curiosity and eventually led to them engaging in livestreaming. Nonetheless, these communal (often financially motivated) dynamics that are typically associated with livestream abuse also facilitate greater detection of instances by law enforcement. A Philippine expert in the field of human trafficking comments:

"We are seeing a small uptick in community reporting in the Philippines as people become more aware, which is really, really encouraging. But because of existing gaps in detection on the platforms where this stuff is happening, you're still only catching a very small sliver of the cases that exist." (Exp. 3, PH)

Case study 02

Jaika, female, aged 17, the Philippines⁶

Jaika and Veronica had been best friends since their school days. Jaika often invited her friend to dinner, until one day it was the other way around. "Where did you get the money?", asked Jaika. Veronika started telling her about an online arrangement that she and her sister had with an Australian man over the Internet. They sent him nude photos and posed on live video chat following his instructions in exchange for money. At first, Jaika was disgusted by the idea.

When Jaika's family fell into financial difficulties following her father's death, Jaika felt obliged to help her family and, out of desperation, turned to Veronica. She introduced Jaika to her Australian online acquaintance. His name was Declan. That day, for the first time, Jaika witnessed Declan instruct Veronica and her sister to pose naked for him. They sent him the photos. Soon the message exchange turned into a live video chat and Jaika joined in. Looking back, she describes the situation as repulsive. It was like physical violence in a sense, as Declan told her and the other girls what to do. During the video call, Jaika's youngest sister Bianca happened to come into the room. She was 5 years old at the time. Declan saw her and wanted to see her naked too. He threatened not to pay for

the pictures they had sent and to publish the pictures on the Internet if they refused.

Jaika says she felt caught in the middle. She had pretty much raised her sister Bianca and felt like a mother to her. While they took photos of Bianca, she remained silent the whole time. After hours of conversation, Declan sent the money to Veronica via Western Union, and Jaika received her share.

Later, Declan travelled to Jaika's hometown. She was surprised to hear that this wasn't the first time Declan had visited Veronica and her sister. She recalls: "I learned that they've been doing it – meeting in person for a number of times before." Declan would direct the girls while taking photos and videos of them. Jaika was present during two of these visits, but after the second time, she wanted nothing more to do with it. Declan was later convicted through the cooperation of Philippine and Australian law enforcement authorities and sentenced to 20 months in prison (Lock 2018). Veronica and her sister, although abuse victims themselves, are serving life sentences in the Philippines for human trafficking for acting as intermediaries in Jaika's exploitation. Jaika received posttrauma support from IJM and is now involved in a network of victims.

⁶ Jaika's case study originates from the work of International Justice Mission (IJM). The case has not yet been disclosed publicly and is presented here with the kind permission of IJM Philippines. The names of the individuals involved are pseudonyms.

However, experts also report cases in which young individuals voluntarily engage in abusive exchange for money:

"If a student sees, or his classmate does this and that, and he or she gets curious: 'Where do you get these really nice things?' – 'Because I have this foreigner chat [with] me.' So the child could learn from it." (Exp. 4, PH)

"They have friends that do this for money. They have phone sex, and then they'll say: 'Oh, that person did it, they got paid. I want the money, too."" (Exp. 1, TH)

Nonetheless, the persons interviewed generally admit that, even in such cases, the parents are usually aware of the ongoing abuse through livestreaming. The percentage of parents who are unaware is believed to be low. Where livestreaming is concerned, it appears as though parents, even if not directly involved in facilitating their children's participation, tacitly allow the abuse, because they indirectly benefit from the income generated through the exploitation.

3) Cybergrooming

Cybergrooming refers to the systematic contact and relationship-building with children online with the intent of sexual exploitation. In Germany, if the victims are under 14 years of age, it is considered a criminal offence according to Article 176a of the German Criminal Code. Cybergrooming is a form of sexual abuse of children that

occurs on the clearnet. Interactions are often initiated on popular social media platforms such as Facebook, Instagram, or TikTok. They then quickly move on to a different communication channel that is end-to-end encrypted, such as WhatsApp. This bypasses technical measures implemented by social media platforms that detect certain communication patterns indicative of cybergrooming and warn the person at risk. While this phenomenon is not new (according to our research, it was first mentioned by Berson in 2003), ongoing technological advancements and, more recently, the widespread adoption of end-to-end encryption by many messaging services have contributed to the proliferation of cybergrooming in various ways.

According to experts in the field of law enforcement, all platforms where children are present (even if using incorrect age data) are utilised. Gaming platforms also play a significant role in this context. Communication (be it through messaging or audio chat functions) may initially appear to be a secondary purpose, but upon closer examination, the communicative aspect is a core component of many online games. According to the respondents, boys are particularly targeted:

"As I've said, it happens via mainstream social platforms like TikTok, Instagram, Facebook. But at the same time, they are also active on mainstream gaming platforms, which tend to be more of a boys' thing. They are more susceptible there. Wherever teenagers are in contact with each other, the offenders are also present, sending out messages to hundreds of users." (Exp. 5, DE)

Case study 03

Roh, non-binary⁷, aged 23, India

When Roh was in Year 8, a boy at school showed an interest in them, but Roh wasn't interested. The two saw each other frequently, rode to school on the same bus and messaged each other online until Roh decided to minimise interaction. While the boy continued to be friendly and respectful in his interactions in real life, he soon complained in his online messages that Roh was ignoring him. Eventually, he created photomontages in which he placed Roh's head and face on pornographic depictions of women in order to coerce Roh into further interaction.

Roh states that it is more straightforward to spot the danger of sexual violence in the analogue world rather

than online, as people are easier to read in analogue contexts. Before the incidents, Roh had never been exposed to sexual images on the Internet.

At first, Roh tried to ignore the perpetrator, which did not, however, produce the desired effect: "But then he kept sending me pictures after pictures." Roh sensed how the boy's behaviour was causing them anxiety and difficulties with concentration, and after three months, they finally confided in their brother, but not their parents. "I was afraid to tell my parents because they would just be like 'why are you using social media?', and they would make me stop using Facebook." After their brother had intervened, the messages stopped. Roh believes that organisations that ensure anonymity when someone reaches out to them are valuable.

⁷ Non-binary refers to the gender identity of individuals who do not identify as either male or female, but rather outside of a binary gender framework.

One characteristic of the online environment is that contact can be initiated very rapidly and effectively. Perpetrators can use "copy and paste" to send the same message to hundreds of individuals within a short period, while translation features make it easy to communicate in different languages. Our interviews and the Honeypot study (Terre des Hommes NL 2023) confirm that after creating a public profile on social networks, it often takes only a few minutes before someone initiates contact, especially if the user's photo or name suggests they are a child. Perpetrators sometimes approach thousands of children, knowing well that one successful attempt is often preceded by a few hundred unsuccessful ones.

Another characteristic of the online environment is that a perpetrator can create and use multiple profiles simultaneously to target a broader range of age groups. Some perpetrators pose as both children and teenagers simultaneously, reaching out to potential victims from different age groups who are led to believe they are speaking with someone their age.

"One offender will have accounts [on] Facebook, Instagram, TikTok, Viber, or what not. They will have 2 or 3, or 4 if not more profiles [on] each platform and they will talk with more than one victim at one time." (Exp. 5, PH)

The strategies for initiating contact vary widely. Some perpetrators become sexually explicit shortly after the initial contact.

Studies have shown that children sometimes maintain contact even when the content becomes heavily sexual (Neutze et al. 2015a), possibly out of curiosity, shame, fear, a lack of awareness that the interaction can seriously harm them, or due to the dominance of the offender over them and misplaced blame.

"Then their perpetrators will also say: 'But look how beautifully you're smiling. You wanted it.' This is also one of the strategies used by the perpetrators. It's nothing other than a reversal of responsibility. 'You wanted it though. You chose to come here after all. You were curious to try it."" (Exp. 6, DE)

Some perpetrators have sometimes established such a strong level of contact and trust with the child that the child does not want to lose this 'attachment figure' (e.g., when they are lonely or suffer neglect). In other cases, the perpetrators "lure" the child with the promise of gifts (e.g., vouchers for online shops or so-called "skins"

on gaming platforms), money or modelling contracts, or threaten the child to publish the child's recordings or send them to the parents if they break off contact. Although perpetrators often assume false identities and pretend to be their peers, children will not necessarily discontinue contact, even if they eventually learn that the other person is actually an adult. When grooming extends over months, the perpetrator might eventually choose to reveal the truth to the child. Instead of breaking off contact because of the breach of trust, some children feel valued because an adult is interested in them and is giving them so much time and attention.

"Interestingly, even if the perpetrators say at some point: 'Oh, I have to tell you something, I'm not 14 like you, I'm actually 43 already.' What we see [in chat evaluations] is that the girls, rather than say something along the lines of: 'You old creep, get out of my life', they say: 'I'm shocked that an adult is interested in me. Wow, unbelievable.' And it actually serves as a confidence boost." (Exp. 3, DE)

Children maintain contact also when sexual topics arise: the MiKADO study found that only around 14% of children immediately broke off contact in such situations (Neutze et al. 2015a, 2).

4) Cyberbullying, sextortion and self-produced material

Cyberbullying refers to the social degradation and defamation (bullying) of a victim using digital communication media, often for reasons of revenge or as a result of rejection. This includes insults and threats, the publication of intimate recordings without the consent of the victim, the dissemination of falsehoods while assuming the digital identity of the victim, and the involuntary or fabricated sexual depiction of the victim (for example, when a person's face is superimposed onto pornographic images). Although cyberbullying itself is not listed in the German Criminal Code, many forms of bullying do constitute actual criminal offences (e.g., Articles 185-187: insult, defamation, libel; Article 131: violent representation), which can be punishable by fines and imprisonment.

The area of sexual violence online involving self-produced photos and videos is becoming increasingly significant. These are created and sent as part of interactions that are initially consensual ("sexting"), but also in order to gain recognition and find resonance on social media, out of curiosity, as a dare, or as an instance of pushing

Case study 04

Kitty, female, aged 17, Thailand

When Kitty was about 12 years old, she received a friend request on Facebook from a stranger who she identified as Indian and estimated to be around 40-50 years old. After looking at the man's profile, she rejected the request. She then received messages, first complimenting her on her appearance, and ultimately asking if she wanted to see his genitals. At the time of the crime, she was with five other friends. At first, they encouraged her to continue messaging with the perpetrator for fun. Kitty herself also says she was curious to see where the exchange would lead. She was amazed to have received a contact request and messages from a foreigner. Eventually, the perpetrator sent her a photo of his genitals and tried to video call her. Kitty declined the call and blocked the contact.

Kitty had heard of similar situations from her friends. They, too, had been contacted by Indian people via Facebook Messenger. In a similar case, the affected child already suspected what was about to happen and accepted the video call in the presence of a group of peers who were immediately confronted with the caller's genitals. The child then turned on their own phone camera, pointing it at the group of children, following which the caller hung up – out of embarrassment, according to Kitty's interpretation. But Kitty says she doesn't want to and wouldn't do something like that. Looking back, she finds the exchange frightening. She says the thought of someone using her face for their own sexual gratification makes her feel bad.

Kitty knows of other cases at school. For example, a boy posted a video of his girlfriend masturbating. She then changed schools. Kitty says that this incident had led her to decide to never send intimate pictures of herself. If, one day, a partner asked her to send these, she would end the relationship.

Kitty would wish to see an organisation that helps affected people like her. There should be a central and easy-to-remember phone number. She is not aware of any such organisation or number. She would also like famous people to raise awareness of the topic.

boundaries. Over three-quarters of reported sexual depictions of children involve self-produced images. While this type of imagery is prevalent among 11 to 13-year-olds, it more than doubled among children aged 7 to 10 in 2022 (Internet Watch Foundation 2023). In this context, it is often initially consensual "sexting", which involves sending sexual self-portraits or videos, that is then followed by abuse, especially when a relationship comes to an end. Under certain circumstances, the materials may then be shared carelessly, as seen in Riona's case (see Case study 05, page 24), or even maliciously. As Riona's case illustrates, the careless sharing of sexual images can also lead to extortion by third parties ("sextortion").

Sextortion, following prior grooming, is currently recognised as a transnational crime involving extortion for financial gain. A male victim from India describes a strategy that focuses on boys:

"There is a huge thing that happens with boys as well. There are guys who pretend to be girls talking to them, sending them some other girl's picture just to make them sure that this is a girl talking to you. [Or] sometimes there's a girl who maybe is video calling you from random numbers, talking to you in a sleazy manner, then recording the whole thing, and then [extorting] you for money. [...] There's a huge component of guys who go through this." (Shubb, male, India, aged 24)

Boys are also contacted in Germany, as reported by an expert we interviewed (Exp. 5, DE). Since late summer 2022, there has been an increase in cases where boys are targeted, supposedly by attractive women, and are ultimately incited to produce and send naked images of themselves. The children are then blackmailed. The amounts demanded are such that children can access and send without the help of an adult, especially through vouchers that they purchase by themselves and then send the redemption codes to the perpetrators.

However, the experts also report cases in which selfproduced material is produced without any features of blackmail:

"Then we have cases, which we as investigators sometimes find irritating, where 13 or 14-year-old girls running a YouTube channel will, for example, offer: 'If we get 1,000 likes here, I'll take off my T-shirt.' [...] For another 1,000 clicks, we'll also take off our panties. And they are doing it voluntarily. [...] What they don't understand is that

they are probably being recorded by perpetrators on the other side. [...] The recordings will then of course be used." (Exp. 5, DE)

Boys are also affected:

"What tends to be more effective with boys, however, is more of a business model. They say: 'Hey, if the guy is stupid enough to give me a tablet or extra game credits just because I send him naked pictures of myself, that's cool." (Exp. 1, DE)

Nevertheless, it would be misguided to regard these actions as mere carelessness. Such an evaluation would neglect the fact that many children and adolescents, depending on their level of maturity and life experiences, may not yet grasp the significance of sexuality in the dynamics of power and violence. This, in conjunction with a lack of knowledge about the ways in which content can be disseminated on the Internet, results in young people having difficulty assessing the risks and consequences of their actions that they will often take in exchange for short-term recognition.

3.2 Factors behind sexual violence in the digital space

Five background factors have emerged as particularly relevant in the data analysis and will be briefly described below: 1) the COVID-19 pandemic, 2) poverty, 3) the ambivalent role of the family, 4) the trauma of "irremovability" of content, and 5) gender.

The COVID-19 pandemic: new opportunities for illicit acts

The COVID-19 pandemic has profoundly altered the realities of children, including digitalised learning that had to be done online from home, often independently, during extended periods of school closures. The experts we interviewed in the field of law enforcement point out that the increasing digitalisation of school and life contexts during the pandemic created more opportunities for offending. Children now spend more time in digital spaces at a younger age, and these have a lower level of parental or teacher monitoring. An expert from India highlights that the pandemic-induced digitalisation of education introduced even those children that came from low-income households to the benefits and dangers of the Internet.

"Another thing we've seen is because of the pandemic, the poorest of the poor have had to have a device because our education was online. There is no child today that is not connected virtually." (Exp. 1, IN)

However, the pandemic also intensified certain dynamics on the side of the perpetrators, as reported by an expert from Germany:

"Because the [perpetrators] were now also working from home, instead of, to put it bluntly, sitting in the office for nine hours, and, as such, they now had a different form of social control. They now did it from home, and they might have had two screens open, one to do actual work for their company, and on the other screen, they may have been in the digital space on a lookout for children. We have thus created completely different opportunities for offending. We simply cannot deny this." (Exp. 5, DE)

The digital changes in the lives of children and adults are profound. Their impact was already recognised early on in the pandemic (Europol 2020). However, it now appears that at least some of these changes have become permanent. The discourse on how to counteract these trends in a world altered by the COVID-19 pandemic requires greater attention from the fields of research, policy, and child protection practice.

2) Poverty: a driving factor

Poverty is often a driving factor for online abuse. A Philippine expert who leads an urban social institution for children reports:

"Our youngest, they are given Jollibee[®] meals. Then the perpetrator would bring them all together in one Barangay[®], in one area. There are also a lot of them already. They're being given Jollibee meals, and then the perpetrators will take photos of them." (Exp. 1, PH)

Also in respect of livestreaming, it is repeatedly observed that the victims themselves or their intermediaries engage in online abuse out of poverty or for financial gain in order to afford everyday items such as cosmetics or simple electronic devices. However, it would be incorrect to assume that children from extremely poor households are unaffected by online abuse due to a lack of digital devices or poor Internet connectivity, as explained by the Philippine expert:

⁸ The largest fast food provider in the Philippines.

⁹ The lowest administrative structure in the Philippines.

"Even those who collect garbage have cell phones at home, because they also have a budget to get hold of a cell phone. After all, it's very important to have that. It's already a necessity in the house. You can access remote friends and watch videos. It's like a radio." (Exp. 1, PH)

Furthermore, the expert notes that Internet connectivity is often available for free, for example, in shopping centres.

However, children from medium and high-income households are obviously also affected, including in Germany. As noted by an expert (Exp. 4, DE) from a national organisation for media oversight, children who lack a stable social environment, who feel lonely or neglected, and those that spend a lot of unsupervised time online, are particularly susceptible to responding to requests from strangers on the Internet.

An expert with experience in a law enforcement agency explains that in foreign contexts, there are frequent cases in which children are coerced by their families into producing abuse material to contribute to the household income. Even though this is less common in Germany, it does occur. What has been increasingly observed lately are cases in which children engage in situations of abuse or circulate self-produced content to "make extra pocket money": "We have these pocket money cases here in Germany. If you search for it – 'how to make extra pocket money' – you'll find it on many platforms." (Exp. 5, DE)

This means that sexual content and potential abuse may arise even on "harmless" swap and sale platforms for classified ads.

There are different economic realities at play, which can sometimes influence and exacerbate each other. On the one hand, there is the poverty of the entire family, where the sexual exploitation of children becomes a significant source of income. On the other hand, there are the material needs of children from households of all income groups which the parents may not be able or willing to fulfil. When these conditions are considered alongside the dynamics of attention and recognition prevalent on the Internet, as well as the boundary-pushing behaviour of some children and adolescents, numerous possible scenarios emerge in which these factors can create and drive situations of abuse.

3) Parents and family: an ambivalent role

The role of parents, siblings, and extended family members is ambivalent. As shown in the cases of Roh (Case study 03, see page 20) and Riona (Case study 05, see below), close family members can be the first to provide support for victims. At the same time, they can also act as intermediaries, especially when livestreaming is concerned. Roles of complicity and providing assistance can become intertwined. Even where parents act as intermediaries in the abuse of their own children through livestreaming, they may still see themselves as protectors

Case study 05

Riona, female, aged 17, India

Riona is a student and lives with her father. Despite having had relevant education at school, Riona was more aware of the danger of sexual violence in the analogue world than in the digital world. She had always felt relatively safe online and was therefore even more shocked when something traumatic happened to her there.

In Year 8, she met an older boy. The two exchanged nude pictures via Instagram. Riona relied on Instagram's disappearing messages feature. Photos sent using this feature can only be viewed once. If a screenshot is taken after receipt, a warning is displayed on the sending device. However, in this case, the boy took photos by photographing the screen with another device – an analogue mechanism that cannot be detected. Riona was later blackmailed into sharing more nude photos by several anonymous accounts. Although her face could not be seen in the photos, third parties had deduced

her identity from the room and furnishings visible in the background and threatened to publish the images. For the next eleven months, Riona was unable to defend herself against the blackmail. She was struggling to study because of the stress she was experiencing. At very last, she confided in her father. Together, they confronted the boy and got him to post a confession on Instagram in the form of a video in which he described exactly what had happened. The boy and Riona posted the video on their respective Instagram accounts. In the aftermath of this unusual confrontation, the extortions stopped. Riona suspects that the blackmailers realised that now that her father had become involved, they no longer had any leverage and, instead, they were likely to face confrontation and reputational damage should their identity become known.

Since then, Riona has wanted to study psychology in order to help other victims in the future.

of their children and be seen as such by them, in line with the "no touch, no harm" concept, shielding them from (supposedly) worse acts, such as "classic" sexual exploitation in the analogue world. The role of parents and other guardians is ambivalent in another sense: while they can be the first to provide effective support, they can also be the first to administer punishment. Children often express fears that if abuse were to become known, their guardians would also be likely to hold them accountable and, for example, prohibit access to social media, gaming platforms, or the Internet as a whole.

A recurring phenomenon makes it particularly clear why it is essential to recognise children's agency in their actions: time and again, children decide to protect their families, even to their own detriment. This dynamic is evident when affected children choose not to tell their families about the abuse because they do not want to burden their families with what they have experienced themselves. As part of the MiKADO study, it was revealed that two-thirds of the interviewed victims had never confided in anyone prior to participating in the study (Neutze et al. 2015b, 7). Eighteen-year-old Ming from Thailand (Case study 01, page 17) says this about her experience on the video chat platform Omegle: "I told all of my friends in my group, but I didn't dare to tell my family. [...] I felt that they probably would feel bad. They would feel as bad as me if they had known what I encountered."

A social worker interviewed in the Philippines reported that children also cover for parents who acted as intermediaries in their own abuse:

"We did everything. We talked to the child, we talked to the cousins, and then we talked to the mother. The mother wouldn't really cooperate. She would just lie and hide. Then eventually the child would withdraw the statement. The child would say that it's no longer happening." (Exp. 2, PH)

Children who are freed from situations of abuse facilitated by their parents may have limited awareness that they were abused. This is due, on the one hand, to the fact that younger children often lack cognitive and linguistic patterns that can help them identify and communicate their own abuse, which is further exacerbated by the absence of child-friendly reporting channels. On the other hand, they are dependent on the care and support

provided by their parents, even if it is characterised by violence (cf. Baker and Schneiderman 2015).

Parents and family members can also inadvertently produce material that is subsequently exploited and disseminated by offenders. This is especially the case with "sharenting"¹¹, when parents post recordings of their children, usually in everyday situations, on their social networks. This not only violates data protection, privacy, the right to one's own image, and sometimes even the dignity of the child (Alig 2023, 1), but can also be quickly disseminated, especially if done on public profiles.

A new law proposed in France aims to impose an obligation on parents to better protect their children online and not to violate their privacy or compromise their protection by carelessly sharing images online. This legislative initiative responds to findings that billions of images and videos are shared on social networks every day, including many of children, sometimes even before birth (Assemblée nationale 2023). The publication of such everyday representations is highly problematic for several reasons. Firstly, there is little control over how this material is shared further. It is believed that up to 50% of the images circulating on abuse forums (referred to as "child pornography forums" in legal contexts) may originate from the parents' social networks (Assemblée nationale 2023). Certain content, such as photos of naked babies or girls in sports clothing, has a particular appeal to consumers of paedophilic material. Secondly, the reason this is damaging in the long-term is because this inadvertently created material can never be completely erased. Furthermore, the information that is posted about children's daily lives can, in the worst case, be used by offenders to identify the child's whereabouts and habits for the purpose of sexual exploitation.

4) Trauma: the practical "irremovability" of the material

Sexual violence in the digital space causes severe and specific trauma marked by lasting emotional and physical harm (Jonsson et al. 2019). Its psychological consequences are also discussed in our interviews, highlighting that it cannot be assumed that experience of abuse is less severe just because it occurs in a digital context:

¹⁰ It is assumed that sexual abuse is equally traumatic regardless of whether it happens online or in person (Joleby et al. 2021).

¹¹ The term combines the words "to share" and "parenting" and describes the (sometimes excessive) sharing/posting of video recordings and photos of one's own children on social media.

"Self-harming? They would do that. They would try committing suicide, or they would say that it's better for us to die. That' how traumatized [they are] because they think that they're so dirty. It's difficult for the child to make even the smallest decision. She would say, I'll try. I'll see. Then they'd say: [...] 'Can you decide for me? Because I think you know what's best for me." (Exp. 2, PH)

Joleby et al. (2021) show that trauma resulting from digital violence is comparable to the psychological consequences of abuse in the analogue world. Survivors go through long processes of coping with trauma, which includes a prolonged phase in which the affected children must first understand how online events have impacted their analogue reality. Additionally, there is a persistent risk of becoming confronted with the image and video material online again at any time.

The practical impossibility of erasing abuse material represents a crucial difference between sexual violence in the digital space and the analogue world. While it is possible to remove abuse material from servers, and this can be enforced, there is always an inherent risk that consumers of such material might save it on private storage media and re-upload it online. This dynamic has several consequences. Knowing that the material continues to exist and is being used by unknown individuals for sexual stimulation and gratification is perceived as a perpetual loss of control and constant retraumatisation. With the advent of new facial recognition algorithms and social media, there is a real danger that perpetrators will actively try to locate individuals they have seen in abuse material.

If it becomes possible in the future to digitally compare photos of faces from childhood and adolescence with photos from later adulthood, this can mean that the digital identity of the survivors of child abuse, with which they want to present themselves, including in their future careers, will forever remain linked to the abuse (Exp. 7, DE). Consequently, they may face such limitations in their job applications and other professional or private uses of their self-image that they could potentially suffer economic disadvantages as a result, especially if they are unable to participate fully or only have limited access to online platforms. Therefore, new forms of social inequality on

a global scale arise from the indelible stigma of sexual exploitation in childhood.

5) Gender: male victims and female perpetrators also exist

Experts consistently report that both boys and girls are affected by sexual violence online.

"What you can say about children is that girls and boys are equally affected. There is no difference at all. [...] As soon as a child uses digital media, they theoretically become a potential victim. In fact, [we] also conducted this survey again specifically with children of primary school age [...] and we actually concluded that a great many children under the age of 10 were affected, which is also due to the fact that children now have access to digital media at an increasingly early age [...]." (Exp. 1, DE)

In some contexts, such as online gaming, boys are disproportionately at risk because they tend to engage in these activities more frequently.

However, even though we wished to ensure a balanced sample for our study, finding male victims willing to give an interview was challenging, with only two deciding to participate. The research team developed a working hypothesis whereby feelings of shame and restrictive norms of masculinity might explain why boys are less likely to discuss their experiences of sexual violence. This hypothesis cannot be definitively confirmed based on the two interviews with male victims, and to date, there has been no further research on this topic. Nevertheless, at least one of the male victims corroborates our shame hypothesis in his interview.

"It's a very male dominant country. It's a very patronizing country. Every time it happens to a girl, the girl is just damaged, destroyed. Most of the time, she just can't believe what has happened to her. How could she trust that person or how could that person take this level? For guys, it is a huge embarrassment, a huge shame. They feel very scared from now on to talk to anybody. I think that's how the females and males share this feeling." (Shubb, male, India, aged 24)

¹² Srivastava et al. (2023) demonstrated that, in the group of children examined in the study, cases where abuse material had been posted online showed higher rates of self-harm and attempted suicide than those with existing but unposted material. The specific challenges related to the impossibility of erasing material are also well-known in trauma therapy (Martin 2016).

Furthermore, a female victim from Thailand noted that when she disclosed her abuse, she received emotional support from her female friends. However, she assumed that male victims would continue to feel ashamed and stigmatised by their experiences of abuse and might even perceive it as emasculating. Quantitative studies have repeatedly shown that there is more abuse material depicting girls than depicting boys. At the same, the abuse of boys can be more severe.

"And what's interesting, in turn, is that in abuse material depicting boys, over half of it shows severe sexual violence. [...] So, we are talking about severe sexual violence

against boys, and we disproportionately often see female perpetrators." (Exp. 6, DE)

According to surveys of victims, female perpetrators constitute a significantly smaller proportion, approximately 15-25%, compared to male perpetrators (Araújo et al. 2022). Nonetheless, it is crucial for digital and analogue intervention and prevention work to recognise that there are also female perpetrators, and encounters with or among female individuals do not automatically offer protection against sexual violence.

Case study 06

Ace, male, the Philippines, aged 19

Ace is 19 years old and lives in Manila with his mother. For him, sports is how he makes friends and what gives him balance to problems in everyday life, such as the loneliness he sometimes feels in his family due to his homosexual identity.

At the age of 16, he became friends with a volleyball teammate who was five years older than him. The young adult then spent two years layering Ace with promises of what he could afford if he took naked photos and videos with him. The perpetrator said that there were foreigners, both male and female, interested in material with young people. First, he showed him pictures of other children. Their faces could not be seen, which encouraged Ace. He agreed in the end. Contrary to the agreement, Ace received no money from the sale of the photos. It also appeared as though the perpetrator, who Ace had referred to as a "friend", was also attempting to blackmail Ace with the photos. Shortly afterwards, the perpetrator persuaded Ace to meet a Chinese man. The wording initially remained vague: "Come with me. There's going to be a party. [...] We're going to make money out of this." When the meeting in person took place, the intermediary "friend" said that Ace could decide for himself what sexual acts he would or would not perform with the man, and then went away, leaving Ace alone. Ace again received no money, only a tip from the perpetrator of abuse.

In another incident, the intermediary "friend" left Ace alone in a taxi again, where he was shocked to be informed that he was going to be abused by a group of people. At a café chosen as the meeting point, Ace was approached by an alleged perpetrator, who was actually an undercover detective. In the police operation that followed, Ace was

rescued and freed from the structures perpetuating his abuse.

Ace describes himself as severely traumatised, including by the rescue operation in the café, which included violent arrests at gunpoint. It was not until months later that he felt able to talk to his family about what had happened. Following his rescue, he is now spending a year in a social facility. Life there is not easy, among other things, because LGBTIQ people are compelled to live in isolation. However, Ace is receiving from a psychologist. Owing to his experience, he has decided to become a psychologist himself in order to help other victims. At the facility, he has met other children whose abuse also started with photos. Ace says in the interview that he also knows that there are children who are abused in the facility itself.

Looking back, he says he was naive: "I was very careless with my actions before. I would easily get excited and I wouldn't care about the consequences until they've shown me that we would do this." In the interview, he reflects that he should have listened to his parents more, but also recognises that they had little time and attention for him. In hindsight, Ace realises that the intermediary perpetrator was able to manipulate him because he had positioned himself as a loyal friend over an extended period, thus building trust.

Ace's self-critical attitude is understandable, but from the perspective of children's rights, it must be noted that no careless action on the part of the child can justify any (not even proportionately) shared responsibility for abuse. Childish carelessness is a part of human development and, in secure settings, fosters maturity and responsibility. In Ace's case, the problem lies less in his actions than in the fact that his needs for protection and prevention were not fulfilled.

"It's a myth we believe in, or in other words, we all still somewhat refuse to accept it [...]. We have a really hard time acknowledging that women can be sexual offenders or that girls can be sexual offenders or potential sexual offenders." (Exp. 6, DE)

Especially in the case of cyberbullying, violence among young people (of the same age) is widespread, including with girls as perpetrators. For example, in a case documented by the HUMAN project, a 13-year-old boy was pressured by a group of 14-year-old female classmates who, using a fake profile, was posing as a 16-year-old female stranger, coerced him into sending them a photo of his penis. In school, the group of girls went on to spread rumours that the boy had "sent the penis photo to the girl just like that", which further stigmatised him as someone that violated sexual boundaries (Vobbe and Kärgel 2022, 147).

3.3 Assistance and prevention

The interviews conducted for our study highlight that child protection in the digital space and assistance for victims can only be effectively improved through the comprehensive interplay of relevant factors and stakeholders.

Prevention: social environment, media literacy, and societal discourse

Our research reveals that children with a stable social environment and strong family and friendship bonds are less vulnerable to online violence (see also Stoilova, Livingstone, and Khazbak 2021). The Youth Media Protection Index ("Jugendmedienschutzindex") measures, among other things, how children in Germany navigate digital contingency experiences. As reported by children themselves, parents, friends, and family members are the first point of contact for assistance (90%), followed

Case study 07

Shubb, male, India, aged 24

Shubb is studying engineering and first encountered sexual violence during his university education. In his university dormitory, there was an initiation ritual during which senior students humiliated new first-year students by forcing them to undress one by one. Shubb explains that while others were affected as well, the level of violence he experienced was higher because he had initially resisted. He had to undress down to his underwear, and a video of him was taken, which was then shared in WhatsApp and Telegram groups. Senior students used this recording repeatedly for the next three to four months to humiliate him and to pressure him into doing certain tasks for them. Shubb says: "[When] my videos leaked, I felt very violated. I felt that I couldn't live there any more. Do you understand? I felt that everybody and anybody can access my photos, access my videos, ask for it, make fun of me. Any time I wanted to have a conversation, maybe it will come up."

Like Ming, Shubb confided in friends but not in his family. "I did not want them to be upset. I was living very far from home. I did not want to include them." A teacher from his former school, to whom he had confided, told him that such things were just part of university life and that he should not worry. Shubb did not receive practical support. Out of fear that this would worsen his situation, he did not approach the dormitory management.

Shubb mentions that he had previously heard of sexual violence online from an older cousin. They also learned about it at school, but this was done from the perspective of female victims only. The violence against him, therefore, caught him off guard.

"I did not know this can happen to boys and girls and how uncomfortable they can make you feel and how scared they can make you feel. I did not know anything [...] in case of boys. In case of females, it was very clear. It was sharing of nude pictures on the Internet. It was taking a video [...] without her consent. These were the basic things that I knew about digital sexual content."

Shubb wishes he could have called an anonymous hotline. He believes that every institution should have one. At the time, he was not aware of any external helplines. Otherwise, he would definitely have used them.

Furthermore, Shubb advocates for early education to give children an understanding of what sexual violence is because, as he has observed among friends, some lack an awareness of boundaries being crossed and actions being trivialised.

by teachers (68%), with significantly lower reliance on local counselling centres (37%) and social workers (35%) (Gebel et al. 2022, 62). Pohle et al. (2023) link these findings to research by Beitzinger et al. (2020) on cyberbullying and observe that often, despite their desire or intention to seek help, children are hesitant to reach out. While two-thirds

of adolescents wish to have parental support, only about half of them actually turn to their parents for help (Beitzinger, Leest, and Schneider 2020, 113–114). This discrepancy between desires and actions is likely due to the fact that even when a child wishes to receive help from their parents, they may be so deeply overwhelmed by shame, fear or mistrust associated with the specific situation that they cannot communicate their need for assistance. The experts we

interviewed are therefore calling for very easily accessible support services.

"Preventive work is needed, and children must have an easily accessible contact person. It doesn't make sense for them to call a helpline somewhere, perhaps one run by the European Union. They need to have a specialist counselling centre at their school or nearby, where children know they can go, or at a police station." (Exp. 5, DE)

Such support services are currently being discussed (e.g., the proposal for a so-called "online child safety watchdog", i.e. "Kinderonlinewache", by the SPD parliamentary group in 2023). However, they can only achieve something if they are well known. They must thus be made widely recognisable, while using them should be incorporated into the school curriculum at an early stage. Furthermore, comprehensive awareness and prevention work for and with parents is crucial, since many children do not turn to their parents out of fear of the consequences. Roh from India (Case study 03, page 20), too, kept the abuse to themselves out of fear that their parents would ban them from using Facebook.

"Actually, at first, it's often not so much the fear of the parents, that we will somehow lash out at them angrily, but the children are instead afraid that their parents might say: 'That's it, you are not allowed a smartphone any more. You are not allowed on the Internet any more.' This is actually very often a reason why children do not confide in their parents. That is why it is so important that parents address such issues when teaching their children how to use media and that they tell the child very clearly: 'Should something like this ever happen to you, you don't

have to be afraid to come to us, and there will be no ban for you, we will stand by your side and make sure that we solve the problem together." (Exp. 1, DE)

Even less obvious stakeholders from the child's social environment can have a preventive effect. Civil society

Our research reveals that children with a stable social environment and strong family and friendship bonds are less vulnerable to online violence.

organisations for prevention play a role in this respect, while attention should also be given to the digital social environment of the child as well as the impact that influencers might have on them. The interviews conducted in Thailand highlight how celebrities can contribute to raising awareness of the issue. When asked what would give her a real sense of assistance, 17-year-old Kitty from Thailand said she wished that organisations that offer support

would make their services more widely recognisable by collaborating with national celebrities. An interviewee from a national law enforcement agency in Thailand describes that such

collaborations are indeed already being implemented:

"Usually, we're on the news quite a lot. There are celebrities who come and do the news with us, and [children] will have a memorable image about that." (Exp. 1, TH)

Here, celebrities, who children follow on social media, in other words, their digital social environment, create awareness of how to use the very same media safely and where to seek help in case of danger. Awareness-raising and support services are thus based in the same channels as those where the threat exists.

School can also serve as yet another important place for prevention. Education on the rights of the child, as well as media literacy and education, must be introduced as a school subject and made into a mandatory component of the training of teachers and caregivers working in schools and childcare facilities. Well-informed and self-determined children who know about their rights and potential threats, both in the digital space and the analogue world, can better protect and defend themselves. What is important in this regard is not only that this education must take place using age-appropriate language but also that it must strike the right tone. "Appropriate sex education with a focus on sexual self-determination and the confident setting of boundaries in dealing with others, as well as an unembarrassed approach to sexuality itself and to young people's curiosity in this respect,

has a risk-reducing effect, not only when it comes to cybergrooming." (Wachs and Bock 2023, 123)
Help systems based on peer-to-peer and mentoring logics are also discussed in research and regarded as forward-looking (cf. Gulowski and Krüger 2020). At some German

schools, a so-called "Medienscouts" model is being implemented, where older students educate and advise younger students through their own experiences on how to behave in such cases (for example, advice on taking screenshots of chats as evidence or how and where to file a report).

"We have entire project schools that continue to implement [this model]. In Munich, for example, older children are the contact persons for their peers and younger children, and they can then, of course with guidance, which often comes from trusted teachers or social workers in schools, act as a link between the child and the help system. When it comes to smaller children, something along the lines of 'here's a number, here's a poster' simply doesn't work." (Exp. 3, DE)

However, education in school and family contexts falls short if the issue of online violence is not simultaneously discussed at a broader societal level in wider public discourse. This discourse can also be initiated and promoted by the state, as demonstrated by the French government's initiative "Je protège mon enfant" (Direction Générale de la Cohésion Sociale 2023). The initiative's website provides essential information on the safety of children online.

In Germany, too, there is already plenty of material for professionals, children, parents, and legal guardians to raise awareness and support age-appropriate media education, such as "Klicksafe" – an initiative of the European Union for more safety on the Internet (klicksafe.de 2023). However, as mentioned earlier, the success of such information and support centres is largely contingent on their level of public recognition.

A final component of comprehensive prevention, mentioned repeatedly in the interviews, is the educational and therapeutic work with potential or already active offenders who display paedophilic tendencies. An ongoing project by the Finnish organisation Suojellaan Lapsia (Protect Children) explores the backgrounds of individuals

who search for sexual depictions of children on the darknet (Insoll, A. Ovaska, and Vaaranen-Valkonen 2022). Through a strategically placed anonymous survey (Help us to help you), available in 21 languages and appearing on the screens of consumers during such searches on the

darknet, new information has been

gathered about the behaviours, However, education in methods, and backgrounds of paedophilic offenders. Over half of school and family contexts the respondents expressed a desire to falls short if the issue of guit consuming abuse material, while 62% had actively attempted to stop online violence is not searching for and viewing such illegal simultaneously discussed content. The survey also revealed that 41% of consumers experienced at a broader societal level negative emotions such as guilt or in wider public discourse. shame while viewing the content, nearly half had had suicidal thoughts This discourse can also be at least once, and had considered *initiated and promoted by* seeking help. However, 23% of the respondents were too afraid to the state actually reach out to support services. An analysis of the data from Germanspeaking respondents (A. Ovaska

2023) paints a similar picture and shows that only 22% of German-speaking consumers saw no need to change their behaviour.

What these research findings indicate is that a significant proportion of individuals with paedophilic tendencies are aware that their behaviour is obsessive and illegal. Unfortunately, without help from elsewhere, they are unable to self-regulate their behaviour in any sustainable way. One of the few and globally unique projects for individuals with paedophilic tendencies is the prevention network "Kein Täter werden" (Don't become an offender) in Germany (Kein Täter werden 2023). This emphasises the need to further expand prevention and support services for (potential) offenders and to replicate similar projects in other countries. Targeted outreach and easily accessible support services are of great importance in this regard.

"It's about contacting these offenders and telling them directly: 'You're lurking around here. Seek help. We can help you.' A certain percentage of offenders will be annoyed at being approached. Others are grateful to have been contacted and will then accept our help because they are well aware they cannot quit it by themselves. [...] This shows that the offender must want it, but I also have to reach out to them, and there is a certain number, I don't want to quantify it statistically, but you can reach them through this." (Exp. 5, DE)

Participation of children and adolescents in prevention: safety by design

As adults often do not understand or share children's digital environments on an equal footing, it is essential to ask the children themselves what technical and legal framework would make their daily lives in the digital space safer. One expert notes:

Although children can still be impulsive, when working with children on online safety, it's quite astonishing how much more perceptive they are than us, adults. Where do they learn this? They learn a lot from peers, from experience. They educate themselves. [...] So, we need to start with them, ask them: 'What are some of your challenges? What do you need?' Only then can we protect them and help them protect themselves." (Exp. 7, DE)

The expert then goes on to talk about a 16-year-old Polish girl who, during the pandemic, created a website disguised as an online cosmetics shops where victims of domestic violence could send coded distress signals. "Ordering" a specific product, for instance, meant that an acute case of domestic violence was happening. This system filled a gap in reporting systems: children who depended on their family members' devices in cases where these family members were also the perpetrators were now able to send distress signals without being

discovered. Even if the perpetrator was looking over their shoulder, the distress signal remained undetected. Such and other peer-to-peer approaches are being researched as part of the "Protection through Online Participation" project (International Telecommunication Union 2023b).

The need for improvement on the part of the platform providers is also evident in our interviews. For example, 18-year-old Ming from Thailand reported that she was not able to find the crucial button to exit the video call with the abuser on the Omegle platform quickly enough (Case study 01, page 17). One of the interviewed experts also calls for "platforms intended for children should be designed in line with the principles of 'safety by design' and 'privacy by design'." These kinds of default settings should be in place, at a regulatory policy level." (Exp. 7, DE)

Based on research and consultation, the World Economic Forum defines safety by design as "ways technology companies can minimise online threats by anticipating, detecting, and eliminating online harms before they occur" (World Economic Forum 2023). In other words, it is a safety philosophy that we take absolutely for granted when it comes to analogue technical installations and that is written into law. The statements of the persons we interviewed underscore safety by design a basic demand.

Abuse victim Kitty from Thailand (Case study 04, page 22) is a victim of inadequate and opaque privacy settings. In the interview, she demonstrates ignorance about Facebook's privacy settings and assumes that Instagram is safer than Facebook. In reality, both platforms, owned by the same company, do offer settings that would have prevented Kitty's experience from happening. Built-in security features should be activated by default when profiles are created, rather than require the user to proactively search through the settings to find them. Due to limited life experiences, children are not aware of these mechanisms. As users of the relevant platforms, they must be consulted as part of the design and maintenance processes. Not only should mechanisms be available and pre-set for them, but they should also be heard as important sources of ideas and are likely to have original design suggestions regarding their own online world.

Basic requirement of "safety by design": preemptive elimination of risks online through a process of consultation and research.

Corporate responsibility: technical prevention

According to the respondents, a significant share of responsibility for children's safety online lies with the companies that provide platforms on which children experience abuse. What technical preventive and support measures are effective? This guestion is always interlinked

with the issue of legal requirements and corporate responsibility to systematically address and close gaps in digital child protection. Experts place a particular focus on age verification procedures.

"There was this case where one perpetrator was posing as a 12-year-old, and the other as a 13-year-old, and then both perpetrators met only to realise that neither of them was a child." (Exp. 3, DE)

However, age verification, or to a greater extent, any mandatory use of real names, is often seen to conflict with the right to privacy, data protection, and anonymity or pseudonymity on the Internet. The discourse around the issue sometimes results in a strong polarisation between child protection and data protection. In contrast, the experts we interviewed made their arguments by drawing an analogy between offline and online spaces. Just as in the analogue world, both these interests must be considered and safeguarded.

"Online platforms: no real name requirements, no registration requirements, no age controls, no moderation. Public spaces are monitored by the police, and there is social control in place. In digital spaces, this is generally not the case. The demand here should be that providers of digital infrastructures accessible to children must be required by policy to implement certain child protection mechanisms as a minimum standard, as an industry standard." (Exp. 2, DE)

Our interviewees dismiss the idea that protective measures like digital age verification constitute a significant violation of data protection and believe it to be unconvincing. "For decades now, you have been required to insert your ID card into cigarette vending machine to prove that you're over 18, and have we ever had much debate about the data protection of that?", notes Expert 2 (DE).

The fact that age verification should be performed by a third party is relevant as, when done this way, the user's right to anonymity (or pseudonymity) is safeguarded. When first registering on the a platform, the user should be directed to an external platform as part of the account creation process. Here, age verification can be performed through methods like uploading an identification document or linking to another service where the user's age is already verified (e.g., a bank or telecommunications provider), and

However, age verification, or to a greater extent, any mandatory use of real names, is often at odds with the right to privacy, data protection, and anonymity or pseudonymity on the Internet.

that the individual wishes to use. Owing to encryption, the verification service provider is not informed which platform the verification request originates from, while the platform only receives information about whether the individual is of legal age.

Just as in the analogue world, it must be possible to adjust and implement protection levels according to age. Privacy protection considerations must not result in perpetrators having easy access to children who can be exploited in unprotected digital spaces. Since the introduction of end-to-end encryption on the most popular messaging services, these chat platforms represent such spaces. One interviewee mentions the current EU regulation proposal for improved child protection on the Internet as an example of a solution to this global problem.

"That's why I'm a big fan of the EU regulation proposal by Ylva Johansson, according to which providers must conduct a risk analysis, develop technical solutions, scan their content for abuse material, and find ways to prevent cybergrooming." (Exp. 6, DE)

In addition to proposals such as the establishment of an EU centre for case reporting and knowledge consolidation, as well as a preventive risk analysis for platform providers, the current draft of the EU regulation also includes a measure to compel platform providers to temporarily lift end-to-end encryption in cases of suspicion and run initial scans for child sexual abuse material using artificial intelligence. This is why the EU regulation is incorrectly referred to as "chat surveillance" by its critics. However, this polarisation, observed both in politics and the media,

ignores the fact that the proposal includes plenty of innovative solutions and should not be reduced solely to this not yet entirely refined technical measure. The controversial discourse surrounding the EU regulation highlights yet again how the positions of data protection and child protection often compete with each other in the political and public arena.

the result is subsequently reported back to the platform



"This is the big, big fight. Is privacy in this case more important or is preventing and responding to abuse and exploitation of children more important?" (Exp. 7, DE)

But according to the respondents, the regulation is not the only possible solution. One expert hopes that "platforms themselves will see this issue as a top priority and perhaps

draw more attention to it, actively raising awareness of it on their platforms. 'If this or that happens to you, get out.'" (Exp. 1, DE)

Such warnings are already common practice on private-to-private sales platforms. When two Internet users trade goods or services through a platform, they do so by using the platform's own chat function. If one person suggests moving the discussion to text messaging or another chat channel, a warning is displayed. These warnings can also relate to photo content. Apple offers

device-based protection by using software on the device (i.e. not on a server) which analyses photos that minors wish to send via the Messages app on an Apple device. If nudity is identified on the image or video, a warning is displayed, without any data being sent to Apple for analysis. Experts also mention "SafeToNet" – a company from the UK which offers a similar analysis capability for detecting violence. However, such solutions have yet to become mainstream. The share of Apple in the messaging market is small, and the protection feature is not set as default. Even in respect of providers like "SafeToNet", an expert from the Philippines believes that it will require more societal pressure and, ultimately, legislative action for these measures to yield significant protective effects.

"I think it probably will take a significant push from consumers, just general users, because – again – a lot of technology companies are for-profit companies. I think it will probably involve some government regulation as well. But I do think that there are ways that we could deter this [online abuse] at the source before it ever gets out there." (Exp. 3, PH)

Legislation and law enforcement: need for regulation

Offences such as

exploitation through

livestreaming or trading

abuse material transcend

continental borders. Such

crimes on the Internet thus

represent a global problem

that requires global and

cross-border solutions.

It is ultimately the responsibility of governments to ensure an improved system of prevention and support. This can be achieved, for example, by enacting mandatory regulations for platform providers, implementing

governmental initiatives to raise public awareness, and allocating funding for various purposes, whether it be for research and science, the establishment of public reporting and counselling centres, prevention programmes for (potential) offenders, or the psychosocial support of victims.

What is essential in this regard is to maintain close collaboration with the various types of stakeholders who know the realities of the issue, so that the measures identified are actually effective and the

consequences of their implementation are appropriately considered. This must be done with a view to avoiding negative "side effects", such as the heightened demand on police capacity or "paralysis" of the police due to the tightening of German criminal law in 2021.

"I believe this is not just about political will, but also because there's a lack of understanding in politics about how advanced the technology is, how adept offenders have become, and how quickly everything happens. And this also means we can't afford to waste much time, as it comes at the expense of children." (Exp. 3, DE)

Another aspect that was mentioned multiple times in our interviews is the need for improved and standardised international cooperation among law enforcement agencies. Offences such as exploitation through livestreaming or trading abuse material transcend continental borders. Such crimes on the Internet thus represent a global problem that requires global and cross-border solutions. However, a major obstacle to implementation arises from different legal frameworks and approaches to data protection, varied priorities in criminal investigation, and disparities in the availability of national reporting and counselling centres and insufficient interconnection between them.

"On an international level, the only thing we seem to be able to agree on is that child abuse must be prosecuted somehow. So the hotlines have very different [...] areas that they focus on. [...] Some only handle child sexual abuse material, some also deal with child trafficking, or offline crimes related to children, but that really depends on the area. [...]" (Exp. 4, DE)

Jaika's case (Case study 02, page 19) underscores the importance of transnational law enforcement to detect cases, assist victims, and convict offenders. However, it also demonstrates how outrageously different sentencing can be, depending on the nationality of the offender, intermediary, and victim.

"In China, but also in Iran or Vietnam, there is the death penalty for child abuse for such offenders, and for this reason, the Federal Criminal Police Office never contacts at any time and the countries where there is the death penalty for child abuse.

This is because there is a risk that a German offender will be apprehended there and will then be sentenced to death there." (Exp. 4, DE)

The relevant paragraph

At this point, it is essential to highlight that despite the 2021 reforms mentioned, German criminal law still fails to sufficiently address different forms of sexual violence against children in the digital space, especially transnational ones. This is most vividly demonstrated in the case of livestreaming, where the consumer, despite their physical absence, exerts influence on the child in real-time, for example, by giving instructions, albeit usually indirectly through an intermediary. Under current law, an individual is considered a perpetrator only where, based on specific digital content, they are found to have had direct influence on the child (online). In other words, under current German criminal law, where the physical contact or communication is not executed personally or directly, a consuming offender can only be

convicted for participation (instigation or aiding and abetting) in such a crime, which carries a lesser penalty. The law sees the intermediary as the primary offender. The

legislation fails to properly reflect the severity of the acts committed by the consuming offenders, whose requests enable the abuse by the intermediary in the first place and who subsequently direct the abuse through their instructions (see International Justice Mission Deutschland e. V. and Rohne 2021).

The relevant paragraph of the German Criminal Code on sexual abuse of children without physical contact with the child, i.e. Article 176a, classifies a crime such as abuse through livestreaming as a petty offence. By contrast, possession of child pornography is a serious crime according to Article 184b, and carries a prison sentence of at least one year. Experts see this as a discrepancy in assessment because the consumer not only initiates and controls the analogue abuse in front of the livestream camera but can also make a recording of the livestream at any time and then disseminate it. Consequently, in its legislative proposal, IJM Deutschland e. V. appeals on the German government to "address [...] these inadequacies in the criminal prosecution of the emerging media-based

of the German Criminal

Code on sexual abuse of

children without physical

i.e. Article 176a, classifies

contact with the child.

a crime such as abuse

through livestreaming

By contrast, possession

of child pornography is a

serious crime according to

Article 184b, and carries a

prison sentence of at least

as a petty offence.

one year.

abuse of children and adolescents" (International Justice Mission Deutschland e. V. and Rohne 2021). This demand, particularly to regulate the demand side of livestreaming abuse, is also finding resonance with experts outside of Germany. For instance, an expert from the Philippines comments:

"I think the laws in the Philippines running after the facilitators, the laws in the Philippines are actually quite good. They're strict. They're quite well-written. Demand-side accountability in Western countries is really important. Increasing penalties and punishments in those places is an important part of it because I don't think it's right that just the facilitator in the Philippines faces life in prison. I think that the people in the Western countries fuelling this with their money and their desire to consume the content

should face stiffer penalties as well." (Exp. 3, PH)

One of the experts identifies another challenge in international cooperation, which is the fact that transnational law enforcement does not yet cover the entire spectrum of violence against children in the digital space. There are already some promising initiatives, particularly in the Asia-Pacific region, for investigating particularly severe forms of abuse, such as livestreaming, sale or commercialisation of abuse material. "This is something where Interpol works together, you have photo DNA from Microsoft that identifies this abuse pictures, so you don't need to look through … I mean, there is work there." (Exp. 7, DE)

When it comes to the issue of cybergrooming or cyberbullying, especially when the perpetrator is unknown, it becomes very challenging for international law enforcement agencies to pursue individual cases since they often lack the necessary technical tools required for this purpose.

In our interviews, it also becomes clear how law enforcement agencies, owing to limited resources, are forced to decide between victim identification, case investigation, or removal of material.

"Of course, it is a concern, but we have to work through investigative priorities step by step, and such material should not be allowed to be on the Internet. [...]

This requires a holistic approach that incorporates the tech industry, which should be required to prevent such material from being available on their servers in the first place. [...] In that case, our focus is on [...] based on the investigative approaches we have, as we probably won't be able to apprehend the perpetrator anyway, as they operate in the darknet for their own satisfaction. However, we might be able to identify the victim, for example, if we see a three-pin socket in the background, which is unique to the UK, [...] and then we might be able

to direct the case accordingly. Then we have approaches where the focus is on identifying the victim and rescuing them. In this case, admittedly, removal of the material has a lower priority, while higher priority is then given to safeguarding the victim's physical integrity. It is, simply speaking, a matter of proportionality." (Exp. 5, DE)

What emerges from the interviews we conducted is that, to overcome this problem and ensure effective (inter) national law enforcement, both financial and personnel resources as well as investment in personnel training must be increased as a matter of urgency. Another aspect is the acquisition and ongoing development of modern technology for law enforcement officers, who often complain that, at least in Germany, they do not have the authorisation to use many technological capabilities for reasons of data protection.

In one interview (Exp. 4, DE), a comparison is drawn to the United States and Canada, where the use of artificial intelligence in pilot projects for the identification of material and criminal investigation resulted in millions of instances of abuse material being removed from the Internet within a week. Another example is the use of so-called "fake child patrols" as seen in the research project "Sweetie 2.0" (Terre des Hommes NL 2023), aimed at proactively identifying exploitation through livestreaming by using a chatbot disguised as a 10-year-old Filipino girl created using computer animation technology. In the 10 weeks during which "Sweetie" was online, 1,000 potential offenders from 71 countries were identified. The data was handed over to Europol for distribution to the law enforcement agencies of the respective countries, resulting in numerous arrests and convictions.13

While complete removal of images from the Internet is nearly impossible, when new material is created, its circulation through downloading and sharing must be curtailed as quickly as possible.

However, the reporting centres and law enforcement agencies, including those in Germany, are currently not adequately prepared to handle such large amounts of data. Following on from that, there is the challenge of the speed at which cases can be processed and the abuse material removed. While complete removal of images from the Internet is nearly impossible, when new material is created, its circulation through downloading and sharing must be curtailed as

quickly as possible. In Germany, the average time from the receipt of abuse material by a reporting centre to its removal is approximately 2.4 days, which is relatively fast in international comparison (Exp. 4, DE). However, because analysing the material is very labour-intensive and detailed (e.g., examination of language or objects in the background) and is performed by specialised investigative

¹³ The "Sweetie" project underwent some changes, while the legal aspects of this innovative project are attracting much debate (N. Sunde and I. M. Sunde 2022, 7; van der Hof et al. 2019).

units, the success rate and speed in identifying victims and perpetrators is comparatively low. Europol, Interpol, Inhope, and the NCMEC each have their own databases and portals where individuals can provide tips for identifying abuse material. One expert comments:

"So, if you were to install technology internationally [...] at complaint centres and police investigative agencies worldwide that allowed you to simply check whether [the material] is known or not, it would translate into a lot of labour being saved and, at the same time, would remove so much child abuse from the Internet. [...] Unfortunately, what is another disadvantage is that there is still no common hash value database¹⁴, because hash values are also controversial, for example, under data protection law." (Exp. 4, DE)

As expressed in the statements made in the interviews, the use of technological innovations in law enforcement must go hand in hand with an increase in personnel resources, as an increase in the amount of material identified also requires a corresponding increase

in case processing capacities. Furthermore, cross-border communication must be improved, while information exchange among countries for investigative, preventive, and protective purposes needs to be intensified. This will allow well-functioning measures implemented in other country contexts to be replicated, and by learning from one another, potential failures can be avoided. Another point raised is the need for closer cooperation between law enforcement and the tech industry, adapted to international standards.

However, there are significant hurdles to implementation at the national level:

"There is no system, no strategy at the national level that brings together all these entities in a harmonised way that would propose a whole package. This is a gap at the country level but it is also something that is at the international level in the sense of ... countries are very much looking for best practices or good practices from other countries to reproduce." (Exp. 7, DE)

Furthermore, what is needed is not only external collaboration among countries but also internal

collaboration within countries, such as among German federal states and ministries, with more effective coordination and a unified, cross-departmental strategy. The current mode of working in "silos" and in independent, non-interconnected areas garners harsh criticism.

More standardisation and

As expressed in the statements made in the interviews, the use of technological innovations in law enforcement must go hand in hand with an increase in personnel resources, as an increase in the amount of material identified also requires a corresponding

increase in case

processing capacities.

More standardisation and networking are also required in the field of reporting and counselling centres, to ensure that victims can be assisted more promptly. Just as with the issue of media literacy as a mandatory school subject, the federal system in Germany encounters limitations due to the varying jurisdictions of the state and federal levels. For example, in North Rhine-Westphalia, there is already a state-funded digital reporting and counselling centre with a helpline and additional information for affected children, family members,

and professionals (The Federal Association of the Child Protection Association in North Rhine-Westphalia 2023). Moreover, cases reported via the platform are directly forwarded to the central contact point for cybercrime in the justice system of North Rhine-Westphalia. However, such centralised support centres do not exist in every federal state. Another example are so-called "online child safety watchdogs" (Federal Criminal Police Office 2023), and although they now exist in every federal state of Germany, they differ significantly in their online presence and scope. For instance, not all online watchdogs provide translations into sign language or plain language, or address the issue of violence in the digital space.

Our interviewees emphasise multiple times how important it is to have demand-oriented, child-friendly, and centralised reporting centres for victims of child abuse and to ensure that access to them is easy, straightforward,

¹⁴ A hash value is a unique alphanumeric value calculated for an image by a special algorithm. Hash values can then be used to identify and store identical or similar images or those depicting the same subject, without using the image itself for comparison, as doing so would violate the privacy of the depicted individuals.



unbureaucratic, and available in the respective national language at all times of the day and night. The discourse surrounding sexual violence against children online is often confined to individual contentious issues in the areas of politics, IT, or law enforcement. Levy and

Robinson aptly outline the problem of such particularistic perspectives: "We believe that one of the challenges with this particular policy debate is that governments and law enforcement have never clearly laid out the totality of the problem being tackled. In the absence of that, people infer a model that turns out to be incomplete or, in some cases, incorrect." (Levy and Robinson 2022a)

While the debate on appropriate measures to tackle online violence against children often gets lost in fragmented and polarised positions, any sustainable improvement in protection levels hinges on the various aspects being considered together and concerted action being taken. One interviewed expert remarks:

"We do believe that online safety is something that you can only tackle in a very complex equal system. You need all these different stakeholders to play their role." (Exp. 7, DE)

With the digitalisation of society, the consumption of child sexual abuse material has become significantly easier. This is because such material is readily available on the Internet, at any time of the day and is tailored to all preferences. At the same time, the Internet offers lower technical barriers to access minors and fewer protective structures than the analogue world. Due to the anonymity of the Internet, absence of borders, and the possibility of communicating in encrypted spaces and sometimes also using a fake profile, perpetrators often go undetected. Likewise, it would be impossible to approach hundreds of children at the same time in the analogue world.

Additionally, when using the Internet, perpetrators experience fewer emotional barriers when it comes to expressing their (tabooed) needs to others. It is reasonable to assume that not only individuals with primarily paedophilic or hebephilic preferences¹⁵ commit such

With the digitalisation of society, the consumption of child sexual abuse material has become significantly occurrence of paedophilia, easier. This is because such material is readily available self-generated material. on the Internet, at any time of the day and is tailored to

acts, as noted by an expert. 16 Just as in the case of exploitation in the analogue world, financial motives and power dynamics can also play a role. Therefore, the prevalence of online violence against children is much higher than the suspected especially if one includes digital violence among peers and sharing

Our interviews, following Neutze et al. (2015a) and Insoll et al. (2022), suggest that increased use of digital representations also leads to more offline incidents as inhibitions decrease, and new stimuli are sought. Bongen and Moßbrucker observe that the Internet often creates an environment "in which

paedophilic offenders get the feeling that it is normal to engage in sexual acts with children. Law enforcement officials who conduct investigations in this area told us during our research that it could often be observed how these platforms led to a loss of inhibitions, potentially leading more people to want to try things out in real life. Child and youth psychologists, as well as the Child Protection Association in Germany also confirm this in their statements." (Bongen and Moßbrucker 2022; see also Insoll, A. Ovaska, and Vaaranen-Valkonen 2022, 16)

The experts we interviewed agree with this assessment:

"Yes, especially when it comes to sexual offenders, they need a sense of excitement to feel any sort of satisfaction in the first place. And when they no longer get that excitement, they will then, of course, proceed to the next level, so images or video chats then naturally lead to meetings in real life." (Exp. 1, DE)

all preferences. At the same

lower technical barriers to

time, the Internet offers

access minors.

¹⁵ Individuals whose sexual interest is primarily or exclusively in children (paedophilic) or adolescents (hebephilic).

¹⁶ See also Sunde and Sunde (2022, 4), where an overview of various offender typologies is provided.

As a result, current research findings suggest that certain ideas, such as the targeted use of virtual reality or humanoid robots to "replace" real children in treating individuals with paedophilic preferences (Rutkin 2016; Chalmers 2022) are not likely to be effective. Qualitative data shows that increased consumption proportionally leads to more abuse and not to a controlled reduction in paedophilic desires (see also Insoll, A. Ovaska, and Vaaranen-Valkonen 2022).

Our interviews indicate a relatively high level of ignorance among the victims prior to their first experience of sexual violence online. This underscores the need for preventive counselling and education for children, particularly in schools, childcare facilities (e.g., daycare, child and youth welfare services), and within families. While many of today's generation of parents practically grew up with the Internet, digital spaces are constantly and rapidly evolving. Therefore, most legal quardians of children are not able to prepare their children for the digital world based solely on their own experience and intuition, nor are they equipped to recognise, prevent (e.g., through avoiding "sharenting") or appropriately respond to cases of abuse of their own children. Institutionalised education is also very slow to respond to the need of protecting young people on the Internet. Media literacy and child protection in the digital space must become government priorities internationally and they cannot afford to be delegated to other entities such as law enforcement agencies, companies, parents, or even federal states, as is the case with our federal education system in Germany.

Our data suggests that the primary threat posed by online violence is its scalability, with perpetrators being able to approach thousands of children relatively effortlessly. The contact attempt may be identified as dangerous and blocked by the majority of children, but given the high volume of attempts, the "small" percentage of children who do respond becomes relatively large. Therefore, the required scale and

reach of any prevention measures must be equally as extensive, taking the form of government awareness campaigns in both the analogue world and the digital space, involving celebrities and news agencies (see also Cousseran et al. 2023).

Livestreaming (including the resulting abuse in the analogue world) often happens in poverty contexts. Statements made by our interviewees clearly confirm this. In the Philippines, for example, the online environment has become very affordable. Even children from poorer backgrounds have access to smartphones and the Internet. In the context of this marginalisation, livestreaming is one of the few accessible ways for them to alleviate their poverty. This means that comprehensive poverty alleviation measures will also have an impact on the prevention of abuse through livestreaming. However, due to the fact that livestreaming is sometimes a community phenomenon, poverty alleviation measures must be offered in a very targeted manner to local communities that are identified as vulnerable. Law enforcement and social projects should always be closely interconnected.

Our data shows that particularly very young users of the Internet, do not yet have the level of maturity required to understand the power and exploitation structures of the Internet. During this phase of life, the need for recognition and validation in both digital and analogue lifeworlds makes children and adolescents vulnerable to control and coercion. While the exchange of sexual content for consumer goods may be more attractive to children from lower socio-economic backgrounds, or to children who are not allowed these goods at home, the validation offered by social media in the form of likes or clicks can be appealing to children from all socio-economic backgrounds. Younger children and adolescents, especially those in contexts where little or no education on sexual

Our interviews indicate a relatively high level of ignorance among the victims prior to their first experience of sexual violence online. self-determination is provided, often lack the sensitivity needed to recognise the dynamics of sexual violence. They may not realise that intimate images or videos can be shared against their will. Additionally, as they lack media literacy regarding the possibilities of material dissemination and the commercialisation of sexual content, children and adolescents are ultimately highly vulnerable on

the Internet. To adequately respond to the fact that the Internet is creating new opportunities for perpetrators every day, decisive and concerted action is urgently required at the levels of politics, law enforcement, education, and social work.



05. Political demands

As our study shows, the issue of sexual violence in the digital space is very complex and can only be addressed through successful collaboration of the various stakeholders involved. The ultimate responsibility for child protection is borne by the state, not least due to the obligations enshrined in the UN Convention on the Rights of the Child.

We therefore call on the German federal government to:

- Prioritise and implement the child's right to protection in the digital space. As part of this, a unified, cross-departmental national strategy should be introduced, while the national legislation must be revised in such a way that offences committed in the digital space can be adequately identified and penalised.
- Work on increasing public awareness and improving danger prevention in the digital space by implementing and promoting awareness-raising measures, such as government campaigns and collaborations with celebrities and media outlets.
- Introduce age-appropriate children's rights education and media literacy as a mandatory school subject from Year 1 and incorporate these areas into early childhood education. Child rights and media education must also be made part of the training curricula of teaching and care staff.
- Hold companies more accountable and advocate for mandatory child protection regulations on digital platforms according to the "safety by design" approach, which could include the introduction of risk assessments, stricter age and identity verification procedures, child-friendly privacy settings when creating user profiles, the introduction of warnings and safety notices, and easily accessible reporting options on the platforms themselves.

- Strengthen national law enforcement agencies through increased investment in knowledge and personnel development, the acquisition and use of new technologies, and mandatory training for police and the judiciary.
- Make children and adolescents part of the development and design of needs-based support and prevention programmes. Children, as "digital natives", are best suited to identify solutions that will work for them.
- Increase funding for research and science to better assess the impact of technological progress and its rapid developments on children, and to develop ways of responding to it effectively.
- Promote the targeted expansion of social and therapeutic support and counselling services, as well as prevention programmes for affected children, their families, and (potential) perpetrators.
- Support families affected by poverty through sustainable development cooperation and strengthening social safety nets to prevent the financially motivated exploitation of children.
- Promote more effective cooperation and collaboration between governments, the tech industry, and transnational law enforcement agencies, in line with international standards. This is because a global problem requires global solutions.

06. Appendix: Overview of interviews

- 1) **Exp. 1,** DE, female, an organisation for media oversight at a regional level
- 2) **Exp. 2,** DE, male, a psychosocial organisation for the prevention of sexual violence against children
- 3) **Exp. 3,** DE, female, a company offering IT forensic services
- 4) **Exp. 4,** DE, male, an organisation for media oversight at a national level
- 5) **Exp. 5,** DE, male, a law enforcement agency at a national level
- 6) Exp. 6, DE, female, an international prevention organisation with a focus on sexual violence against children
- 7) **Exp. 7,** DE, female, a multilateral institution for information and communication technologies
- 8) **Exp. 1,** IN, female, a prevention and advocacy organisation at a national level with a focus on sexual violence against children
- 9) **Exp. 2,** IN, male, an advocacy and research organisation at a national level with a focus on sexual violence against children
- 10) **Exp. 3,** IN, female, a private psychotherapeutic practice and counselling centre with a focus on primary prevention of sexual violence
- 11) **Exp. 4,** IN, female, a help, prevention, and advocacy organisation at a national level with a focus on sexual violence against children
- 12) Vict. 1, IN, non-binary, pseudonym "Roh", aged 23
- 13) Vict. 2, IN, female, pseudonym "Riona", aged 17
- 14) Vict. 3, IN, male, pseudonym "Shubb", aged 24
- 15) **Exp. 1,** PH, female, an urban social institution
- 16) Exp. 2, PH, female, a non-governmental organisation at a national level with a focus on human trafficking
- 17) **Exp. 3,** PH, male, a non-governmental organisation at a national level with a focus on human trafficking
- 18) **Exp. 4,** PH, female, an international non-governmental organisation with a focus on child protection
- 19) **Exp. 5,** PH, male, multilateral institution for drug control
- 20) Vict. 1, PH, male, pseudonym "Ace", aged 19
- 21) Exp. 1, TH, female, national law enforcement agency with a focus on technology and crime
- 22) Exp. 2, TH, male, a judicial institution at a regional level
- 23) Exp. 3, TH, female, an international network with a focus on sexual violence against children and human trafficking
- 24) **Exp. 4,** TH, female, a research and education institution at a national level with a focus on women's rights, rural development, and social sciences
- 25) Exp. 5, TH, female, social institution at a national level with a focus on women's rights and child protection
- 26) Vict. 1, TH, female, pseudonym "Ming", aged 18
- 27) Vict. 2, TH, female, pseudonym "Kitty", aged 17

07. Bibliography

Akgul, Arif, Cuneyt Gurer and Hasan Aydin. 2021. "Exploring the Vicitmization of Syrian Refugees through the Human Security Model: An Ethnographic Approach". Studies in Ethnicity and Nationalism 21 (1): 1–21.

Ali, Sana and Saadia Anwer Paash. 2022. "A Systematic Review of the Technology Enabled Child Sexual Abuse (OCSA) & Its Impacts". Journal of Legal, Ethical and Regulatory Issues (25, S5): 1–18.

Alig, Olivia. 2023. Sharenting, Mama-Blogger, Kinderinfluencer & Co. Eine rechtliche Betrachtung. Bonn: Bundeszentrale für Kinder- und Jugendmedienschutz. Retrieved on 3 July 2023. https://www.bzkj.de/bzkj/service/publikationen/bzkj-aktuell/sharenting-mama-blogger-kinderinfluencer-co-eine-rechtliche-betrachtung-187318.

Araújo, Ana Valentina Medeiros de, Cristine Vieira do Bonfim, Magaly Bushatsky and Betise Mery Alencar Furtado. 2022. "Technology-Facilitated Sexual Violence: A Review of Virtual Violence against Women". Research, Society and Development 11 (2). https://doi.org/10.33448/rsd-v11i2.25757.

Baker, Amy and Mel Schneiderman.

2015. Bonded to the Abuser: How Victims Make Sense of Childhood Abuse. Lanham: Rowman & Littlefield.

Beitzinger, Franz, Uwe Leest and Christoph Schneider.

2020. Cyberlife III: Spannungsfeld zwischen Faszination und Gefahr. Cybermobbing bei Schülerinnen und Schülern. Dritte empirische Bestandsaufnahme bei Eltern, Lehrkräften und Schüler/-innen in Deutschland. Karlsruhe: Bündnis gegen Cybermobbing, Techniker Krankenkasse.

Berson, Ilene. 2003. "Grooming Cybervictims". Journal of School Violence 2 (1): 5–18. https://doi. org/10.1300/J202v02n01_02.

Bongen, Robert and Daniel Moßbrucker. 2022. "Darstellungen von Kindesmissbrauch: Das Netz vergisst nichts, solange es nicht vergessen soll". Retrieved on 12 April 2023. https://netzpolitik.org/2022/darstellungen-von-kindesmissbrauch-dasnetz-vergisst-nichts-solange-es-nichtvergessen-soll/.

Boracetti, Marco. 2017. "Trafficking in Human Beings and Human Security: A Comprehensive Approach". In Blurring Boundaries: Human Security and Forced Migration, edited by Stefan Salomon, Lisa Heschl, Gerd Oberleitner and Wolfgang Benedek, 185–210. Leiden, Boston: Brill.

Bundeskriminalamt. 2023.

"Onlinewachen der Landespolizeien". Retrieved on 10 July 2023. https://www.bka.de/DE/KontaktAufnehmen/Onlinewachen/onlinewachen_node.html.

Chalmers, David. 2022. Reality+: Virtual Worlds and the Problems of Philosophy. New York: Norton.

Cousseran, Laura, Christa Gebel, Johanna Tauer and Niels Brüggen. 2023. Umgang von Kindern mit Interaktionsrisiken im Internet. Berlin: Deutsches Kinderhilfswerk. Retrieved on 10 July 2023. https://www.dkhw.de/schwerpunkte/medienkompetenz/informationen-zur-mediennutzung/studie-online-interaktionsrisiken/. DeFelice, Deborah. 2017. "The Right

to Security of Online Childhood". The International Journal of Children's Rights 25 (3-4): 573–98. https://doi.org/10.1163/15718182-02503001.

Direction Générale de la Cohésion Sociale. 2023. "Je protège mon enfant: la plateforme d'information et d'accompagnement à la parentalité numérique". Retrieved on 5 July 2023. https://jeprotegemonenfant.gouv.fr/.

Durkin, Keith and Ronald DeLong. 2012. "Internet Crimes Against
Children". In Encyclopedia of Cyber
Behavior, edited by Zheng Yan.
3 Bände, 799–806. Hershey: IGI Global.
https://www.igi-global.com/chapter/
encyclopedia-cyber-behavior/64803.

ECPAT Deutschland, 2023.

"Kinderpornografie". In Worte schaffen Wirklichkeit: Der Begriffscheck: https://www.terminologie.ecpat.de, edited by ECPAT Deutschland.

ECPAT International. 2016.

Terminologischer Leitfaden: Für den Schutz von Kindern vor sexueller Ausbeutung und sexualisierter Gewalt. Adopted by the Interinstitutional Working Group in Luxembourg on 28 January 2016. https://ecpat.de/wp-content/uploads/2018/11/ECPAT-Terminologischer-Leitfaden-DE.pdf.

Engfer, Anette. 2006. "Misshandlung, Vernachlässigung und Missbrauch von Kindern". In Entwicklungspsychologie: Lehrbuch, edited by Rolf Oerter and Leo Montada. 5th edition, 800–817. Weinheim: Beltz.

Europol 2020. Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic. Retrieved on 4 July 2023. https://www.europol.europa.eu/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf.

Fleer, Marilyn. 2016. "Theorising Digital Play: A Cultural-Historical Conceptualisation of Children's Engagement in Imaginary Digital Situations". International Research in Early Childhood Education 7 (2): 75–90. https://eric.ed.gov/?id=ej1138705.

Gebel, Christa, Claudia Lampert, Niels Brüggen, Stephan Dreyer, Achim Lauber and Kira Thiel. 2022.

Jugendmedienschutzindex 2022.
Der Umgang mit online bezogenen
Risiken: Ergebnisse der Befragung von
Kindern, Jugendlichen und Eltern.
Berlin, Hamburg, München: FSM –
Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. Retrieved on
26 June 2023. https://www.fsm.de/
files/2023/01/fsm_jmsindex_2022_
barrierefrei.pdf.

Gulowski, Rebecca and Christina Krüger. 2020. "Jugendliche reden über sexualisierte Gewalterfahrungen vor allem mit ihren Peers: Erste Erkenntnisse aus dem BMBF-Projekt 'Peers als Adressatinnen und Adressaten von Disclosure und Brücken im Hilfesystem". Bundeszentrale für gesundheitliche Aufklärung - Forum Sexualaufklärung und Familienplanung (1): 30–33. https://shop.bzga. de/pdf/13329236.pdf#page=30.

Haq, Mahbub ul. 1995. Reflections on Human Development. New York, Oxford: Oxford University Press.

Hengst, Heinz and Helga Zeiher.

2005. "Von Kinderwissenschaften zu generationalen Analysen. Einleitung". In Kindheit soziologisch, edited by Heinz Hengst and Helga Zeiher. 1st edition, 9–24. Wiesbaden: VS Verlag für Sozialwissenschaften.

Hosny, Nadine, Adam Danquah, Katherine Berry and Ming Wai Wan.

2020. "Children's Narratives of Family Life in Ghana: A Cultural Lens via Story Stems". Journal of Child and Family Studies 29 (12): 3521–35. https://doi.org/10.1007/s10826-020-01839-6.

Insoll, Tegan, Anna Ovaska and Nina Vaaranen-Valkonen. 2022.

CSAM Users in the Dark Web: Protecting children through prevention - Redirection survey report. Helsinki: Suojellaan Lapsia / Protect Children. Retrieved on 10 July 2023.

https://www.suojellaanlapsia.fi/en/post/csam-users-in-the-dark-web-protecting-children-through-prevention

Insoll, Tegan, Anna Katariina Ovaska, Juha Nurmi, Mikko Aaltonen and Nina Vaaranen-Valkonen. 2022. "Risk Factors for Child Sexual Abuse Material Users Contacting Children Online". Journal of Online Trust and Safety 1 (2): 1–24. https://doi.org/10.54501/jots.v1i2.29.

International Justice Mission and Inter-Agency Council against Trafficking. 2020. Online Sexual Exploitation of Children in the Philippines. Washington: IJM & IACAT. Retrieved on 17 March 2023.

International Justice Mission Deutschland e.V. and Holger

Rohne. 2021. Vorlage für einen Entwurf eines Gesetzes zur Änderung des Strafgesetzbuches zur Bekämpfung sexualisierter Gewalt an Kindern, insbesondere sexueller Online-Ausbeutung von Kindern (OSEC). Berlin: IJM. Retrieved on 10 July 2023. https://paragonn-cdn3.ams3.digitaloceanspaces.com/ijmdeutschland.de/documents/Studien/IJM-Gesetzesentwurf-zur-A%C-C%88nderung-des-StGB-zur-Beka%CC%88mpfung-sexualisiert-er-Gewalt-an-Kindern.pdf.

International Telecommunication Union. 2023a. "Digital Development Dashboard: An Overview of the State of Digital Development Around the World Based on ITU data; Infrastructure and Access". Retrieved on 7 June 2023. https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx.

International Telecommunication Union. 2023b. "POP: Protection through online Participation". Retrieved on 5 July 2023. https://www.itu.int/en/ITU-D/

Cybersecurity/Pages/COP/POP.aspx.

Internet Watch Foundation.

2023. "'Self Generated' CSAM: 2022's Trends & Data". Retrieved on 22 June 2023. https://annualre-port2022.iwf.org.uk/trends-and-data/self-generated-csam/.

Joleby, Malin, Sara Landström, Carolina Lunde and Linda Jonsson.

2021. "Experiences and Psychological Health among Children Exposed to Online Child Sexual Abuse: A Mixed Methods Study of Court Verdicts". Psychology, Crime & Law 27 (2): 159–81. https://doi.org/10.1080/1068 316X.2020.1781120.

Jonsson, Linda, Cecilia Fredlund, Gisela Priebe, Marie Wadsby and Carl Göran Svedin. 2019. "Online Sexual Abuse of Adolescents by a Perpetrator Met Online: A Cross-Sectional Study". Child and Adolescent Psychiatry and Mental Health 13 (32). https:// doi.org/10.1186/s13034-019-0292-1.

Kein Täter werden. 2023. "Hilfe für Menschen, die sich sexuell zu Kindern hingezogen fühlen: Präventionsnetzwerk". Retrieved on 10 July 2023. https://www.kein-taeter-werden.de/.

Kinderschutzbund Landesverband Nordrhein-Westfalen. 2023.

"Beratungsangebote per Telefon und im Internet - Kinderschutz in NRW". Retrieved on 10 July 2023. https://www.kinderschutz-in-nrw. de/rat-und-hilfe/beratungsangebote-per-telefon-und-im-internet/.

Kjaerulf, Finn and Rodrigo Barahona. 2010. "Preventing Violence and Reinforcing Human Security: A Rights-Based Framework for Topdown and Bottom-up Action". Revista Panamericana de Salud Pública 27 (5): 382–95. https://doi.org/10.1590/s1020-49892010000500009.

klicksafe.de. 2023. "klicksafe.de: Die EU-Initiative für mehr Sicherheit im Netz". Retrieved on 10 July 2023. https://www.klicksafe.de/. Levine, Diane, Alison Page, Effie Lai-Chong Law and Michelle O'Reilly. 2021. Children and Families' Wellbeing in a Digital World: a Four-Dimensional Model. London: University of Leicester. https://www.researchgate.net/profile/diane-levine-2/publication/354468302_children_and_families'_wellbeing_in_a_digital_world_a_four-dimensional_model/links/6139fd39d1bbee063c5adeaa/children-and-families-wellbeing-in-a-digital-world-a-four-dimensional-

Levy, lan and Crispin Robinson. 2022a. "Is It Possible to Reconcile Encryption and Child Safety?". Retrieved on 9 May 2023. https://www.lawfareblog.com/ it-possible-reconcile-encryption-and-child-safety.

model.pdf.

Levy, lan and Crispin Robinson. 2022b. "Thoughts on Child Safety on Commodity Platforms (Preprint)". https://arxiv.org/pdf/2207.09506.pdf.

Liebel, Manfred. 2017. Postkoloniale Kindheiten: Zwischen Ausgrenzung und Widerstand, Weinheim: Beltz

Lock, Sam. 2018. "Paedophile Complains He's Been Humiliated by People on the Street". Daily Mail Online Australia, 14 May 2018. ... https://www.dailymail.co.uk/news/article-5725055/Depraved-paedophile-complains-hes-humiliated-street-outraged-passers-by.html.

Martin, Jennifer. 2016. "Child Sexual Abuse Images Online: Implications for Social Work Training and Practice". British Journal of Social Work 46 (2): 372–88. https://doi.org/10.1093/bjsw/bcu116.

Mayring, Philipp. 2022. Qualitative Inhaltsanalyse: Grundlagen und Techniken. Weinheim, Basel, Grünwald: Beltz.

National Center for Missing & Exploited Children. 2021a. "2021

Reports by Electronic Service Providers (ESP)". Retrieved on 2 May 2023. https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-esp.pdf.

National Center for Missing & Exploited Children. 2021b.

"CyberTipline Reports by Country". Retrieved on 23 May 2023. https://www.missingkids.org/content/dam/missingkids/pdfs/2021-reports-by-country.pdf.

National Center for Missing & Exploited Children. 2023.

"CyberTipline Data". Retrieved on 28 June 2023. https://www. missingkids.org/gethelpnow/ cybertipline/cybertiplinedata.

Nennstiel, Sabrina und Meike Isenbarg. 2021. Kinder und Jugendliche als Opfer von Cybergrooming: Zentrale Ergebnisse der 1. Befragungswelle. Düsseldorf: Landesanstalt für Medien NRW. Retrieved on 12 May 2023. https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Medienorientierung/Cybergrooming/211216_Cybergrooming-Zahlen_Praesentation_LFMNRW.PDF.

Neutze, Janina, Rainer Banse, Peer Briken, Jörg Fegert, Lutz Goldbeck, Jürgen Hoyer und Pekka Santtila. 2015a. MiKADO - Missbrauch von Kindern: Aetiologie, Dunkelfeld, Opfer: Zentrale Ergebnisse des Foschungsverbundes. Retrieved on 24 May 2023. http://www.mikado-studie.de/tl_files/mikado/upload/MiKADO_Zusammenfassung.pdf.

Neutze, Janina, Michael Osterheider, Rainer Banse, Peer Briken, Jörg Fegert, Lutz Goldbeck, Jürgen Hoyer und Pekka Santilla. 2015b.

MiKADO – Missbrauch von Kindern: Ätiologie, Dunkelfeld und Opfer. Präsentation "Von MiKADO lernen". Regensburg: Universität Regensburg. Retrieved on 24 May 2023. http://www.mikado-studie.de/tl_files/mikado/upload/MiKADO%20_%20 Ergebnisse.pdf.

Ovaska, Anna. 2023. Deutschsprachige Nutzer von Darstellungen sexuellen Missbrauchs von Kindern im Darknet. Helsinki: Suojellaan Lapsia / Protect Children. Retrieved on 10 July 2023. https://www.suojellaanlapsia.fi/en/post/communication-on-german-speaking-csam-users.

Pohle, Sophie, Kai Hanke, Julia Landrock und Cornelia Jonas. 2023.

Bewältigungsstrategien von Kindern im Kontext von Online-Interaktionsrisiken: Metarecherche 2023. Berlin: Deutsches Kinderhilfswerk.

Proposition de loi n°758 visant à garantir le respect du droit à l'image des enfants. Assemblée nationale. 13 January 2023. Retrieved on 3 July 2023. https://www.assemblee-nationale.fr/dyn/16/textes/116b0758proposition-loi#_ftn5.

Rutkin, Aviva. 2016. "Could Sex Robots and Virtual Reality Treat Paedophilia?".

Retrieved on 24 May 2023. https://www.newscientist.com/ article/2099607-could-sex-robots-and-virtual-reality-treat-paedophilia/.

Salminen, Mirva und Kamrul

Hossain. 2018. "Digitalisation and Human Security Dimensions in Cybersecurity: An Appraisal for the European High North". Polar Record 54 (2): 108–18. https://doi.org/10.1017/s0032247418000268.

Salter, Michael and Tyson Whitten. 2022. "A Comparative Content Analysis of Pre-Internet and Contemporary Child Sexual Abuse Material". Deviant Behavior 43 (9): 1120–34. https://doi.org/10.1080/016 39625.2021.1967707.

SPD-Bundestagsfraktion. 2023. Kinder vor sexualisierter Gewalt schützen: Kinderschutz geht uns alle an. Retrieved on 19 June 2023. https://www.spdfraktion.de/presse/pressemitteilungen/kinderschutz-geht-uns-alle.

Srivastava, Ankur, Joshua Rusow, Sheree Schrager, Rob Stephenson and Jeremy Goldbach. 2023. "Digital Sexual Violence and Suicide Risk in a National Sample of Sexual Minority Adolescents". Journal of Interpersonal Violence 38 (3-4): 4443–58. https://doi.org/10.1177/08862605221116317.

Steel, Chad. 2009. "Web-Based Child Pornography". International Journal of Digital Crime and Forensics 1 (4): 58–69. https://doi.org/10.4018/jdcf.2009062405.

Stoilova, Mariya, Sonia Livingstone and Rana Khazbak. 2021. Investigating Risks and Opportunities for Children in a Digital World:
A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Paper, Nr. 03. Florenz: UNICEF. Retrieved on 29 March 2023. https://www.unicefirc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf.

Sunde, Nina and Inger Marie Sunde. 2022. "Conceptualizing an Al-based Police Robot for Preventing Online Child Sexual Exploitation and Abuse". Nordic Journal of Studies in Policing 8 (2): 1–21. https://doi.org/10.18261/ issn.2703-7045-2021-02-01. Terre des Hommes NL. 2023. "Sweetie: Our Weapon against Child Webcam Sex". Retrieved on 22 June 2023. https://www.terredeshommes.nl/en/projects/sweetie.

Van der Hof, Simone, Ilina Georgieva, Bart Schermer and Bert-Jaap Koops. 2019. Sweetie 2.0: Using Artificial Intelligence to Fight Webcam Child Sex Tourism. Information Technology and Law Series 31. The Hague: T.M.C. Asser. https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=5811803.

Vobbe, Frederic and Katharina Kärgel. 2022. "Umgang mit Ängsten als Folge mediatisierter sexualisierter Gewalt". In Sexualisierte Gewalt und digitale Medien, edited by Frederic Vobbe and Katharina Kärgel, 143–66. Wiesbaden: Springer Fachmedien Wiesbaden.

Wachs, Sebastian and Sophia Bock. 2023. "Cybergrooming: wenn Jugendliche online sexuelle Grenzverletzungen und Gewalt erfahren". In Digitale Kindeswohlgefährdung: Herausforderungen und Antworten für die Soziale Arbeit, edited by Kay Biesel, Paul Burkhard, Rahel Heeg, Olivier Steiner, Heinz Kindler, Thomas Meysen, Daniel Hajok, Nadia Kutscher, Sebastian Wachs and Clarissa Schär, 110–31. Leverkusen-Opladen: Verlag Barbara Budrich.

Wihstutz, Anne, ed. 2019. Zwischen Sandkasten und Abschiebung: Zum Alltag junger Kinder in Unterkünften für Geflüchtete. Leverkusen: Budrich.

World Bank Open Data. 2023. "Population, total: All Countries and Economies". Retrieved on 23 May 2023. https://data.worldbank.org/.

World Economic Forum. 2023. "Safety by Design (SbD)".

Retrieved on 30 June 2023. https://www.weforum.org/projects/safety-by-design-sbd.

Wright, David and Fanny Rotino. 2020. Guidelines for Policy-Makers on Child Online Protection. Geneva: International Telecommunication Union (ITU). Retrieved on 29 March 2023. https://www.itu-cop-guidelines. com/.

Zumbrängel, Lambert. 2020. "Digitale Lebenswelten von Kindern und Jugendlichen. Eine medienpädagogische Querschnittsaufgabe für die Jugendarbeit". Forum für Jugendarbeit (3): 35–38. https://www.kinder-undjugendarbeit. de/fileadmin/user_upload/ FORUM_2020/Zumbraegel_ FORUM_3-2020-3.pdf. Retrieved on 8 June 2023.











