Der Kinderschutzbund
Bundesverband

Statement by the Child Protection Association (Der Kinderschutzbund Bundesverband e.V.) on the Public Hearing of the Digital Affairs Committee on "Chat Control" on Wednesday, March 1, 2023, 2 to 4 p.m.

Content

The Child Protection Association

The Child Protection Association has been committed to the protection of children in Germany and their rights since it was founded in 1953 in Hamburg. We want to ensure that children grow up without poverty and are protected from violence. Our goal is a child-friendly society in which the mental, emotional, social and physical development of children and adolescents is promoted. Children and adolescents should be involved in all decisions, planning and measures that affect them. Our work is based on the Convention on the Rights of the Child and ranges from lobbying for child-friendly legislation to practical daily work with children, youths, and their families. In doing so, it also focuses on the digital world and follows General Comment No. 25 of the UN Committee on the Rights of the Child. For more information on the goals of the Kinderschutzbund, please refer to the mission statement, the supplementary digital mission statement and the children's policy program.

We appreciate the opportunity to comment on the questions below. We will answer questions 1-18 from the questionnaire on the following pages.

The Proposal and its Implications

1. **The EU Commission's proposal for the CSA Regulation, also known as chat control, has generated much discussion since its publication in May 2022. Please explain the technical, legal, privacy, social and/or societal implications of the proposal.**

The EU initiative sends a clear signal to all EU states to take stronger action against sexualized violence against children. We strongly welcome this and agree with several aspects of the proposal. The core of the EU Commission's regulatory proposal to establish rules to prevent and combat sexualized violence against children (CSAR) focuses on child protection online. The goal is to combat the creation and digital dissemination of depictions of sexualized violence against children and thus the violence itself. To implement this important goal, the directive proposes necessary and correct measures, but goes too far at crucial points. In particular, scanning encrypted private communications in messenger services (such as WhatsApp or Signal) or emails without any reasonable cause is neither proportionate nor effective. This deeply interferes with the fundamental rights of children and young people, whose growing up in an environment where freedom of expression and confidential communication are only natural, is an essential pillar of democracy and participation. We also fear that when scanning is carried out without any reason, children and young people will be criminalized much more frequently - a trend that is already visible in German crime statistics. This is due to the fact that children and young people themselves often send images that can be classified as pornographic, making them liable to prosecution.

In this debate, data protection and child protection are often played off against each other - an approach that does not do justice to the matter at hand. Children's rights need both: the right to physical integrity, but also the right to protected communication. An unprovoked attack on encrypted personal messages invalidates an essential constitutional right, and with it several children's rights that have constitutional status in the EU. They are pillars of our democracy and growing up in a liberal democratic society is shaped by such warranty.

The right to privacy in particular, but also the right to freedom of expression, the right to information, and protection against violence, are essential for children's development. Only if they can trust that they will not be constantly monitored can they develop the necessary trust in their guardians, teachers and friends, which helps them to seek help from trusted persons when necessary and to inform themselves about certain topics without having to fear consequences. This is particularly relevant for children and young people who are affected by discrimination because of their sexual or gender identity, disability, origin or skin color or other markers of discrimination, because they are exposed to special risks online.[1]

Useful Methods for Children's Rights Online

For instance, we consider effective age verification (albeit without mandatory identification and collection of biometric data) to be a reasonable method in the proposal, as are security requirements and the obligation to conduct risk analyses for providers - both of hosting and of platforms such as those subsumed under social media. They are to protect their facilities from being used for purposes of offering, storing, or sharing depictions of sexualized violence against children. The same applies to cyber-grooming

[1] https://home.crin.org/readlistenwatch/stories/encryption-debate

- here we also advocate for requirements such as high-quality, sensitive moderation of chats, age verification (with the above-mentioned restrictions) and so-called pattern analysis, which can be used to detect groomers in order to block and/or report them. In addition, easily accessible reporting procedures for children and young people who need help are necessary. There must be easily understandable descriptions of the help offered and professionally qualified offers. We support the plan to make the previously voluntary scanning of images on large public platforms and filehosters mandatory – both the search for known material (hashes) and for new data (AI support). We also applaud the establishment of a central authority that, like the NCMEC, collects data, develops strategies, supports new technical procedures, and both controls and accompanies companies in risk assessments. This body, in our opinion, must be independent (especially from Europol) and work closely with child protection organizations.

However, we do not agree with one key component of the Commission's proposal, which is the so-called "discovery order", commonly referred to as "chat control". According to this, it is possible to scan the communications of all customers of a provider for weeks and months at the end of an official and legal procedure. This applies to companies that fail to meet their obligations to minimize risk and where a "significant risk" pertains. This groundless monitoring of communications is a deep intrusion into the fundamental right of freedom of communication, an essential component of freedom of expression, and an important right of children. We fear repercussions on the behavior of children and young people simply by having this option. A "chat control" contradicts the effort to balance fundamental rights and to weigh the interests. Investigators and AI experts also view this component critically.

Regardless of these concerns, we point out that the wrong people are being held accountable juggling the legal aspects of the issue: If service providers do not follow the requirements, customers' rights are restricted (imagine something similar with the Money Laundering Act - if banks are negligent, the accounts of all customers would then be monitored).

One of our key demands is to invest more in research. We need data, facts, and figures to put the broad discussion on a common ground. For example, the known numbers of investigative successes are only comprehensible from the brightfield. However, there is a much larger dark field, which is why we are also calling for research into it:

- Impact of digitally available representations and chats on the dark field, on perpetrators and acts in the social surroundings (interaction).
- Cyber-grooming - research of cases, verification of resulting acts / real encounters / weaknesses in chats and chat moderation / approach of perpetrators
- The connection and interactions of online material, chats, communities to real acts
- Perpetrator profile: abuse of power between pedosexuality and redirection activity
- Does David Finkelhor's theory of grooming (four-factor model) also apply in digital space?
- The acts in the social surroundings, in families, neighborhoods, circles of friends, clubs, etc. and the resulting digital acts
- Where does new material come from and how can it be tracked safely?
- New technical possibilities for risk reduction - the new EU authority in duty

There is no doubt about the urgency of this bill's concern to combat sexualized violence against children. However, as we have outlined here, we strongly doubt the effectiveness of the proposed measures in their current form. Once again, we highlight the UN Convention on the Rights of the Child as well as

General Comment 25 (i.e. children's rights in the digital world), which is equivalent to a federal law. This is because, in addition to the protection of children, their participation and empowerment must also be given the same priority when formulating legal measures.

Cyber-Grooming

2. The Commission's proposal provides for the issuance of detection orders, which will lead to providers of communications services or devices having to covertly leak information if there is a suspicion that abusive material is being exchanged via these services or devices or that grooming is taking place on them. In your view, which services and devices are potentially affected by this and to what extent, and what impact will this have on their users?

The recent study on cyber-grooming from 2022 by the Media Authority of North Rhine-Westphalia (Landesanstalt für Medien NRW)[2] has shown that cyber-grooming is increasingly taking place on Instagram, TikTok, on WhatsApp and also on gaming platforms. It can basically happen at any place that offers contact opportunities. Services frequently used by children and young people are particularly interesting for perpetrators. These include large online platforms such as YouTube and Twitch, social networks such as TikTok, Instagram and Facebook, but also online games and gaming platforms such as Fortnite, Steam, FIFA22 Online, or Minecraft. In order to circumvent the security precautions of the platforms, the perpetrators often try to switch to more private communication channels after the initial contact, for example to messengers such as WhatsApp or video chat services.[3] These are platforms with a very large reach that are used by millions of users every day.

Abusive material is often exchanged on public platforms - on the one hand, to make the material easily accessible and attract interested parties, and on the other hand, offers from "newcomers" can be found on large platforms. More professionally, perpetrators create accounts (e.g. on TikTok, etc.), set them to private and provide them with abusive material, and then transmit the access data. Abusive material that is offered in closed groups, for instance, including on the darknet, could best be discovered by enabling investigators to "patrol" online more frequently. The legal means to do so exist (e.g., offering artificially generated material as a ticket).

The impact on users is severe. People affected by digital violence (e.g. cyber bullying, cyber grooming, hate speech) often withdraw from the internet.[4] They are thus restricted in their fundamental rights such as participation, access, freedom of information and expression, and also privacy. Moreover, it is now known that digital violence has just as devastating an impact on mental health as all other forms of violence. Often, victims do not seek help, for example because they are ashamed or do not trust other

[2] see https://www.medienanstalt-nrw.de/themen/cybergrooming/ein-viertel-aller-kinder-und-jugendlichen-wurde-bereits-im-netz-von-erwachsenen-zu-einer-verabredung-aufgefordert.html
[3] see https://www.klicksafe.de/cybergrooming
[4] Girls and young women in particular, especially those who face multiple forms discrimination, are affected by digital violence. Plan International's 2020 study on digital violence against girls and young women ("World Girl Report") shows that those affected withdraw from social media and are thus excluded from participation, freedom of expression, freedom of information and other fundamental rights. https://www.plan.de/presse/pressemitteilungen/detail/welt-maedchenbericht-2020-digitale-gewalt-vertreibt-maedchen-und-junge-frauen-aus-den-sozialen-medien.html

people (or authorities) enough to seek appropriate support.

Technology Alone Does Not Protect from Violence

3. In your opinion, why is the Commission's proposal suitable or not suitable to effectively protect children from (sexual) assault and the dissemination of abusive material, and where do you see a concrete need for action?

The proposal in its current form not only raises constitutional questions, but overall the technical implementation remains poor. The focus on a technical solution is too biased and remains blind to a problem that affects society as a whole. Relying on purely technical solutions to protect children from sexualized violence online is a fatal mistake with devastating consequences for the fundamental democratic rights of all people, especially children. Experts from different fields (IT, data protection, human rights, lawyers, etc.) have repeatedly shown that such reliance on technology that carries the potential for mass surveillance is naïve and simply ignores the protection of the fundamental rights of all people.

The EU Commission counts on the high hit rate of automated systems to detect sexualized violence against children, but solely relies on information provided by the manufacturers.[5] This is a mistake, because independent data collection is needed so that manufacturers and providers cannot put their own interests first when passing on the data.

We also share the criticism, as formulated for example by EDRi[6], that the regulation wants to focus exclusively on the dissemination on the Internet, but not on the actual production of sexualized violent depictions of children. It also argues that the proposed measures are inadequate to combat dissemination. Among the sensible measures that the proposal outright ignores are a reninforcement of investigative capacities and adequate funding for institutions that actively work to protect children. In its current form, the draft even creates obstacles for investigators, as the enormous amounts of false reports that will inevitably result from the regulation could make it even more difficult to investigate the perpetrators.[7] Furthermore, it must be taken into account that the depictions of sexualized violence by organized groups are hardly disseminated through the channels controlled by this law.

Useful Methods:

- Hold providers accountable for tracking down, reporting and, above all, deleting the material and implementing protection concepts[8] transparently.
- Prevention and education: We focus on joint information for parents, children, and teachers/caregivers. By this we mean, among other things, the promotion of media literacy (e.g., to accompany children appropriately and in an age-appropriate manner when using the Internet,

[5] https://www.heise.de/news/Chatkontrolle-EU-Kommission-vertraut-bei-Trefferquote-auf-Meta-und-Hollywood-7286503.html
[6] https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf
[7] https://www.childrenrights.de/special/bibliothek/bibliothek-details/privacy-and-protection-a-childrens-rights-approach-to-encryption
[8] see Reform of the youth protection legislation in 2021: https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/reform-des-jugendschutzgesetzes-tritt-in-kraft-161184

to inform them about the risks of publishing data), media and sexual education for children, parents and teachers (e.g., training on sexualized violence), protection concepts in the digital space. [9]

- Strengthening the investigative authorities, e.g., it would be desirable for the Federal Ministry of the Interior to create structures that support the police in their investigative work and prosecution of crimes such as cyber-grooming across the board and that this is not the responsibility of the federal states alone. Among other things, there is a massive lack of trained staff who are also on the move and approachable online. A kind of online watchdog that children and young people can contact directly and where reports can be made easily, would presumably increase the likelihood that crimes such as cyber-grooming would be reported at all. It also includes spreading information by the security authorities: What counts as a crime online? How can I protect myself? How do I proceed as a victim, e.g., when it comes to securing evidence? [10]
- Close cooperation between the police and, for example, child protection organizations and youth welfare offices would be extremely important and useful.
- We also consider the planned EU center to be useful, but it is of particular importance not to use it to create a European central police authority controlled by INTERPOL/EUROPOL; the center must be independent:
    - the creation of an EU center as the central EU contact point to combat sexualized violence is an important step. Here, efforts must be coordinated, corporate actions monitored, material assessed and cataloged, and forwarded to national investigative authorities - which has so far been done largely in the US.
    - Important European institution, analogous to NCMEC (U.S.), that manages a database of imagery and forwards reports to INTERPOL/EUROPOL and national law enforcement agencies ("gatekeeper function" to weed out false positives).
    - Important institution in the support of victims, also to delete circulating material.
    - If necessary, technical and financial support for service providers who cannot afford their own forces for this purpose
- Training of the police
- Enable "quick freezes" or log-in traps to give investigating authorities time to check initial suspicions and, if necessary, access data to identify perpetrators.
- more visible police presence online ("patrols")
- more governmental hotlines, also online
- Increased efforts to prevent sexualized violence, i.e. increased vigilance/awareness in the social environment of children, suitable and widely available prevention offers for children, parents and pedagogical staff.
- Promotion of media literacy
    - Education regarding identification of grooming and how to deal with it
    - Education of children and adolescents regarding the punishability of sexting content.
- Education of children and adolescents in the area of crime "distribution, acquisition and possession of child and youth pornography" (§184b/c German penal code), in order to avoid

[9] More information: https://beauftragte-missbrauch.de/themen/schutz-und-praevention/schutz-im-digitalen-raum

[10] For instance, the German police offers a website for such information – such offers should be expanded: https://www.polizeifuerdich.de/

criminalization of children and adolescents, provided that no pedo-criminal intent can be determined.

We also draw attention to the provisions of the DSA, many of which are also suitable for preventing the dissemination of depictions of sexual violence and at least making cyber-grooming considerably more difficult. Before restricting constitutional rights, we would like to give the DSA a chance to take effect.

Private Communication Targeted by the Authorities

4. How do you assess the risk of innocent citizens coming under suspicion through false positive automated detection and what would be the impact of such false positives on both the suspects and the investigating authorities?

The number of false positives is relevant precisely because "innocent messages, chats and photos of innocent people with explicit content could end up on the investigators' screens and the people concerned could fall under suspicion." The EU Commission calculates that one in ten automated reports in machine searches of chat histories for cyber-grooming cases would reveal perfectly legal communications. This could quickly lead to millions of legal message exchanges being unfairly targeted by authorities. [11]

The files of depictions of sexualized violence against children (photos, videos) are located on computers (servers / filehosters) on the Internet. The fact that they are discovered is due to voluntary agreements. In the US, especially the companies of the Meta Group (Facebook, Instagram) scan their databases. They alone report more than 20 million discoveries per year. In Europe, filehosters also scan their servers and trigger notices - permission to do so is provided by an exemption in a data protection regulation, the EU Privacy Directive. Both the American and European companies report their finds to an American non-governmental organization called NCMEC (National Center for Missing and Exploited Children). Here the material is sighted and classified. Most of the material is already "known", but every year in Europe around 500,000 new images and videos are added - documents of current acts of violence. The NCMEC notifies the law enforcement agencies in the respective countries of the criminally relevant finds - including the IP address from which the files were loaded - in Germany, the Federal Bureau of Investigation (Bundeskriminalamt, short BKA). Approximately 80,000 such reports are received here each year. As a rule, the BKA can then use the IP address to track down not only the provider, but also the person who was active at that time with the reported address. Since providers are not obliged to keep this data, it is deleted as soon as it is no longer needed for internal reasons - usually within a week. After that, it is no longer possible to establish a connection between the IP address and its user. Although the NCMEC works very quickly, knowing the German data protection guidelines, procedures (albeit a minority at present) can no longer be followed for the above reasons.

The scanning and reporting processes described here are the only significant source for initiating investigative and subsequently criminal proceedings. Tips from the public account for less than two percent. If the online reports lead to criminal proceedings, the investigators usually find evidence of

[11] https://www.heise.de/news/Chatkontrolle-EU-Kommission-vertraut-bei-Trefferquote-auf-Meta-und-Hollywood-7286503.html

accomplices or entire networks. Doing without the automated scanning processes would make the investigators virtually blind.

We therefore advocate extending the exemption once again, implementing some proposals from the EU Commission and other stakeholders that we believe are uncontroversial, and analyzing the impact of these measures together with the DSA. Together with results of the research we hope to conduct, insights can then be gained, if necessary, as a basis for further legislation or new strategies.

Four more important points:

- The sheer volume of reports pushes the investigative authorities to their limits - the BKA, which sights everything and initiates proceedings; the police departments, which have to go out and act on the spot; and the judicial authorities.
- In Germany, almost half of the identified perpetrators are under 18 years old - they can be divided into three groups: One group has consensually made the recordings with children or has received them by children (sexting). The second group has been sent such material - for example, in a group chat - and it has been secured by the often activated automatic storage on the smartphone. By far the smallest group are minors who create, possess and/or distribute such images and videos for their own pedosexual inclinations or with the intention of selling them.
- Experts assume that the majority of these acts are not motivated by pedosexual inclinations, but are a substitute for the satisfaction of needs, especially for male perpetrators.
- In the so-called darknet, pedosexual groups are active with almost mafia-like structures; access is often bought through pictures and videos.

AI as Support, but not as Replacement

5. Hosting service providers and providers of interpersonal communication services that have received a discovery order shall, according to Article 10 CSAM-E, install and operate technologies that detect contact with children with intent to abuse ("grooming"). Are you aware of technologies that can reliably distinguish between harmless, sexually or romantically charged, communications and grooming?

In general, the question arises to what extent it would be possible to differentiate between harmless and sexualized communication purely on a technical level. Although a technology can learn to recognize patterns (machine learning), we doubt that perpetrator strategies can be detected in this way alone. In the fight against cyber-grooming, there are already numerous approaches in place that use AI-based text forensics. In the UK and Australia, an AI developed by linguists at Swansea University ("Dragon Spotter") has already been successfully used by the police to detect cyber-grooming. In Germany, as well as in numerous other countries around the world, police use Microsoft's PhotoDNA software, which is however not suitable for finding new material. Another globally known software called Safer is marketed by the NGO Thorn and used by companies such as Microsoft or Vimeo to report image and text material that suggests cyber-grooming to the authorities. What data sets these AIs are trained with, however, is not further known. [12] Technology can thus be used to support investigations rather than replace them.

Pattern analysis: WhatsApp as an example

[12] https://netzpolitik.org/2022/chatkontrolle-was-unternehmen-schon-freiwillig-tun/

On platforms used for communication (i.e.: also chats accompanying games), a similar procedure should be applied as already used for WhatsApp. This is currently done as follows: If a suspicious account contacts a number of other accounts, some of which report abuse, then a closer look is taken and investigated - i.e., on a warranted / issue-driven basis.

Here, it is particularly important that the reports are taken seriously quickly, and that investigations are not carried out only after countless reports have been made. On the one hand, this requires trained staff on the platforms, but it also requires trained investigative authorities to be able to respond to the cases accordingly.

Beyond the DSA regulations, we expect platform operators to be held more accountable. Especially in the area of monitoring interaction possibilities (chats, games, lootboxes, etc.), strict rules must apply analogous to the above-mentioned pattern analysis. In the case of platforms heavily frequented by children, behavior that points to adult users must also be identified and understood as a warning signal.

6. **Which technical approaches do you consider to be effective alternatives to the measures envisaged in the draft regulation that do not raise any fundamental rights concerns?**

Scanning of large public platforms (public content) using various tools (matching hashes, AI), which is already taking place as part of content moderation measures, is an appropriate tool to locate, review, and remove publicly posted material. The extension of the exemption allows this. We can also imagine an obligation. The new European Center would have to independently provide and update the necessary hashes and research the effect of scanning.

We believe that all the major platforms serving the advertising market are already quite good at predicting behavior (their profiling is also pattern analysis). The DSA obliges them to switch the offer to child friendly as soon as their own systems assume that they are dealing with a child user.

We also advocate that commercial/institutional online services provide an easily accessible explanation in plain language in addition to the imprint/general terms and conditions/privacy policy in order to explain the purpose and background of the presence to children and to offer advice and help.

Wherever providers offer discounted "family accounts," parents must enter the age information with their children - this should not be changeable (similar to dating services) and, if necessary, be read by apps for the age information.

Age verification

7. **The Commission's proposal includes a call for mandatory age verification. Where exactly and under what conditions would Internet users have to verify their age according to this proposal, and what technical approaches exist or are currently being researched to implement age verification in compliance with fundamental rights while preserving the anonymity of users on the Internet?**

In line with the General Comment No. 25 of the Children's Rights Committee, we call for age verification that works in both directions (hiding content from younger users; preventing older users from accessing content used by children). In this context, it is important to design this in accordance with fundamental

rights. The following are red lines though: Compulsory identification, the collection of biometric data, and interference with encrypted communication.

Large, user-centric and advertising-financed platforms in particular have long been able to identify children and young people as users. As stated in the DSA, in such cases (user is a child/underage) they should be obliged to automatically switch their service to an adapted, child-safe mode (youth-safe). (Reference DSA Recital 71 and Article 35 j))

We advocate that parents create smartphone accounts with their children and proceed correctly with the (voluntary) age declaration - which in some cases also has financial advantages for them. Important: This age information should not be changeable and can be used as a default (voluntary) option to indicate the age to other platforms (and apps). Chats and similar offers that complement platforms that are heavily used by children and young people or are created specifically for them should be set to child-friendly by default.

We recommend taking a look at the contact point for child and youth protection online net in Germany, the Commission for the Protection of Minors in the Media (Kommission Jugendmedienschutz, KJM), which among other things reviews and evaluates already existing age verification systems from a youth protection perspective. [13]

Privacy is a Fundamental Right

8. **The Commission's proposal would make it possible to require private communications services to issue discovery orders, among other things to obtain content from private and encrypted chats (including client side scanning), to detect grooming or to verify age; as a consequence of the technology-neutral approach, network blocking is also potentially conceivable. What would be the international consequences of such possibilities to analyze user behavior or to restrict access to online content and safe spaces - especially with regard to a higher risk of illegal intrusions (hacking) into the privacy of European citizens from abroad and with regard to authoritarian states using EU rules as a blueprint for illegitimate surveillance measures without constitutional containment?**

A “Chat control" would create a surveillance structure that could also be abused for other purposes. For example, the proposal also threatens certain professions that are bound to secrecy. Technology that enables censorship of certain content even before it is sent or uploaded endangers people living in (partly) authoritarian countries who are politically active, journalists or people in the LGBTIQ+ communities. This affects children as well, especially the most vulnerable children. We think it is problematic to base such a pilot project on the topic of children and encourage a broad debate about fighting crime and enforcing rights on the internet (and metaverse).

9. **Most recently, the Child Rights International Network underlined in a study the importance of "leaving behind the framing of privacy versus child protection in order to protect the rights of all children" (reported at netzpolitik.org 02.02.2023). How does the current EU Commission proposal relate to children and young people's right to privacy and secure IT systems, and what**

[13] See list of checked systems of age verification: https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/

would be the short-term and long-term consequences of the Commission proposal in this regard?

The security of private communications and personal data are also essential children's rights in their own right. But not only. The certainty of expressing opinions, attitudes and preferences freely and confidentially are the foundations of the democratization of children and young people. Anyone who infringes on this right - and in our opinion, the mere possibility of doing so is enough - weakens the development of future generations into democrats (see answer to question 1).

Potentials of the DSA

10. **In your opinion, which package of political measures is promising in order to take action against sexualized violence against children in an efficient, effective and fundamental rights compliant way – where do you see potential for improvement in the area of prevention and in the fight against sexualized violence and its presentation on the Internet?**

We are not aware of a holistically promising package of measures. However, there is legal potential that can be exploited before a new law, which would presumably be ruled contrary to fundamental rights before the European Court of Justice and would therefore be withdrawn, is passed, and thus years of work would have to start all over again.

Often left out of the discussion of the CSA-regulation is the possibility of extending the exemption from the ePrivacy Directive for the time being that the new law is intended to replace.

Basics:

1. the CSA-regulation proposal is prompted by the end of the exemption from the ePrivacy Directive, which currently allows providers to voluntarily scan unencrypted interpersonal communications. There is concern that without a permanent solution to succeed the exemption, a large number of child abuse depictions, and thus potential leads to perpetrators, will go undetected.
2. the Digital Services Act applies since November 2022 and will come into force in February 2024. This already contains a wide range of measures to ensure more child protection online. The extension of the ePrivacy exemption combined with strict enforcement of the DSA, making full use of the child protections it contains, already provides a solution to the issues raised by the Commission.

It should first be closely monitored whether the enforcement of the DSA in combination with an extension of the exemption and in combination with the implementation of individual further proposals, including the European center to become independent from NCMEC, has the desired effect on the problems mentioned before considering further, very profound measures.

Articles in the DSA to be highlighted in particular.

- Art. 7 - Voluntary investigations on own initiative and compliance with legislation.

- Art. 8 - No general obligation to monitor or actively investigate.

- 23 (Measures and protection against misuse)

- Recital 12

- Recital 71

- Article 28 Online protection of minors

- Article 34 - Risk assessment

- Article 35 - Risk mitigation

- Article 44 - Standards

The focus on prevention is enormously important from a child protection perspective.

All experts familiar with the topic are certain that the dark field of sexualized violence is immensely large. We know that perpetrators mainly come from the so-called social surroundings (family, relatives, friends, neighbors, clubs). Research into the dark area of sexualized violence (social proximity) must continue without losing sight of all forms of digital violence against children in order to improve prevention and intervention. This also includes questions of perpetrator development with regard to known theories on the matter and possible changes due to the immense digital availability of materials and representations of sexualized violence.

- What is the role of the Internet (images and videos in perpetrator development, chats in solicitation, messengers in engaging potential victims)? Research into the role of online components in the environment of the acts and the initiation must also be expanded for the above reasons.
- Analysis of the origin of new material (both digital and its original source - i.e., the location of the crime). Without reliable figures and structural knowledge, even far-reaching political measures will come to nothing.

Child protection associations have been calling for these preventive measures for years:

- Incorporating child protection topics with a digital component into the training of all relevant professional groups.
- Including online behavior in diagnostic interviews, for example in cases of eating disorders and identity problems.
- Prevention measures in daycare centers and schools with the active involvement of parents and children.
- Protection concepts mandatory in all associations and schools - constant monitoring and further development
- Prevention of cyber-grooming
- Youth media protection as a cross-sectional concern in all school subjects - especially in the subject lessons - of elementary schools.
- Technical protection - images that cannot be redistributed, blocking screenshots, preventing images from being downloaded => preventing redistribution.

We would like to point out that the BIK initiative (Better Internet for Kids) of the EU Commission contains many such approaches. [14]

[14] See “A European strategy for a better internet for kids (BIK+)” https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids

11. Does the European Commission's proposal cover all platforms on the Internet on which child pornography material can be disseminated in a targeted manner, or in what way might there be a need for improvements with regard to the scope of application?

The means of dissemination are very likely to be more diverse and used more flexibly than we might imagine. As an example: We assume that there is close interaction and a lot of exchange between the darknet and the open Internet, which can be broken through police work (internationally) and consistent deletion. That would also be something to look at politically.

The EU Center

12. Have instruments for better law enforcement and prosecution been sufficiently assessed in the EU Commission's proposal, where might there be a need for improvement, and what instruments would be necessary to achieve this?

This requires a legal assessment that can holistically evaluate both the EU level and the state and country-specific criminal law rules in this context. Basically, instruments are needed that provide the investigating authorities with sufficient staff, as well as psychological and technical resources for processing such materials in the area of sexualized violence, in order to be able to work effectively with the sheer mass of materials, perpetrator networks, etc.

Despite its distance to Europol, the new center would be well suited to measure and communicate the success and failure of different investigative approaches and to derive international strategies from them.

Redundancies are to be avoided.

13. Will the new EU center be able to adequately support national law enforcement agencies and Europol, according to current plans, and which equipment would it need to do so?

Until it is clarified which final authorities this center will encompass, we cannot answer this question.

In principle, the creation of a European version of the "National Center of Missing and Exploited Children" is very welcome. However, a close coupling, of any kind, to Europol should be rejected. This EU center should be completely independent of Europol, both financially and locally. It must ensure close cooperation with child protection organizations and hotlines. Further responsibilities should be the management of the hash database with already known material as well as the research of trends in the field of dissemination or similar.

However, cooperation with national investigators is also necessary. We do not consider the center as part of the police work, but it evaluates and shares experiences - certainly also with technical support tools and methods of national cooperation and legislation.

It would also be helpful to support small and medium-sized providers both financially and with know-how and concrete (software) solutions to make their offers and services childproof and to detect suspicious material.

In addition: See answer to question 3

Child Friendly Technologies by default

14. In your view, does the EU Commission's proposal include all technical approaches that can be used to achieve the goal of protecting children, and what other technical approaches would be necessary in your view?

The current technical approaches in the draft are not sufficient. In order to gain better insight into technical options that comply with data protection and safeguard fundamental rights, research and education are needed at this point.

Already effective and promising approaches include server-side scanning of public platforms. Already taking place as part of content moderation measures, scanning of large public platforms (public content) using a variety of tools (matching hashes, AI) is a suitable tool to locate, review, and remove publicly posted material. On the other hand, the so-called log-in trap[15] as well as "Quickfreeze" [16] are suitable to consistently delete extreme material, which often originates in the Darknet, to stop the cycle of copying and preparing such material. In order to identify perpetrators, we advocate, among other things, the use of the so-called log-in trap, in which the identity of users is recorded on an ad hoc basis. Alternatively, we advocate the storage of address data for a limited period of time and to a limited extent (quick freeze) in order to give investigators a reliable chance. This requires a corresponding legal basis and significantly improved human resources at law enforcement agencies. Appropriate technologies for the digital preservation of evidence must also be made available. The basic principle for technical measures to preserve evidence must be to exclude encrypted communication from it.

Pattern analysis using the example of WhatApp (see answer to question 5).

Child-friendly design and mandatory notices to children including consulting services and assistance

In addition to the technical possibilities of deleting video and image material depicting sexualized violence against children and identifying the perpetrators, a child-friendly design of websites and apps is desirable in principle (in line with General Comment 25 of the UNCRC).

On the one hand, websites could be required to provide child-friendly information (in plain language) about what is shown on the website and what the website is for, in addition to the terms and conditions, data protection and imprint. This information can also help parents to better assess what their children are confronted with. Second, platforms that are primarily used by minors should offer low-threshold reporting, redress and complaint mechanisms (see recital 89 DSA). This includes making it clear to minors who they can turn to should they feel unsafe. This could be, for example, a chat that is staffed 24 hours a day by qualified personnel. Their availability and competence could be ensured by child protection organizations.

In addition, it should be made clear in an easily understandable way which offers of help are suitable for the respective situation (situation-based services) (central national office that ensures allocation to aid

[15] Further Information about Login traps- https://d-64.org/login-falle/
[16] Further Informationen about Quickfreeze: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/22_QuickFreezeStattVorratsdatenspeicherung.html-Quickfreeze

organizations).[17]

15. **The draft regulation also provides for the possibility of network blocking of individual URLs, which is even to be extended in the course of the draft amendments made so far during the Czech Council Presidency. In view of the widespread use of https encryption for URL retrievals, do you consider it technically possible to block individual URLs in a targeted manner without resorting to blocking entire domains, if so, in what way should this be possible, and if not, can network blocking in this way satisfy the requirements of the European Court of Justice regarding the targeting of network blocks?**

Blocking is at best a last resort - we believe that technically skilled users can circumvent it. It would be better to delete the material. We would talk about having Internet access facilities delivered in a child-safe version by default and tying this to age ratings for content and interaction options. This would save parents having to deal with parental control software and installing it on different devices.

The EU Center II

16. **How do you assess the role and character of the EU center planned according to the EU draft regulation, on the one hand, with regard to the performance of primarily preventive tasks and, on the other hand, with regard to tasks concerning the development and use of technical monitoring tools?**

We don't see the framing for prevention at the EU center; but the provision of information, research results and findings for the development of prevention offers are welcome. There must be a close coordination of the different aspects of the fight against sexualized violence anyway (and not only be focused on the fight against the dissemination of depictions of sexualized violence). We see the EU center strongly focused on

- The detection and deletion of the material,
- the fight against dissemination,
- assisting (intelligence, technology, funding) in identifying the perpetrators and gathering and securing evidence,
- the fight against attempts to prepare new acts digitally, which are connected to cyber-grooming
- Helping to improve preventive services, but also to provide better support for those affected.
- Assistance with legal frameworks

17. **If it were not the end devices that were searched, but the communications ("chats") possible with them, this would also apply to end-to-end encryption of messenger services, for example. Here, too, countless law-abiding citizens would be targeted by the authorities simply because they use a certain service with the appropriate software. Are you aware of software solutions that allow real-time reading or at least cracking of end-to-end encrypted communications? Do**

[17] More background information see this paper (especially page 7):
https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf

you think it is justifiable to abolish the confidential private communication guaranteed by the Basic Law by means of algorithms?

Currently, we are not aware of any such technologies.

As already stated several times: We do not consider it justifiable to use algorithms to override end-to-end encryption in guaranteed confidential private communications. Unprovoked scans of encrypted communications are disproportionate and do not achieve their goals. The right to privacy is a fundamental right of all people, including children. On the subject of privacy, see the answer to question 1.

The so-called "chat control" is not expedient in the view of the Child Protection Association. We consider the scanning of communications to be a disproportionately large intrusion into the privacy of citizens - and especially children - that does not comply with the required balancing of different fundamental rights.

18. **The draft regulation states that the Center for Child Sexual Abuse in The Hague, which is to be established, is to provide binding indicators for images of sexual abuse that are to be used by the scanning companies. Experienced investigators know that it is by no means possible to clearly define and prove in each individual case on the basis of which criteria what is to be regarded as a family photo, as self-documented play among children and young people, as a random snapshot of a sporting event, or even as child pornography. Are there any findings about the methodological approach of the EU center mentioned above? And if so, can this procedure be assessed as reliable and suitable?**

Before the EU center is even established, we can hardly judge the methodological approach.

At this point, we can once again emphasize that a purely technical solution that relies on the reliability of an AI is not expedient, because the error susceptibility is too high and especially for such distinctions, a professionally competent assessment by trained staff is always required. See also the answer to question 5.

Investigators tell us, however, that new material can usually be found where old material has been discovered. AI can be trained to scan to the same extent as before and thus help to find suspicious new material. The EU Center can also help to identify the best methods (and programs) for each case manufacturer-independently.

Berlin, 27.02.2023

Der Kinderschutzbund Bundesverband e.V.
Schöneberger Str. 15
10963 Berlin
Tel (030) 21 48 09-0
Fax (030) 21 48 09-99
E-Mail info@kinderschutzbund.de
www.kinderschutzbund.de

The German Child Protection League (DKSB) - For the future of all children!

The Child Protection Association, founded in 1953, is Germany's largest child protection organization with 50,000 members in over 400 local associations. The DKSB campaigns for the interests of children as well as for changes in politics and society. Its work focuses on children's rights, children in poverty, violence against children, and children and the media.