The German Society for the Protection of Children

Federal Association

Statement from the German Society for the Protection of Children for the public hearing held by the German Bundestag's Committee on Digital Affairs on the subject of "chat control" on Wednesday, 1 March 2023, from 14.00 to 16.00 hrs.

The German Society for the Protection of Children

The German Society for the Protection of Children (DKSB) is an advocate for the rights of all children and young people in Germany. It wants to see a child-friendly society in which the mental, spiritual, social and physical development of children and young people is supported. Children and young people should be involved in all decisions, plans and measures affecting them. The German Society for the Protection of Children intervenes for the benefit of children and young people – in legislation at federal and *Land* (state) level, and in planning and decision-making in our towns, cities and communities. It calls for an improvement in the material living conditions of children and families, a child-friendly and healthy environment, and good facilities for children and young people. It also looks at the digital environment in this context, in line with general comment no. 25 adopted by the UN Committee on the Rights of the Child. Further information on the goals of the German Society for the Protection of Children can be found in our mission statement, our supplementary digital mission statement, and our programme for children's policy.

The German Society for the Protection of Children thanks the Committee for giving us the opportunity to set out our view on these issues. You will find our answers below to questions 1 to 18 from the list of questions.

The draft Regulation and its implications

1. The European Commission's proposal for a CSA Regulation, also known as the "chat control" proposal, has been the subject of a great deal of discussion since its publication in May 2022. Please explain the technical, legal, fundamental-rights, data-protection, social and/or societal implications of the proposal.

The EU initiative sends a clear signal to all EU countries to take stronger action to combat sexual violence against children. We very much welcome this. A great deal of the proposal reflects the positions supported by the German Society for the Protection of Children. The core elements of the European Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse (CSAR) focus on child protection online. The aim is to combat the production and digital dissemination of child sexual abuse material, and thus the abuse itself. To achieve this commendable aim, the Regulation proposes necessary and appropriate measures, but there are key areas where it goes too far. In particular, scanning private communications in messaging services (such as WhatsApp or Signal) or emails without a reasonable suspicion of wrongdoing is neither proportionate nor helpful. It represents a far-reaching interference in the fundamental rights of children and young people; their ability to grow up in an environment where freedom of expression and confidential communication are a given is a cornerstone of democracy and participation. We are also concerned that general scanning will result in children and young people being criminalised much more frequently – a trend which is already visible in Germany's criminal statistics today. This is due to the

fact that children and young people themselves often send visual material which is categorised as pornographic, thus opening themselves up to prosecution.

In this debate, privacy and child protection are often played off against each other – an approach which fails to do justice to this subject. Children's rights require both: the right to physical integrity, but also the right to secure communication. An attack on encrypted personal messages, without a reasonable suspicion of wrongdoing, overrides an important constitutional right and multiple children's rights which enjoy constitutional status in the EU. They are pillars of our democracy – guaranteeing them shapes how young people grow up in a free, democratic society.

The right to privacy, in particular, but also the right to freedom of expression, the right to information, and protection from violence, are essential for children's development. Knowing that they are not being constantly monitored is the only way children can develop the necessary trust in their parents or guardians, teachers and friends which helps to ensure that they seek help from people they trust when they need it, and gather information about certain topics without having to worry about the consequences of doing so. This is particularly relevant for children and young people who face discrimination because of their sexual or gender identity, a disability, their origin or skin colour, or other characteristics, as they face specific risks online.[1]

Useful measures to protect children's rights online

There are a number of measures in the proposal which we regard as useful, such as effective age verification (but without an obligation to provide proof of identity or the collection of biometric data), security requirements, and the obligation for providers to perform risk assessments – both hosting providers and providers of platforms, such as those collectively known as social media. They are supposed to protect their systems from being used for the purpose of the supply, storage or sharing of child sexual abuse material. The same applies to cyber-grooming – we too are calling for requirements such as high-quality, sensitive moderation of chats, age verification (subject to the limits set out above), and pattern analysis, so that groomers can be detected and subsequently blocked and/or reported. There should also be low-threshold reporting processes for children and young people who need help, with easy-to-understand descriptions of the assistance that is available and professional services. The scanning of visual material on the servers of platforms and file-hosting services currently takes place on a voluntary basis, and we support the plan to make this mandatory – in the case of both known material (hashes) and new material (AI support). We also endorse the establishment of a central agency which, like NCMEC, collects data, develops strategies, supports new technical processes, and monitors companies' compliance while also assisting them in performing risk assessments. In our view, this institution must be independent (especially of Europol) and work closely with child protection organisations.

The key element we do not support in the Commission's proposal is the detection order, also known as "chat control". This would establish an administrative and legal process which would allow the communications of a provider's entire customer base to be scanned for weeks or even months. It applies to companies who fail to meet their risk mitigation obligations, where a "significant risk" exists. This surveillance of communications without a reasonable suspicion of wrongdoing represents a far-reaching interference in the fundamental right of freedom of communication, which is a key element in freedom of expression and an important children's right. We are concerned that the mere existence of this option will have an impact on the behaviour of children and young people. "Chat control" runs counter to efforts to balance fundamental rights and weigh competing interests. Investigators and AI experts are also critical of these aspects of the proposal.

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

Irrespective of these concerns, we would like to draw attention to the fact that, from a legal perspective, the situation is being turned on its head and the wrong people are being held to account. If service providers fail to comply with the requirements, it is their customers whose rights are restricted (imagine a similar scenario under the Money Laundering Act – it is the equivalent of banks acting negligently, and this resulting in the accounts of all their customers being monitored).

One of our key demands is for greater investment in research. Facts, data and figures are needed to establish a solid basis for the wider discussion. For example, the figures relating to successful investigations apply only to the field of reported and recorded crime. Yet there is a much larger "dark field" of unreported and unrecorded crime, and so we are calling for it to be researched as well.

- The impact of digitally available material and chats on the "dark field" of unreported and unrecorded crime, and on perpetrators and crimes in the victim's close social environment (interaction)
- Cyber-grooming – research into these cases, verification of the resulting crimes / real-world encounters / weaknesses in chats and chat moderation / perpetrators' modus operandi
- How online material, chats and communities are connected to and interact with real-world crimes
- Profile of perpetrators: the abuse of power between paedophilia and offences committed as "surrogate actions"
- Does David Finkelhor's theory of grooming (four-factor model)[2] also apply in the digital environment?
- Offences committed in the victim's close social environment, in families, neighbourhoods, friendship groups, clubs, etc., and the resulting digital actions
- Where does new material come from and how can it be reliably detected?
- New technical options for risk mitigation – a responsibility for the new EU agency

The urgency of the aim of this draft legislation to combat sexual violence against children is not in question. As we have set out here, however, we have serious doubts about the effectiveness of the proposed measures in their current form. In this context, we draw attention again to the UN Convention on the Rights of the Child and general comment no. 25 (on children's rights in the digital environment), which has equivalent status to a federal law. Children's participation and development must be given the same weight as child protection when formulating legislative measures.

Cyber-grooming

2. The Commission's proposal provides for the issuance of detection orders requiring providers of communications services or devices to covertly access information if it is suspected that abuse material is being shared via these services or devices or that grooming is taking place on them. In your view, what services and devices are potentially affected by this and to what extent, and what effects will this have on their users?

The latest cyber-grooming study, published by the Media Authority of North Rhine-Westphalia[3] in 2022, has shown that cyber-grooming is increasingly taking place on Instagram, TikTok, WhatsApp and gaming platforms. Ultimately, it can take place anywhere where contact options exist. Services frequently used by children and young people are of particular interest 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

[2] See Finkelhor 1984

[3] 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

Minecraft. To circumvent the platforms' safeguards, perpetrators often try to switch to more private communication channels after the initial contact, for example to messaging services such as WhatsApp or video chat services.[4] These are, in other words, platforms with a very wide reach, used by millions of users every day.

Abuse material is often shared on public platforms – firstly to make the material easily accessible and draw in people who are interested in it, and secondly because material provided by "newcomers" can be found on large platforms. Some perpetrators are more professional in their approach, creating an account (e.g. on TikTok or a similar service), making it private and adding abuse material to it, then sending out the access details. The best way to detect abuse material offered in closed groups, for example, including on the dark web, would be for investigators to be empowered to "patrol" online more frequently. The legal framework for this already exists (e.g. the supply of artificially generated material in order to gain access).

The effects on users are serious. Victims of digital violence (e.g. cyber-bullying, cyber-grooming, hate speech) often leave online platforms.[5] In other words, their fundamental rights are restricted, such as their right to participation, access, freedom of information and freedom of expression, and their right to privacy. In addition, we now know that digital violence has just as devastating impacts on mental health as all other forms of violence. Victims often do not seek help because they are embarrassed or do not trust other people (or the authorities) enough to seek appropriate support.

Technology alone does not offer protection from abuse

3. Why, in your opinion, is the Commission's proposal fit for purpose or not fit for purpose when it comes to protecting children effectively from (sexual) abuse and the dissemination of abuse material, and where do you believe concrete action is needed?

The proposal in its current form not only raises constitutional issues, but also falls short in terms of the technical implementation. The focus on a technical solution is too one-sided and ignores the fact that this is a problem for society as a whole. Relying solely on technical solutions to protect children from sexual violence online is a fatal error with devastating consequences for the fundamental democratic rights of all people, especially children. Experts from a range of fields (IT, data protection, human rights, lawyers, etc.) have repeatedly shown that this kind of faith in technology, which has the potential to develop into mass surveillance, is naïve and simply ignores the importance of respecting the fundamental rights of all people.

The European Commission is basing its approach on the high accuracy rate of automated systems to detect sexual violence against children, but it is relying on the claims made by the vendors of these systems.[6] This is a mistake, because independent data is needed to ensure that the data offered by vendors and providers is not coloured by their own interests.

[4] See https://www.klicksafe.de/cybergrooming

[5] Girls and young women, especially those exposed to multiple discrimination, are particularly affected by digital violence. The study on digital violence against girls and young women published by Plan International in 2020 (the State of the World's Girls report) highlights that victims leave 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

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

We also share the criticism voiced by EDRi[7], for example, that the Regulation focuses solely on the dissemination of child sexual abuse material online, and not on the actual production of this material. EDRi argues that the proposed measures are also unsuited to combating dissemination. Useful measures which are completely disregarded by the proposal include investigative capacity building and the provision of adequate resources for institutions that actively work to protect children. In its current form, the proposal actually creates obstacles for investigators, as the enormous number of false reports that would inevitably result from the Regulation could make it even harder to investigate perpetrators.[8] Furthermore, it must be kept in mind that organised groups generally do not disseminate sexual abuse material via the methods that would be monitored as a result of this legislation.

Useful measures:

- Requiring providers to detect, report, and above all to delete material, and to transparently implement protection strategies[9]
- Prevention and education: Our approach here is based on joint information for parents, children, and teachers/carers. By that we mean, for example, support for media literacy (e.g. to support children in a suitable and age-appropriate way as they use the internet, and to provide information about the risks of disclosing information), media and sex education for children, parents and teachers (e.g. training on sexual violence), and protection strategies in the digital environment[10]
- Strengthening the investigating authorities: for example, the Federal Ministry of the Interior should ideally create structures to provide nationwide support to the police in the investigation and prosecution of criminal offences such as cyber-grooming, rather than this being the sole responsibility of the *Länder* (federal states). Among other things, there is a massive shortage of trained personnel who are also present and contactable online. A kind of online police station which children and young people can contact directly and which offers a low-threshold means of filing a complaint would probably increase the likelihood that offences such as cyber-grooming are even reported to the police. Education efforts by law enforcement agencies are also an important aspect: what counts as an offence online? How can I protect myself? What should I do, as a victim, when it comes to securing evidence, for example?[11]
- Close cooperation between the police and, for example, child protection organisations and youth welfare offices would be incredibly important and useful
- We also believe the plan to establish an EU Centre makes sense, but crucially this must not result in the creation of a central European police authority controlled by INTERPOL/EUROPOL; the Centre must be independent:
    - The creation of an EU Centre as a central EU point of contact to combat sexual violence is an important step. The Centre must coordinate efforts, oversee the measures taken by companies, inspect and catalogue the material and forward it to

[7] https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR.pdf
[8] https://www.childrenrights.de/special/bibliothek/bibliothek-details/privacy-and-protection-a-childrens-rights-approach-to-encryption
[9] See the 2021 reform of the Protection of Young Persons Act (*Jugendschutzgesetz*): https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/reform-des-jugendschutzgesetzes-tritt-in-kraft-161184
[10] Information about this is available from the Independent Commissioner for Child Sexual Abuse Issues, for example: https://beauftragte-missbrauch.de/themen/schutz-und-praevention/schutz-im-digitalen-raum
[11] There is an information and education website run by the police, for example, and this kind of service should be expanded: https://www.polizeifuerdich.de/

the national investigating authorities – a process which currently takes place mainly in the United States
    - The Centre should be an important European institution, along similar lines to NCMEC (United States), which maintains a database of visual material and forwards reports to INTERPOL/EUROPOL and national law enforcement agencies (playing a "gatekeeper" role to filter out false positives)
    - The Centre should be an important institution when it comes to supporting victims, including with regard to deleting material that is in circulation
    - It should potentially offer technical and financial support to service providers who do not have adequate resources to deal with this issue
- Training for the police
- Facilitating a "quick freeze" process and/or log-in traps to give the investigating authorities time to examine whether an initial suspicion of wrongdoing exists and, if so, to enable them to access data to identify perpetrators
- A more visible police presence online ("patrolling")
- More public reporting points, including online
- Greater efforts to prevent sexual violence, i.e. increased vigilance/awareness-raising in children's close social environment, and appropriate and widely available prevention services for children, parents and teaching staff
- Support for media literacy
    - Educating people about how to identify and deal with grooming
    - Educating children and young people about the criminality of sexting content
- Educating children and young people about the subject of the "dissemination, procurement and possession of child and youth pornographic content" (section 184b/c of the Criminal Code (*Strafgesetzbuch*)), in order to avoid criminalising children and young people in cases where no paedophiliac criminal intentions are found to exist.

We also wish to draw attention to the provisions of the Digital Services Act (DSA), many of which also seek to prevent the dissemination of sexual abuse material and to at least make cyber-grooming much more difficult. Before constitutional rights are restricted, we would like to give the DSA a chance to have an effect.

Private communication in the sights of the authorities

4. How great is the risk, in your view, of innocent members of the public coming under suspicion due to false positives produced by automated detection, and what would the impact of such false positives be for both the suspects and the investigating authorities?

The number of false positives is so important because "harmless messages, chats and photos containing explicit content which belong to innocent people could end up on investigators' screens and those affected could come under suspicion". The European Commission expects that one in ten automatic reports generated by automated searches of chats for cyber-grooming cases would be a completely legal communication. This could quickly lead to millions of legal message exchanges wrongly ending up in the sights of the authorities.[12]

The files containing depictions of sexual violence against children (photos, videos) are stored on computers (servers / file-hosting services) online. Their detection is based on voluntary agreements. In the United States, the companies in the Meta group (Facebook, Instagram), in particular, scan their

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

files. These companies alone make more than 20 million reports per year. In Europe, too, file-hosting services scan their servers and make reports – they are allowed to do so on the basis of a derogation from the ePrivacy Directive. Both American and European companies report the material they find to an American NGO called NCMEC (the National Center for Missing and Exploited Children). NCMEC inspects and categorises the material. In most cases, it consists of "known" material, but each year around 500,000 new images and videos appear in Europe – documents depicting current abuse. NCMEC passes on criminally relevant material to the law enforcement agencies in the countries concerned – including the IP address from which the files were uploaded. In Germany, the relevant law enforcement agency is the Federal Criminal Police Office, which receives around 80,000 such reports each year. The Federal Criminal Police Office can usually use the IP address to identify not only the provider, but also the person who was active with the reported IP address at that time. As providers are not required to retain this data, it is erased as soon as it is no longer needed for internal reasons – usually within a week. After that, it is no longer possible to attribute the IP address to the user. NCMEC is aware of Germany's data protection rules and thus works very quickly, but sometimes investigations can no longer be conducted for this reason (although currently this happens only in a minority of cases).

The scanning and reporting processes outlined here are the only significant source of information leading to investigations and subsequently prosecutions. Information provided by the public accounts for less than two per cent of reports. If online reports lead to criminal proceedings, investigators usually also find information about co-offenders or entire networks. Without automated scanning, the investigators would be all but blind.

We are therefore calling for a further extension of the derogation, for the implementation of some proposals made by the European Commission and other stakeholders which we view as uncontentious, and for an analysis of what impact these measures have in combination with the DSA. Together with the results of the research that we hope will be carried out, this may produce findings which can form the basis for further legislation or new strategies.

There are four more important points we would like to make:

- The sheer volume of reports is pushing the investigating authorities to their limits – the Federal Criminal Police Office, which inspects them all and launches investigations; the police, who are dispatched and have to take action on the spot; and the judicial authorities.
- In Germany, just under half of identified perpetrators are under the age of 18. They fall into three groups: one group consists of minors who have taken photos consensually with children or have been sent photos by children (sexting). The second group consists of minors who have been sent such material – for example in a group chat – and it has been saved on their smartphone by the automatic saving feature that is often activated. By far the smallest group consists of minors who produce, possess and/or disseminate such images and videos due to their own paedophiliac inclinations, or with the intention of selling the material.
- Experts assume that a large proportion of offences are committed not because of paedophiliac inclinations, but rather as a "surrogate action" mainly by male perpetrators to satisfy their needs.[13]
- Paedophile groups with almost mafia-like structures are active on the dark web; people often buy their way in by supplying images and videos.

[13] For a definition of sexual violence against children, see Deegener, Professor Günther: *Kindesmissbrauch. Erkennen – helfen – vorbeugen*. Weinheim 2010, p. 22

AI: a source of support, not a substitute

5. According to Article 10 of the draft CSAM Regulation, providers of hosting services and providers of interpersonal communications services that have received a detection order are to install and operate technologies to detect the solicitation of children with abusive intentions ("grooming"). Are you aware of technologies that can reliably distinguish between unobjectionable sexual or romantic communication and grooming?

In principle, the question is to what extent a distinction can be made between unobjectionable and sexual communication by technical means alone. Technology can learn to recognise patterns (machine learning), but we doubt that perpetrators' strategies can be detected in this way alone. In the fight against cyber-grooming, there are already many approaches which use AI-based text forensics. In the UK and Australia, an AI tool ("Dragon Spotter") developed by language researchers at Swansea University has already been successfully used by the police to detect cyber-grooming. In Germany and in many other countries around the world, the police use the Microsoft software "PhotoDNA"; however, this is not designed to detect new material. Another piece of software known worldwide, "Safer", is marketed by the NGO Thorn and is used by companies such as Microsoft or Vimeo to report visual and text material that appears to be cyber-grooming to the authorities. That said, it is unclear what data is used to train these AIs.[14] In other words, technology cannot be used as a substitute for investigations, only to support them.

Pattern analysis: the example of WhatsApp

Platforms which are used for communication (including, for example, chat features attached to games) should adopt a similar approach to that which is already being used for WhatsApp. The process is currently as follows: if a suspicious account contacts a number of other accounts, some of which report misuse, this account is looked at more closely and investigated – in other words, when there is a reasonable suspicion of wrongdoing.

In this context, it is particularly important for reports to quickly be taken seriously, rather than investigations being launched only after large numbers of reports have been received. This requires trained staff working for the platforms, but also trained investigating authorities, so that cases can be handled properly.

Going beyond the DSA provisions, we expect platform operators to be made to take more responsibility. Particularly when it comes to monitoring opportunities for interaction (chats, games, loot boxes, etc.), strict rules must apply, similar to those for pattern analysis set out above. In the case of services which are heavily used by children, behaviour indicating that a user is an adult must also be identified and seen as a warning sign.

6. What technical approaches do you believe offer effective, rights-compliant alternatives to the measures set out in the draft Regulation?

The scanning already performed by large public platforms (public content) as part of their content moderation measures, using various tools (hash comparison, AI), is a suitable tool to detect, review and remove publicly posted material. Extending the derogation allows this to take place. We could also envisage making such measures mandatory. The new European Centre ought to independently provide and update the necessary hashes and study the impact of scanning.

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

In our view, all large platforms which serve the advertising market are capable of predicting behaviour very accurately (their profiling is also a form of pattern analysis). The DSA requires them to make their service child-appropriate as soon as their own systems suggest that the user is a child.

We are also calling for online commercial/institutional services to provide, in addition to their legal notice / terms and conditions / privacy notice, an easy-to-find explanation for children which sets out, in simple language, the purpose and background of the website and offers them advice and help.

Wherever providers offer "family accounts" at a reduced price, information about users' ages should be entered by the parents together with their children. It should not be possible to subsequently change this information (similarly to dating sites and apps), and apps should potentially be able to draw on this age information.

Age verification

7. The Commission's proposal includes a call for mandatory age verification. Where exactly, and in what circumstances, would internet users have to verify their age under this proposal, and what technical options exist or are currently being explored to implement age verification in a rights-compliant manner that preserves the anonymity of users online?

In line with general comment no. 25 adopted by the UN Committee on the Rights of the Child, we are calling for age verification which applies in both directions (hiding content from younger audiences; keeping older people from accessing services used by children). It is important for this to be designed in a rights-compliant manner. The following points are red lines: any requirement to provide proof of identity, any collection of biometric data, and any interference in encrypted communication.

Large, heavily user-centric platforms funded by advertising, in particular, have long been capable of detecting that users are children or young people. As the DSA states, they should be required in such cases (where the user is a child/minor) to automatically switch their service to an adapted, child-safe (or minor-safe) mode (recital 71 and Article 35 j) of the DSA).

We are calling for parents to set up smartphone accounts together with their children and to (voluntarily) provide accurate age information – which in some cases also has financial benefits. An important point is that it should not be possible to subsequently change this age information, and this information can (voluntarily) be used as the default option when providing information about the user's age to other platforms (and apps). Chats and similar services which are part of platforms used heavily by or created specifically for children and young people should be set to be child-appropriate by default.

We recommend looking at the work carried out by the contact point for the protection of children and young people online in Germany, the Commission for the Protection of Minors in the Media (KJM); for example, it reviews and assesses existing age verification systems from a youth protection perspective.[15]

Privacy is a fundamental right

8. The Commission's proposal would make it possible for private communications services to be required to comply with detection orders, including to obtain content from private and encrypted chats (for example through client-side scanning) to detect grooming or for the purpose of age

[15] See the list of age verification systems which have been reviewed: https://www.kjm-online.de/aufsicht/technischer-jugendmedienschutz/unzulaessige-angebote/altersverifikationssysteme/

verification; the technology-neutral approach means that access blocking is potentially also conceivable. What would the international consequences be of such means of analysing user behaviour or restricting access to online content and safe spaces – especially regarding the higher risk of illegal foreign encroachments on European citizens' privacy (hacking), and regarding authoritarian regimes' use of the EU rules as a blueprint for illegitimate surveillance measures that are not constrained by the rule of law?

"Chat control" would create a surveillance structure which could also be misused for other purposes. The proposal also poses a risk to certain professional groups which are bound by confidentiality, for example. Technology which allows the censorship of certain content before it is even sent or uploaded poses a particular risk to people living in (semi-)authoritarian countries who are politically active, journalists, or people in LGBTIQ+ communities. This also affects children, especially children who are particularly vulnerable. We regard it as problematic to carry out this kind of pilot project in relation to children, and suggest that a broad debate should take place about combating crime and enforcing rights online (and in the metaverse).

9. The Child Rights International Network recently underlined in a study the importance of "mov[ing] beyond a privacy versus protection framing if we are to ensure that all children's rights are protected". What approach does the European Commission's current proposal take to the right of children and young people to privacy and secure IT systems, and what short-term and long-term consequences would the Commission's proposal have in this context?

The security of private communication and personal data is, in itself, also an important children's right. But that is not all. The certainty that opinions, attitudes and preferences can be expressed freely and confidentially is the foundation for raising children and young people to be democrats. Anyone who interferes with this right – and in our view, the very existence of such an option would do so – is undermining the development of future generations into democrats (please see our answer to question 1).

Potential of the Digital Services Act

10. In your view, what package of political measures would, taken together, offer a promising approach to tackling sexual violence against children in an effective and rights-compliant manner? Where is there potential for adjustments and improvements in the field of prevention and in tackling sexual violence and online material depicting it?

We are not aware of a package of measures which, taken together, offers a promising approach. However, full use should be made of the potential offered by existing legislation before new legislation is adopted which the European Court of Justice would probably find to be contrary to fundamental rights. If this happened and the legislation were withdrawn, years of work would have to be started again from scratch.

In the discussion about the CSA Regulation, the possibility of initially extending the derogation from the ePrivacy Directive, which the new legislation is meant to replace, is often ignored.

Reasoning:

1. One reason for the proposal for a CSA Regulation is the expiry of the derogation from the ePrivacy Directive, which currently allows providers to voluntarily scan unencrypted interpersonal communications. There are concerns that, without a permanent solution as a successor to the derogation, a large quantity of child abuse material and thus potentially clues to perpetrators might not be detected.

2. Parts of the Digital Services Act have applied since November 2022, and the Act as a whole will enter into force in February 2024. It already contains a wide range of measures to ensure greater child safety online. The extension of the derogation from the ePrivacy Directive in combination with greater enforcement of the DSA, with full use of the safeguards for children it contains, already offers a solution to the problems raised by the Commission.

We should first observe closely whether the enforcement of the DSA, together with an extension of the derogation and the implementation of some other proposals – which should definitely include the European Centre, in order to become independent of NCMEC – has the desired effect on the specified problems, before further, very far-reaching measures are considered.

Particularly relevant articles of the DSA

- Article 7 – Voluntary own-initiative investigations and legal compliance
- Article 8 – No general monitoring or active fact-finding obligations
- Article 23 – Measures and protection against misuse
- Recital 12
- Recital 71
- Article 28 – Online protection of minors
- Article 34 – Risk assessment
- Article 35 – Mitigation of risks
- Article 44 – Standards

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

All experts familiar with the issue are sure that there is a huge "dark field" of unreported and unrecorded sexual violence. We know that perpetrators mainly come from the victim's close social environment (family, relatives, friends, neighbours, clubs). Further research into the "dark field" of unreported and unrecorded sexual violence (in the close social environment) must continue, without losing sight of all the forms which digital violence against children takes, in order to improve prevention and intervention. This includes research into questions about how people become perpetrators, with regard to established theories on this subject, and possible changes caused by the vast digital availability of material and depictions of sexual violence.

- What role does the internet play (what role do images and videos play in people's development into perpetrators, what role do chats play in grooming, what role do messaging services play in establishing links with potential victims)? Research into the role of online components in the context of offending and grooming must also be expanded for the above reasons.
- The origin of new material (both in digital terms and its original source – i.e. the place where the offence was committed) must be analysed. Without reliable figures and structural knowledge, even far-reaching political measures will not achieve anything.

Child protection organisations have been calling for the following preventive measures for years:

- Cover child protection issues, including digital components, in the training of all relevant professional groups
- Cover online behaviour in discussions to arrive at diagnoses, for example in the case of eating disorders and identity issues
- Introduce prevention measures at child day care centres and schools, with the active involvement of parents and children

- Make protection strategies mandatory for all clubs and schools – constant monitoring and updates
- Take action to prevent cyber-grooming
- Incorporate the protection of minors in relation to the media as a cross-cutting issue in all school subjects – especially general studies – at primary school level.
- Take technical protection measures – preventing images from being shared, disabling screenshots, disabling the downloading of images => preventing dissemination

In this context, we wish to expressly draw attention to the fact that the European Commission's Better Internet for Kids initiative contains many such approaches.[16]

11. Does the European Commission's proposal effectively cover all online platforms on which child pornography material can be disseminated, and if not, what kind of improvements are potentially needed regarding the proposal's scope of application?

The dissemination methods are very probably used in a much more wide-ranging and flexible way than we can imagine. As an example: we assume that close interaction and a great deal of sharing takes place between the dark web and the open internet, which can be disrupted by police work (internationally) and systematic deletion. This should also be considered by policy-makers.

The EU Centre

12. Does the European Commission's proposal give sufficient consideration to instruments to improve prosecution and enforcement? Where are improvements potentially needed, and what instruments would be necessary for this purpose?

This requires a legal assessment which can take a holistic view of the criminal law rules which exist in this context both at EU, national and sub-national level. In principle, there is a need for instruments which ensure that the investigating authorities are adequately equipped in staffing, psychological and technical terms to deal with this kind of sexual abuse material, so that they can effectively handle the sheer volume of material, offender networks, etc.

Provided that it is independent of Europol, the new centre would be well-suited to judging and communicating the success and failure of various investigative approaches, and developing international strategies based on this.

Duplication of effort should be avoided.

13. Will the new EU Centre be able to adequately support national law enforcement agencies and Europol, according to the current plans, and what resources would it require to do so?

This question cannot be answered until it is clear what powers this centre will ultimately have.

In principle, the creation of a European version of the National Center for Missing and Exploited Children is welcome. However, any close links with Europol, no matter what kind, should be opposed.

An EU Centre should be entirely independent of Europol, both financially and in terms of location. It must ensure close cooperation with child protection organisations and hotlines.

[16] See "A European strategy for a better internet for kids (BIK+)": https://digitalstrategy.ec.europa.eu/en/policies/strategy-better-internet-kids

Other responsibilities should include maintaining the hash database for known material and researching trends with regard to dissemination, etc.

That said, cooperation with national investigators is also essential. We do not envisage the centre as being part of the police work, but it should conduct evaluations and communicate lessons learned – including with regard to technical support tools and approaches to take in national cooperation and legislation.

It would also be helpful to assist small and medium-sized providers both financially and by offering expertise and concrete (software) solutions, so they can make their sites and services safe for children and detect suspicious material.

Please also see our answer to question 3.

Child-friendly technologies by default

14. In your opinion, does the European Commission's proposal encompass all technical approaches which can be used to achieve the aim of protecting children, and what other technical approaches would be necessary, in your view?

The current technical approaches in the draft are not sufficient. Research and education is needed on this issue in order to gain a better understanding of privacy- and rights-compliant technical options.

Approaches which are already effective and promising include, firstly, the server-side scanning of public platforms. The scanning already carried out by large public platforms as part of their content moderation measures (public content), using various tools (hash matching, AI), is a suitable instrument for the detection, review and removal of publicly posted material. Secondly, there are approaches such as the "log-in trap"[17] and the "quick freeze" method[18]; when extreme material is detected, often originating on the dark web, these approaches aim to break the cycle of the copying and preparation of such material and to systematically delete it. We are calling for the log-in trap to be used when investigating perpetrators; this offers a means of identifying users when a reasonable suspicion of wrongdoing exists. Alternatively, we are in favour of the storage of limited address data for a very short period ("quick freeze") to give investigators a reliable opportunity to carry out their work. A corresponding legal basis and a significant improvement in law enforcement agencies' human resources are essential for this. Suitable technologies for securing digital evidence also need to be made available. The guiding principle for technical measures to secure evidence must be not to approach this via the communication.

Pattern analysis: the example of WhatsApp (see our answer to question 5)

Child-friendly design and mandatory information for children, including advisory and help services

In addition to the technical options to delete video and visual material depicting sexual violence against children and to identify the perpetrators, websites and apps should ideally be designed to be child-friendly (in line with general comment no. 25 adopted by the UN Committee on the Rights of the Child).

Firstly, websites could be required to offer child-appropriate information (in simple language) in a manner suitable for children, in addition to their terms and conditions, privacy notice and legal

[17] More in-depth information about the "log-in trap": https://d-64.org/login-falle/
[18] More in-depth information about the "quick freeze" process: https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2010/22_QuickFreezeStattVorratsdatenspeicherung.html

notice; this should explain the website's subject matter and purpose. This information could also help parents to gain a clearer picture of what their children will encounter on the site. Secondly, platforms used primarily by minors should offer low-threshold notice and action and complaint mechanisms (see recital 89 of the DSA). This includes making clear to minors who they can contact if they feel uneasy. This may, for example, be a chat staffed by specialist personnel around the clock. Its availability and professionalism could be ensured by child protection organisations.

It should also be made clear, in an easy-to-understand manner, what help services are available for a given situation (situation-based services) (central national body which directs people to organisations that can help them).[19]

15. The draft Regulation also provides for the possibility of blocking access to individual URLs, and changes to the proposal during the Czech Presidency of the Council even seek to further expand this possibility. Given the widespread use of https encryption for URL requests, do you believe it is technically feasible to specifically block individual URLs without resorting to blocking entire domains? If so, how is this possible, and if not, can this kind of access blocking comply with the requirements established by the European Court of Justice as regards the targeting of access blocking?

Access blocking is, at best, a last resort – we believe that users with technical knowledge can circumvent it. It would be better to delete the material. We would like to see a discussion about making child-safe versions of internet access devices available, and tying this to age classifications for content and interaction options. This would save parents from having to deal with child protection software and installing it on various devices.

The EU Centre II

16. What is your view of the role and nature of the planned EU Centre envisaged by the draft EU Regulation, firstly with regard to the performance of primarily preventive tasks, and secondly with regard to tasks relating to the development and use of technical surveillance tools?

We do not really envisage the EU Centre as providing the framework for prevention; however, we would welcome it if the EU Centre made information, research results and lessons learned available which can be used in the development of prevention services. In any case, close coordination is needed of the various aspects of the fight against sexual violence (rather than focusing solely on the fight against the dissemination of sexual abuse material). We envisage the EU Centre as being highly focused on

- the detection and deletion of material,
- the fight against dissemination,
- assistance (intelligence, technology, financing) in identifying perpetrators and securing evidence,
- action to combat attempts to make digital preparations for new crimes associated with this and with cyber-grooming,
- assistance in improving preventive services, but also in providing better support to victims,
- assistance with legal parameters.

17. If scanning targeted the communications taking place on devices ("chats"), rather than the devices themselves, the same issues would exist regarding the end-to-end encryption of messaging

[19] More detailed thoughts and background information can be found in this paper (see page 7 in particular): https://www.cl.cam.ac.uk/~rja14/Papers/chatcontrol.pdf

services, for example. Again, countless law-abiding citizens would end up in the sights of the authorities simply because of their use of a specific service and the corresponding software. Are you aware of software solutions that allow end-to-end encrypted communications to be read in real time or at least decrypted? Do you believe it is justifiable to use algorithms to break the confidentiality of private communications, which is guaranteed by the German constitution?

We are not currently aware of any such technologies.

As we have already stated several times: we do not believe it is justifiable to use algorithms to break the guaranteed confidentiality of private communication in the case of end-to-end encrypted communications. Scanning encrypted communications without a reasonable suspicion of wrongdoing is disproportionate and unhelpful. Everyone has a fundamental right to privacy, including children. Regarding the issue of privacy, please see our response to question 1.

In the view of the German Society for the Protection of Children, "chat control" would not lead to the desired result. We regard the scanning of communications as a disproportionately severe interference in the privacy of members of the public – and children, in particular – when instead various fundamental rights should be weighed against each other.

18. The draft Regulation states that the EU Centre on Child Sexual Abuse to be established in The Hague is to generate binding indicators of sexual abuse material, which are to be used by the companies carrying out the scanning. Yet experienced investigators know that it is impossible to unequivocally define and substantiate on a case-by-case basis what criteria determine what constitutes a family photo, a self-documented game among children and young people, a chance snapshot of a sporting event, or, indeed, child pornography. Is any information already available about the methodology used by the EU Centre? And if so, can this methodology be regarded as reliable and suitable?

It is difficult to judge the methodology before the EU Centre has even been established.

We would like to take this opportunity to emphasise once more that a purely technological solution based on AI reliability would not lead to the desired result, as the error rate is too high and a professional assessment by trained staff is always necessary, especially when it comes to making these types of distinctions. Please also see our response to question 5. Investigators tell us, however, that new material can usually be found where existing material has been detected. AI can be trained to perform scans within the current scope and thus help to detect suspicious new material. The EU Centre can also help to identify the best methods (and programs) INDEPENDENTLY of the vendors.

Berlin, 27 February 2023

The German Society for the Protection of Children – Federal Association

Schöneberger Str. 15

10963 Berlin

Tel: +49 (0)30 21 48 09-0

Fax: +49 (0)30 21 48 09-99

Email: info@kinderschutzbund.de

www.kinderschutzbund.de

The German Society for the Protection of Children (DKSB) – For the future of all children!

The German Society for the Protection of Children, established in 1953, is Germany's largest child protection organisation, with 50,000 members and more than 400 local associations. The DKSB is an advocate for children's interests and for political and societal change. The priority areas of its work are children's rights, child poverty, violence against children, and children and the media.