Statement on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (2022/0155 (COD))[1]

On March 1, 2023, the German Bundestag's Committee on Digital Affairs held a hearing named "Chat Control". We welcome the fact that the committee took up this topic in order to develop a position on the proposed regulation. Nevertheless, we note with regret that there is apparently little interest among the parliamentary factions to take a balanced view of the regulatory project. In our view, this is indicated by the selection of experts invited, among whom stakeholders who take a constructive stance toward the project[2] were unfortunately absent, as well as the designation of the hearing with an alarmist term that does not do justice to the facts underlying the EU regulatory proposal. The term chat control, which is not used in the draft regulation, was used by actors to introduce a debate which describes the concern for child protection as being in conflict with privacy and data protection, and which is conducted with the aim of discrediting the proposed regulation. In addition the wording of the questionnaire, which was sent to the invited experts for answering, in part does not correctly reflect the regulatory proposal, but is rather formulated suggestively and indicates a certain bias of the authors.[3]
In light of this, we are providing our opinion on the draft regulation from the perspective of civil society and children's rights, and would like to contribute to the consultation and opinion-forming process. This is done on the basis of the questionnaire of the Committee on Digital Affairs of the German Bundestag.

1) The EU Commission's proposal for the CSA regulation, also known as chat control, has caused a lot of discussions since its publication in May 2022. Please explain the technical, legal, constitutional, data protectional, social and/or societal implications of the proposal.

The European Commission published its Better Internet for Kids (BIK+) strategy on May 11, 2022. This strategy bundles objectives and measures to enable children to use the digital environment independently and safely. Age-appropriate services should protect children from harmful and illegal content, promote media literacy, enable children to act independently and safely in digital spaces, via participative functionalities as well as involve children themselves in the design of online services suitable for them.[4] On the same day, the European Commission presented the draft regulation discussed here. Both projects must be considered together and should jointly contribute to young people being able to participate in digital experiences without being harmed.
The draft regulation addresses a specific and serious risk that many young people face online. According to the JIM Study 2022[5], a quarter of boys and girls in Germany between the ages of 12 and 19 have been contacted by strangers in the digital environment in the past twelve months. This does not necessarily mean a risk in every case. Nevertheless, the initiation and perpetration of sexualized violence against children is a real danger. Perpetrators extensively use digital environments to approach and get to know children, to communicate with each other on their intentions regarding children's abuse, and to disseminate material depicting sexualized violence. In 2021, Internet companies identified and reported 85 million images and videos of corresponding crimes worldwide.[6] In the same year, according to police crime statistics, Germany recorded an increase of around 110

[1] Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:13e33abf-d209-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF
[2] Overview of stakeholders who welcome a European regulation available at: https://childrens-rights.digital/transfer/assets/9063.pdf
[3] Questionnaire available in in German language at: https://www.bundestag.de/resource/blob/935152/2d25b625bc92f26518236334dbd2ada8/Fragenkatalog-data.pdf
[4] Further information available at: https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids
[5] Available at: https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2022_Web_final.pdf, English summary on page 61
[6] Further information available at: https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-abuse_en

percent in the distribution, acquisition, possession and production of depictions of sexualized violence against children and young people.[7][8] These are only the cases known to law enforcement. According to the Independent Commissioner for Child Sexual Abuse Issues (UBSKM) Kerstin Claus, Europe has become a hub for the dissemination of such abuse images.[9] Given these circumstances, it is an obvious step that the European Commission has issued a proposal to prevent and combat such crimes, which has the support of a majority of the population. For example, in a survey of 9,410 adults in eight European countries[10], just over three-quarters (76 percent) were in favor of the automatic detection, reporting and removal of material depicting sexual violence against children.[11]
With its draft regulation, the European Commission intends to oblige online service providers to assess their services to identify relevant risks (see Art. 3 of the draft) and to counter these risks with suitable precautionary and security measures (see Art. 4 of the draft), to detect and report sexualized violence against children and to either remove such depictions or deny access to these (see Art. 1 of the draft). If it is found that the measures taken will not sufficiently mitigate potential risks, it is possible to issue a so-called detection order (see Art. 7 of the draft). The technologies used in implementing the detection order must be effective in detecting and preventing the dissemination of known or new depictions of sexualized violence against children. They must also be sufficiently reliable with respect to potential false positives. The users' right to privacy and to confidentiality of communications and the protection of personal data should be respected as far as possible (see Art. 10 of the draft). Accordingly, the responsible data protection authorities are to be involved in the procedure. Legal action may redress the issuance of a detection order (see Art. 9 of the draft).
With the Better Internet for Kids Strategy (BIK+), the European Commission addresses the important societal concern of empowering young people to use and participate independently and safely in the digital environment. This concern is supported by the draft regulation discussed here, which addresses a relevant risk. The draft shows measures to prevent sexualized violence against children and to prosecute criminally relevant acts within the interest of the majority of the population of the European Union. After weighing the legal aspects, the proposed measures appear justifiable and feasible in order to achieve the formulated objectives.

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

First, we note that a detection order should not be issued based on suspicion of the exchange of incriminated material; rather, the process begins with a risk assessment of the service by the provider and measures to mitigate identified risks. Only if it is determined in the subsequent process that the risk mitigation measures are not having the required effect a detection order is taken into consideration. Furthermore, it is incorrect that in the case of a detection order, a "hidden" disclosure takes place; rather, information obligations of the providers towards the users are mandatory in Art. 10 para 5 of the draft.
The question of which services and devices could potentially be affected, and to what extent, cannot be answered in a generalized manner. Theoretically, every communication service and every service that enables an exchange among users in order to disseminate known and unknown material of sexualized violence against children or to contact children with the intention of committing

[7] According to the police crime statistics, child sexual abuse cases increased by 6.3% to over 15,500 cases in 2021. There was a 108.8% increase in depictions of abuse to over 39,000 cases
[8] Further information available in German language at: https://beauftragte-missbrauch.de/presse/artikel?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_n
[9] Ebd.
[10] France, Germany, Italy, Netherlands, Poland, Sweden, Hungary, Spain
[11] Further information at: https://ecpat.de/wp-content/uploads/2021/11/Summary-Report-Polling-Research.pdf

sexualized violence can be considered. As a result, any device that provides access to the aforementioned services is potentially addressed by the European Commission's draft regulation. Because of this, the need arises to assess the services' risks to identify precisely those that must take precautionary measures as well as implement safety concepts for their users. If the providers concerned do not take sufficient measures to mitigate the risk of sexualized violence against children, a detection order may be considered. If, in this case, the interest in preventing and combating sexualized violence outweighs the potentially negative impact on the (fundamental) rights of the users of the service (see Art. 7 para 4a and 4b of the draft), a detection order will be issued. In this case users are informed that appropriate measures have been taken to prevent and combat sexualized violence against children and that, as a result if necessary, reports of communication and content can be made to the EU Center (see Art. 10 para 5 of the draft). Therefore, the users are always aware when relevant material or information might be disclosed, so no hidden and/or general monitoring will take place. With this transparent approach, the European Commission is pursuing the goal of preventing such activities and informing the users of the service that they are participating in a digital environment that may harbor risks and dangers for them.

3) Why do you think the Commission's proposal is 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?

Sexualized violence is a serious problem in our society. It must be addressed with a comprehensive approach. Most stakeholders e.g. providers, regulators, educators and guardians are aware that they have to work together and share responsibility in order to achieve sustainable and efficient results. Precautionary and protective measures, such as those set in the 2021 amendment of the German Youth Protection Act[12] and already practiced in the context of safety-by-design concepts, are just as much a part of this as policies and regulatory approaches that oblige providers to invest in the safety of their services. Furthermore, this includes educational institutions, child and youth services, and civil society actors that enable children, legal guardians, and professionals to deal with digital services in a safety-conscious manner.
Through the General Comment No. 25[13][14], the United Nations Committee on the Rights of the Child provided guidance and suggestions to States Parties on how to apply the United Nations Convention on the Rights of the Child in the digital environment to realize the rights to protection, provision and participation for all children. In Europe, both the Council of Europe's Strategy for the Rights of the Child[15] and the EU Strategy on the Rights of the Child[16] highlight the need for protection and participation of young people in the digital environment.
The draft regulation supports the implementation of these guidelines through measures to prevent and combat sexualized violence against children. Thus, it is obvious and at best intrinsically motivated that providers assess their services for possible risks and hazards and then take appropriate measures to provide young users with a safe online experience. After all, safe services for children increase the attractiveness of a service and are perceived positively in terms of taking responsibility in the community. However, where providers are unwilling or unable to do so, state and public sector stakeholders intervene on a temporary basis to assist in the realization of a safe online environment and to enforce the obligation to ensure the safety of young people.
In summer 2024, the interim derogation from the ePrivacy Directive for the protection of children on the Internet will expire. Therefore, there is a concrete need for action with regard to the regulation

[12] See Paragraph 24a JuSchG (German Youth Protection Act)
[13] Original document available at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
[14] German translation available at: https://kinderrechte.digital/hintergrund/index.cfm/key.1738/topic.324
[15] Available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a5a064
[16] Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:e769a102-8d88-11eb-b85c-01aa75ed71a1.0002.02/DOC_1&format=PDF

of a risk assessment-based obligation to monitor already known and previously unknown depictions of sexualized violence against children as well as communications with the intention of cyber grooming. This need is intended to be met by the European Commission's draft regulation.

4) How do you assess the danger of innocent citizens coming under suspicion due to false positive automated detection and what consequences would such false positive reports have for both the suspects as well as the investigating authorities?

No investigative process - whether based on human or technical factors - is free of errors and false assessments. Therefore, potentially criminally relevant behavior or material must be evaluated as objectively as possible and in context. The presumption of innocence applies until proven otherwise. Accordingly, investigation processes must be handled sensitively, comprehensibly and in accordance with the legal system. Prejudgment is not permitted.
However, it should also be a matter of course that illegal behavior will be uncovered, the perpetrators investigated and criminal consequences drawn. In this specific context, it is necessary to use technical means to counter the large number of known illegal and unknown illegal materials in circulation as well as the initiation of contacts between adults taking advantage of young people's age and inexperience with the aim of committing sexualized violence against children.
Both quantitatively and qualitatively, technology can be a valuable support and supplement to human intelligence and law enforcement efforts. In this context, it should be emphasized that technologies should not be responsible for the final evaluation, but that this should always be left to a human being.
The European Commission's draft regulation stipulates that communications or materials that have been disclosed (see Article 12 of the draft) must first be examined by employees of the EU Center (see Article 48 of the draft). In this way, the European Commission makes a significant contribution to relieving the national prosecution authorities, which can concentrate on cases that have been assessed by independent experts as relevant for prosecution. On the other hand, it also counteracts potential prejudgments, since not every report that needs to be assessed is relevant to criminal prosecution. The EU Center can therefore also be seen as a further guarantee of security, as experts in sexual violence against children process and sort out the facts before they come to the attention of the criminal prosecution authorities and are pursued there. Overall, it can be assumed that this procedure will have a positive impact on possible suspects and the investigating authorities, since the assessment of independent experts can be expected to reduce the number of suspicious cases and thus allow the investigating authorities to concentrate on relevant cases.
With this approach and the willingness to establish and equip the EU Center, the European Commission underlines its responsibility both for the protection of children and for the protection of the rights of users of high-risk online services.

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

No technology can be 100% relied upon to detect children being contacted by adults with the intention of committing sexualized violence. This is precisely why it is so important that not every report made by technology is forwarded unchecked by a human being to law enforcement authorities, causing overload and expose those involved in the process to possible prejudgment. Nevertheless, there are procedures which, while maintaining encryption mechanisms, are able to detect with a high degree of probability whether the messages are SPAM messages or malware, for example, on the basis of metadata and/or patterns. In principle, these technologies can also be used to detect grooming intentions. To reduce the potential burden of false positives, reporting thresholds

can be implemented that only lead to a corresponding system response once a certain number of potential suspicious cases have been detected within a defined period of time.
For further information, please refer to our comments in the answer to question 4.

6) What technical approaches do you consider to be effective and constitutionally acceptable alternatives to the measures envisioned in the draft regulation?

The draft regulation, with its combination of technology deployment and human review, proposes the best possible approach to this day to prevent and track sexualized violence against children online. In doing so, the European Commission takes the comprehensive significance of the fundamental rights of users of online services into account and balances these with the protection and participation rights of children and young people in the digital environment. The European Commission also envisions a multi-stage process consisting of risk assessment, the implementation of precautionary and protective measures, and any necessary detection of illegal practices. Precisely because a detection order is sensitive to fundamental rights and affects all users of a service, it imposes strong requirements on the implementation of a detection order (see Articles 7 and 10 of the draft). The issuance of such an order is also subject to critical consideration by various actors and thus contributes to a balanced, targeted and effective decision (see Art. 7 of the draft), to which the affected provider can file a legal appeal (see Art. 9 of the draft).

7) The Commission's proposal includes a demand 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 in order to implement age verification in compliance with fundamental rights while preserving the anonymity of users on the Internet?

The aim of the proposed regulation is to protect children and young people from sexualized violence and to prosecute this violence. Following the necessary risk assessment, providers should therefore take effective measures to protect minors in their services in a meaningful way. For this purpose, it would be useful or even necessary to know the age of users (see Art. 3 of the draft). Consequently, the draft regulation authorizes providers to check the age of users after the risk assessment has revealed a certain potential of threats in order to minimize these (see Art. 4 of the draft). The same shall apply to app store providers if they offer applications with proven risks (see Art. 6 of the draft). In this respect, age verification would apply to every user who makes use of an evidently risky service.
Existing age verification procedures are based on the verification of highly personalized data, e.g., by presenting or transmitting information from the ID card, and/or use biometric data in live verification procedures, which are also very sensitive.[17] The anonymity of the user is not guaranteed in any of the existing procedures, as more data is regularly collected and processed than is necessary to determine the age. In line with the objective of this proposed regulation, it seems sufficient not to know the precise age of the users, but to make meaningful distinctions between age cohorts in order to be able to provide effective precautionary and security measures for these groups. An age verification procedure in compliance with fundamental rights, data-minimizing, and anonymity preserving is currently being discussed within the German government.

8) The Commission's proposal would make it possible to impose detection orders on private communication services, e.g. to obtain content from private and encrypted chats (e.g. client side scanning), to detect grooming or to verify someone's age; as a consequence of the technology-neutral approach, network blocking is also potentially conceivable. What would be the international

[17] Explanations of corresponding procedures within the scope of the PostIdent service are available in German language at: https://www.deutschepost.de/de/p/postident.html

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?

The question addresses potential (side) effects of the draft regulation that (could) lie outside the European Union and take unknown third parties into consideration. As it is mentioned that corresponding technologies could be used in other countries and possibly in other contexts, it should be noted that it is not the technology and the data collected with it that pose a potential problem, but rather their use in contexts that would not be considered democratic and/or constitutional by local standards.
The European Commission's draft regulation sets strong standards for the technologies used in implementing a detection order. These must be effective in detecting the spread of known or new depictions of sexualized violence against children or contact with children and sufficiently reliable with regard to false reports. They should interfere as little as possible with users' right to privacy and to confidentiality of communications and protection of personal data (see Art. 10 of the draft). This technology neutral approach is set as an incentive for service providers to develop correspondingly powerful systems in order to ensure the protection of children in the digital environment as well as the protection of the privacy of all users in their services. Systems that are not capable of meeting these requirements may not be used in accordance with the requirements of the draft regulation. We consider the risk that effective systems for detecting incriminated material will be used in non-European jurisdictions for other, potentially non-democratic purposes to be low. In this regard, we also refer to the fears expressed accordingly following the Network Enforcement Act in Germany, which, however, have not materialized. So far the Act has not been imitated in other countries or instrumentalized for undemocratic purposes.

9) Recently, in a study the "Child Rights International Network" underlined the importance of "leaving behind the framing of privacy versus child protection in order to protect the rights of all children" (coverage 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 would be the short-term and long-term consequences of the Commission's proposal in this regard?

With the study "Privacy and Protection: A children's rights approach to encryption"[18], the Child Rights International Network (CRIN) contributes to a holistic view of children's rights as enshrined in the Convention on the Rights of the Child[19] adopted by the United Nations in 1989. According to this, all children's rights are to be considered equally important and can only be mutually realized. It follows that the rights of the child to protection from violence (Art. 19 UN CRC) or from sexual abuse (Art. 34 UN CRC) and to the protection of privacy (Art. 16 UN CRC) are equally relevant and are not in a relationship of superiority or subordination to each other. The rights are also interdependent and contribute mutually to their realization. CRIN's study investigated the impact of encryption (technologies) on children's development and lives. In doing so, the study establishes references to the Convention on the Rights of the Child, taking the General Comment No. 25 into account as well as concrete situations in which children benefit from encryption or are adversely affected by it. It identifies the benefits and risks of encryption for the realization of children's rights. CRIN advocates for recognizing that children are individuals, not a homogeneous group, and promotes taking into account that the impact of encryption can vary greatly depending on the child's background, needs, and identity. With this report, the network therefore proposes different scenarios to open up the discussion beyond the paradigm of privacy versus protection and gives examples of the diversity and

[18] Available at: https://static1.squarespace.com/static/5afadb22e17ba3eddf90c02f/t/63c9173dc9ac2348a1d9eac7/16741230
[19] Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

complexity of ethical, legal and practical issues. Overall, the network's stakeholders assume that privacy and protection should be thought of together and that all measures taken to protect young people should be assessed to determine their impact. Furthermore, they point out that debates about the protection of children and young people in the digital environment should not be reduced to technical approaches alone and they call for existing protection systems for young people to be considered holistically. Lastly, they draw attention to the fact that children, with their views and perspectives, should participate in corresponding debates. As a result, providers should be held accountable and encouraged to transparently explain how they counteract violations of children's rights in their services, and receive advice and support on how they can make their products safe for children. CRIN considers child-friendly reporting procedures to be a key instrument in this regard. The handling of such reports should be timely and comprehensible. The excessive use of technologies should be avoided.
The draft regulation discussed here is part of a broader strategy for the safe participation of children in the digital environment and does not only focus on technical possibilities of protection against sexualized violence. The approach of the European Commission follows the recommended procedure of the CRIN for the protection of children against sexualized violence online. In their report, the authors warn against narrowing the discussion on the protection of young people to the dimension of surveillance and advocate for a multifaceted approach: *No single law, policy or technological development can protect children online or secure their human rights more broadly. Encryption cannot be addressed in isolation, but only as part of a wider ecosystem with a range of actors that can meaningfully interact, each with its own role that it can effectively and legitimately play* (see page 104).

10) In your opinion, which package of political measures is promising in order to take action against sexualized violence against children in an efficient and effective way in accordance with fundamental rights? Where is potential for improvement in preventing and combating sexualized violence and its depiction on the Internet?

The European Commission's package of measures consisting of the Better Internet for Kids Strategy (BIK+) as well as the draft regulation discussed here shows both comprehensive and meaningful ways to prevent and prosecute sexualized violence against children. For the rest, we refer to our comments in the answer to question 3, in which reference has already been made to corresponding diverse measures.

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

Insofar as the question is aimed at the fact that the European Commission's draft regulation does not address the darknet, we would like to draw attention to the fact that crime does not take place exclusively in the dark. Even if the findings can only refer to the so-called bright field for understandable reasons, it is clear that the exchange of criminally relevant material takes place to a considerable extent on the Internet[20]. Also, with regard to grooming, i.e. adult strangers contacting children with the intent of committing sexualized violence, it can be assumed that this takes place primarily on the openly accessible Internet, since children in general are not on the darknet and thus obviously cannot be approached by perpetrators there.
In this context, we would also like to point out that every new photo or video found to be incriminating leads to an additional hash value, thus contributes to expanding the database of known material and to reduce the dissemination of (then) known material of sexualized violence against children. This is of particular importance, as any forwarding, re-posting or making this material

[20] See https://home-affairs.ec.europa.eu/whats-new/campaigns/legislation-prevent-and-combat-child-sexual-abuse_en

available in any other way represents a perpetuation of a crime, which can lead to re-victimization for the children depicted, as well as impair healing and coping processes or even lead to further harm. Furthermore, every photo or video image that becomes known and has already been clearly classified as criminally relevant and illegal contributes to relieving the burden on investigative and prosecution authorities, since corresponding assessment processes do not have to be carried out again.
Regardless of this, the European Commission's draft regulation aims to prevent sexualized violence against children, so it makes sense to focus on the Internet. The proposed measures, together with the plans of the Better Internet for Kids Strategy (BIK+), appear to be suitable as an effective contribution to the protection of children in the digital environment.

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?

The regulation aims to reduce the amount of widespread depictions of sexualized violence against children as well as the number of cases of grooming through prevention and deterrence. Perpetrators currently do not face a high probability of their criminal acts being discovered, neither on the open Internet nor on the darknet. The draft responds to this with the threat of a detection order if the risk assessment for the service shows a high probability of such crimes being committed. Cases detected in this way result from well-founded monitoring and a high percentage of them may therefore be considered valid. As a result, they will entail a corresponding investigative effort on the part of the competent law enforcement authorities with the aim of enforcing the law. How extensive this effort will be and what human resources will be needed for it will depend crucially on the extent to which a deterrent effect can be achieved through the threat of detecting the crimes - a high degree of deterrence brought about by criminal law generally leads to a reduction in the number of cases. Nevertheless, it is generally desirable to improve resources of the investigating authorities; however, this is the responsibility of national authorities and cannot be ordered by the European Commission by means of a regulation.

13) According to current plans, will the new EU Center be able to adequately support national law enforcement agencies and Europol and what equipment would be required to do so?

The planned center will be established as an independent legal entity of the European Union (see Art. 41 of the draft) and aims to prevent and combat sexualized violence against children. According to the draft regulation, it will collect and provide information and expertise, assist in the detection, reporting, removal and blocking of relevant materials, and support the work of other public and private institutions through cooperation (see Art. 40, 43ff of the draft). Europol as well as national law enforcement authorities working in cooperation with the EU Center will have access to the databases as well as to the indicators and reports upon request, provided that this is necessary and useful for their work (see Art. 46 of the draft). In addition, the EU Center should have the competence to independently forward information on possible criminal offenses directly to Europol and competent law enforcement authorities (see Art. 48 of the draft). The processes envisioned for cooperating and providing support appear to be suitable for effectively achieving the goal of preventing and combating sexualized violence against children.
The preparation and execution of the budget, including the staffing plan, is the responsibility of the Executive Director of the EU Center. Each year, the Executive Director submits an estimate to the Executive Committee. The Executive Committee shall prepare a final draft on the basis of the estimate and forward it to the European Parliament, the Council and the European Commission. Taking into account the budgetary and personnel resources deemed necessary by the European Commission, the European Parliament and the Council shall approve the funds for the EU Center (see

Art. 67 of the draft). It is therefore up to the European Parliament and the Council to decide to support the EU Center with adequate resources.

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?

With its draft regulation on preventing and combating child sexual abuse, the European Commission has opted for a technology-neutral approach. Especially considering the ongoing development of technologies, it is highly welcomed that the regulatory document does not stipulate the use of specific technologies. This would mean that the regulation would have to be regularly updated with regard to newly available resources. Since technological developments often evolve more quickly than a formal amendment or new legislative process, there would be a very great risk that the regulation would regularly fall short of what is technically possible and, as a result, children would not receive the best possible protection against sexualized violence. In addition, the absence of specific technologies opens up a free space for providers to use and/or (further) develop suitable procedures to prevent and combat sexualized violence against children, taking the requirements set by the regulation into account.
Since the technology neutral approach is future-oriented, the German legislator also implements it. For example, the amendment of the German Youth Protection Act enacted in 2021 defines objectives for the safe participation of children and young people in the digital environment and does not conclusively describe which measures providers should meaningfully and effectively implement. In this way, the German legislator is following the same approach as the European Commission in the proposed regulation.

15) The draft regulation also foresees the possibility of blocking individual URLs from the network, which will even be extended in the course of the draft amendments made so far during the Czech Council Presidency. Given the widespread use of https encryption for URL enquiries, do you consider it technically possible to block individual URLs in a meaningful manner without resorting to blocking entire domains? If so, in what way should this be realized, and if not, can blocking networks in this way satisfy the requirements of the Court of Justice of the European Union regarding the equifinality of blocked networks?

In our view, the draft regulation gives clear priority to deletion of incriminated material over blocking. Given the https transport encryption required for secure online transactions, detection of incriminated content being transmitted would require deep package inspection, such as that used to combat viruses, spam, and protocol violations. For the material to be combated by the draft regulation, deletion should be given priority as a matter of principle, due to the serious and traumatizing consequences for the individuals affected by its production and dissemination. After all, material that has not been deleted can be made retrievable and disseminated again at any time.

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

In our view, a center that monitors and coordinates preventive measures at European level is a welcome development. As stated in question twelve, prevention and deterrence help to reduce the number of cases and thus to concentrate investigative work on the relevant ones. However, prevention does not consist solely of educational and pedagogical measures towards children and those responsible for their upbringing; rather, it must also include the use of preventive technical instruments, specifically for the prevention of sexualized violence against children. In our view, the

development of such technical instruments is the responsibility of the providers of services and platforms where significant risks have been identified.
We see the EU Center's task as facilitating the exchange of knowledge and findings with regard to the use and effectiveness of technical instruments. In addition, the EU Center is expected to support victims of sexualized violence - regardless of the origin of the victims and the perpetrators; this approach is welcomed from the perspective of civil society and children's rights.

17) If not the devices but the communications ("chats") possible with them are investigated, this would also apply to end-to-end encryption of messenger services, for example. Here, the authorities would focus countless law-abiding citizens simply because they use a certain service with the corresponding software. Are you aware of software solutions that allow real-time reading or at least breaking of end-to-end encrypted communication? Do you think it is justifiable to abolish the confidential private communication guaranteed by the constitution by using algorithms?

The draft regulation calls for a detection order if a service poses significant risks of sexualized violence against children and if the prevention and combating of this abuse outweighs the potentially negative impact on the (fundamental) rights of the users of the service (see Art. 7 para. 4 a and b of the draft). If a detection order is implemented, all users of the service will be informed in advance that appropriate measures will be taken within the service to prevent and combat sexualized violence against children and that, as a result, reports will be made to the EU Center if necessary (see Art. 10 para. 5 of the draft). In this sense, users of the service are aware that detection of materials and communications is carried out by use of technology and it is assumed that this has a highly deterrent effect on perpetrators. If, on the basis of the algorithm used, the corresponding materials and communications are disclosed, the EU Center's experts will check whether these represent potentially criminal acts. Taking further measures is therefore not based solely on the algorithm used. Knowledge of the communication content is not necessarily required for the detection of potentially criminally relevant actions within communications. Rather, instruments for detecting patterns are already used today in other contexts. For example, financial service providers analyze financial flows to determine whether micro-payments are received simultaneously from different regions of the world in certain accounts and can thus contribute to the detection of live-streamed sexualized violence against children. Corresponding patterns, e.g. a large number of contact requests to users not previously connected to the profile of the person making the request, may be an indication of a broad-based grooming process. In this case, a more extensive analysis of interpersonal communication would not be a general surveillance measure, but rather an investigation based on initial suspicion.
The right to privacy and confidential communication is essential for our coexistence and represents a valuable good. No less important is the protection of children from sexual violence and their right to grow up healthy. With this in mind, the European Commission's draft regulation sets strong standards for a detection order as well as the technologies used in the process. These must be effective in detecting the spread of known or new depictions of sexualized violence against children or in preventing contact to children with sexual intent, and must function with sufficient reliability with regard to potential false positives. They should interfere as little as possible with users' rights to privacy and to confidentiality of communications and protection of personal data (see Art. 10 of the draft).

18) The draft regulation states that the proposed EU Center for Child Sexual Abuse in Den Haag should provide binding indicators for images of sexual abuse to be applied by the companies doing the scanning. Now, experienced investigators know that it is by no means possible to clearly define and prove in individual cases what criteria should be used to determine what is a family photo, self-documented play among children and young people, a random snapshot of a sporting event, or in fact child pornography. Are there already any findings about the methodical procedure of the mentioned EU Center? If so, can this procedure be assessed as reliable and suitable?

Since the EU Center does not yet exist, there is no basis for making serious statements about a potential methodological approach and to evaluate it professionally. It seems foreseeable that knowledge, indicators and technologies will gradually develop further through the implementation of the regulation and that, as a result, the reliability of investigations will increase and the error rates will decrease. Nevertheless, it cannot be assumed that technologies alone will be able to cope with the tasks of preventing and combating sexual violence in the foreseeable future without human involvement.