EUROPEAN COMMISSION

Brussels, 2.3.2023
C(2023) 1584 final

Dear Chair,

The Commission would like to thank the Eerste Kamer for its Opinion on the proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse {COM(2022) 209 final}.

The proposal is one of the initiatives adopted under the 2020 EU strategy to fight against child sexual abuse, which takes a holistic perspective on this crime, leveraging all relevant tools and mobilising all relevant stakeholders, from public authorities to the private sector. The proposal complements other legislative instruments in the field of child sexual abuse, in particular the 2011 Child Sexual Abuse Directive, by obliging relevant online service providers to assess the risk of child sexual abuse on their services and take mitigating measures; to report, remove and block online child sexual abuse on their services; and to proactively detect online child sexual abuse if ordered to do so by a judicial or independent administrative authority. The main aim of the proposal is to ensure that online service providers take responsibility for protecting children on their services from online child sexual abuse.

The Commission appreciates that the Eerste Kamer decided to analyse this proposal and agrees on the importance of striking the right balance between the protection of children and other fundamental rights.

The Commission agrees with the fundamental importance attached by the Eerste Kamer to the right to privacy and with the need to ensure that any interference with such right is limited to what is necessary and proportionate in view of the objective pursued. In relation to the concerns expressed in the Opinion on the compliance of the proposal with the principles of proportionality and subsidiarity, the Commission would like to stress that the proposal respects both.

In response to the related question and more technical comments raised by the Eerste Kamer in its Opinion, the Commission would like to refer to the clarifications provided in the attached annex. The Opinion has been made available to the Commission representatives in the ongoing negotiations of the co-legislators, the European Parliament and the Council, and will inform these discussions.

Ms M. de Boer
Chair of the Standing Committee
for Justice and Security
Eerste Kamer
Postbus 20017
NL-2500 EA DEN HAAG

cc: Mr Jan Anthonie Bruijn
President of the Eerste Kamer
Postbus 20017
NL-2500 EA DEN HAAG

The Commission hopes that the clarifications provided in this reply address the issues raised by the Eerste Kamer and looks forward to continuing the political dialogue in the future.

Yours faithfully,

Maroš Šefčovič
Vice-President

Ylva Johansson
Member of the Commission

Annex

The Commission has carefully considered each of the issues raised by the Eerste Kamer in its Opinion and is pleased to offer the following clarifications.

1) The proposal does not involve indiscriminate scanning of communications.

The Commission is aware of the need to ensure the necessity and proportionality of any interference with the right to privacy and data protection that might result from the implementation of detection orders, especially in relation to detection in the context of interpersonal communications. The proposal contains a series of safeguards that ensure the strict necessity and proportionality of detection orders.

First, the proposal frames detection as a last resort measure. If the rules are adopted as proposed, all providers within its scope will have to comply with risk assessment and risk mitigation obligations. It is only when, despite the mitigation measures taken, a significant risk of use of the service in question for the purpose of child sexual abuse remains, that providers could be ordered to detect online child sexual abuse.

Secondly, once the need for a detection order arises, the proposal takes into account the necessity to ensure a correct balancing of all fundamental rights at stake and, in particular, to minimise the interference with the right to privacy of online users. For this reason, the procedure to issue a detection order will involve several steps and entities. In particular:

- *Before requesting a detection order, the Coordinating Authority of establishment must prepare a draft request and notify it to the provider concerned and the European Centre to prevent and counter child sexual abuse (the 'EU Centre').*

- *The EU Centre may offer its opinion, based, among other things, on its expertise on technologies.*

- *The provider drafts an implementation plan and requests the opinion of the competent data protection authority.*

- *Taking into account the draft implementation plan, the opinion of the data protection authority and the opinion of the EU Centre, the Coordinating Authority has to decide whether to request the issuance of the order. When doing so, the Coordinating Authority has to consider whether (i) the order is as targeted as possible, (ii) it is necessary and proportionate, (iii) available technologies exist that enable effective detection on the specific type of service concerned without entailing a disproportionate interference with the privacy of electronic communications.*

- *The final decision on whether to issue a detection order belongs to a judicial or independent administrative authority. Because of the independent nature of the latter, their involvement constitutes an important additional safeguard, reviewing the assessment made by the Coordinating Authority in an unbiased and objective manner. In particular, the issuing authorities are required to ensure a fair balancing of all the fundamental rights involved.*

- The detections orders are limited in time and subject to regular reporting and review after they have been issued. The rights of redress of the service providers and users concerned are also guaranteed.

- Detection orders remain limited to the use of indicators, provided by the EU Centre, which creates and manages them, subject to a number of safeguards ensuring their accuracy and reliability. In addition, any mandatory scanning is to be carried out using technology meeting strict requirements.

Thirdly, the proposal seeks to ensure that detection orders, in particular, regarding the solicitation of children ('grooming') are as targeted as possible. Such detection order can only concern communications if one of the users is a child below the age of 17 (the highest age of sexual consent in the EU). In addition, the proposal goes beyond what is required by Article 36 of the General Data Protection Regulation[1] (GDPR) by requiring providers (i) to request the opinion of the data protection authorities on any draft implementation plan concerning the detection and (ii) to do so before the detection order is even requested by a Coordinating Authority to the issuing authorities. In addition, detection orders regarding the solicitation of children are subject to specific requirements and safeguards, for instance, regarding the particular manner in which the required 'significant risk' is defined and the duration of such orders.

In light of the above, the Commission considers that the proposal – and, in particular, its detection provisions, which are framed as last resort and targeted measures – complies with the principles of necessity and proportionality. In that regard, account should also be taken of the nature and severity of the crimes that the proposed obligations aim to combat and the need to involve the online service providers covered to achieve that.

2) The Commission considers that the choices made in the proposal correspond to the most effective method of preventing and combating child sexual abuse.

First, the proposal emphasises the importance of prevention, imposing a blanket obligation on services at risk of misuse for the purpose of child sexual abuse to assess such a risk and adopt mitigating measures. In 2020, around 95% of the reports of Child Sexual abuse reaching the US Centre for Missing and Exploited Children (NCMEC) came from one service provider only, and 99% were submitted from five service-providers only. Most service providers do not report child sexual abuse voluntarily. Hence, the Commission considers that the extension of the obligation to conduct a risk assessment and adopt mitigating measures to all relevant service providers operating in the EU Digital Single Market will bring about a significant improvement in terms of child safety.

Secondly, the proposal moves away from a model of voluntary detection, allowing service providers to choose whether and how to balance their own interests, child protection and the interests of users. It establishes instead a model of mandatory detection orders, to be issued on a case-by-case basis by judges or independent

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

administrative authorities. Under the proposal, it is for these independent public authorities – rather than for private companies – to establish when a detection order is necessary and proportionate (also in terms of scope and duration). Considering how delicate the balancing of fundamental rights on the online space is and the safeguards provided for, the Commission considers this a significant improvement of the current model.

3) The Commission will neither collect nor process any data under the proposal.

When mitigation measures prove insufficient and a judge or independent administrative authority has established that in the case at hand the issuance of a detection order is necessary and proportionate, the service provider concerned will carry out the detection, after consulting the competent data protection authority. If potential child sexual abuse is detected, a report will be forwarded to the EU Centre, which according to the proposal would be established as an independent, decentralised EU agency. The Commission will not receive or collect data. The EU Centre will have the function of, inter alia, (i) filtering obvious false positives, ensuring that only reports with investigative value reach law enforcement, (ii) providing feedback to providers on the quality of their reports, so that detection accuracy can improve over time and (iii) creating and managing the indicators to be used for detection purposes.

Actionable reports will then reach the European Union Agency for Law Enforcement Cooperation (Europol) and national law enforcement. The data will be erased or stored by these entities according to the applicable legal framework.

4) The proposal does not intend to replace the current notice and action mechanisms in place and the relevant activities of hotlines.

On the contrary, the proposal builds on these mechanisms and reinforces them. Hotlines will be able to continue flagging child sexual abuse on providers' services and asking for its removal. In addition, if providers do not comply voluntarily, hotlines will be able to bring child sexual abuse material to the attention of the newly established Coordinating Authorities, which can in turn issue a removal order where the applicable conditions are met. In other words, the activities of hotlines will gain effectiveness and benefit from the proposed enforcement mechanism.

As part of the proposed tasks of the EU Centre relating to the sharing of knowledge and expertise for the prevention and combating of child sexual abuse, the EU Centre will also be able to work with hotlines.

The proposal also expressly empowers Coordinating Authorities and, in some cases, the EU Centre to notify content considered to be child sexual abuse material to relevant service providers. In this manner, too, the proposal builds on notice and action mechanisms.

5) The proposal is part of a broader EU Strategy to prevent and combat child sexual abuse.

The Commission constantly monitors the progress of Member States in the implementation of the 2011 Child Sexual Abuse Directive[2], most notably in the context of infringement procedures. In addition, the Commission is undertaking a process of revision of the 2011 Directive to ensure that children are adequately protected in light of the societal and technological developments of the past 11 years. In the context of this revision, the Commission is exploring all avenues to better prevent and combat child sexual abuse, including further harmonisation of minimum standards, enhanced assistance and support to victims, and strengthened prevention programmes.

6) The process that led to the adoption of the proposal by the Commission was conducted in consultation with the broadest possible set of stakeholders.

The Commission exchanged views on several occasions with representatives of law enforcement authorities, national hotlines, service providers affected and survivors of child sexual abuse.

Part of the service providers involved voiced concerns on the technical feasibility of detection on end-to-end encrypted services. The Commission discarded the possibility to exclude these services from the scope of the proposal for at least two reasons. First, a balance between the interests of the service providers, the protection of children and the interests of users must be struck throughout the digital single market, and end-to-end encrypted services cannot constitute a blind spot in this respect. Secondly, exempting end-to-end encrypted services from the scope of application of detection orders would have amounted to depriving detection of any effectiveness: service providers could have opted out from any form of mandatory detection by moving to end-to-end encryption.

Some providers of interpersonal communication services have asked the Commission to include in the proposal a legal basis for voluntary detection of child sexual abuse. This request was not granted, as providing a legal basis for voluntary detection next to mandatory, order-based, detection would have undermined the logic of the proposal. The proposal ensures that a detection order is issued whenever necessary and proportionate in a specific case. When a detection order is not issued, the criteria of necessity and proportionality of detection are not met, hence providers are not allowed to detect on a voluntary basis. As mentioned above, the required balancing of all fundamental rights affected should be carried out by competent authorities, within a framework set out in law, rather than be left to the service providers.

Finally, certain companies have suggested that detection of solicitation of children could be conducted through metadata collection and scanning, rather than through text-based detection. However, current evidence suggests that metadata scanning is a very intrusive and insufficiently effective method to detect such solicitation. Making any kind of assumption of solicitation of children based on metadata would require the collection and scanning of a considerable amount of metadata from both parties, likely revealing

[2] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

their location, friend-network, frequency of interaction and habits over a sustained period of time. This is arguably no less intrusive than targeted text scanning based on an order issued by a judge or independent administrative authority after careful consideration and balancing of all the rights and interests involved. Moreover, metadata-based detection of solicitation of children is significantly less effective in achieving the aim of identifying abuse, as solicitation typically occurs in conversations between two parties that display no peculiar pattern. Finally, metadata-based scanning does not produce any evidence of possible solicitation. Hence, it cannot lead to the submission to law enforcement authorities of any actionable report containing indications of child sexual abuse.

7) The Commission attaches the utmost importance to support and assistance to victims and to prevention, focussed both on potential victims and potential perpetrators.

The 2011 Child Sexual Abuse Directive already contains provisions on prevention and assistance to victims and the Commission monitors the programmes and measures adopted by Member States to comply with these provisions closely. Hence, the upcoming revision of the Child Sexual Abuse Directive is the appropriate context to tackle outstanding challenges related to crime prevention, support and assistance to victims. The Commission is evaluating how to strengthen these two aspects and address outstanding issues, such as the challenges encountered by several Member States in establishing specific and effective programmes and measures on perpetrator prevention.

As opposed to the Child Sexual Abuse Directive, the proposed regulation was adopted on an internal market legal basis. Hence, it is not the appropriate legal instrument to require Member States to establish new preventive programmes or take measures on assistance and support to victims. Nevertheless, the proposal leverages the Coordinating Authorities and EU Centre in order to provide a specific form of assistance to victims, namely support in finding information and obtaining removal of child sexual abuse material concerning them.

In conclusion, the proposal for this regulation and the existing 2011 Directive are complementary and should be considered together when assessing the current EU efforts in the fight against child sexual abuse.

8) The proposal introduces safeguards to ensure that the execution of detection orders does not lend itself to any type of 'function creep'.

First, detection orders are as targeted as possible, limited in time and implemented based on a plan submitted by the provider concerned to both the issuing judge and the competent data protection authorities.

Secondly, detection can only be implemented using the mandatory list of indicators of child sexual abuse kept by the EU Centre. These indicators work on a 'hit-no-hit' basis. Hence, they do not allow providers to acquire any other information beside the existence of a match between an indicator, on the one hand, and an image, video or text pattern on their services, on the other.

Thirdly, detection orders can only be issued by a judge or independent administrative authority when technologies exist that are (i) effective in detecting child sexual abuse, (ii)

deployable on the specific service and (iii) sufficiently protective of privacy and other users' rights. The proposal provides for the consultation of the EU Centre and of the competent data protection authority in relation to planned detection orders to support this assessment.

9) Whilst the proposal sets out a range of safeguards in relation to the creation and management by the EU Centre of the digital identifiers used as indicators of child sexual abuse, it does not contain any exhaustive catalogue thereof. The latter choice is due to the need to ensure that the proposal remains future proof, as new types of indicators with higher accuracy rates than those currently in use could emerge with technological development.

Currently, indicators used for voluntary detection are:

- *(i) hashes (i.e. numerical 'fingerprints' associated to child sexual abuse material that has already been verified as such) and Uniform Resource Locators ('URLs') pointing to specific items ('deep links') for known child sexual abuse material;*
- *(ii) artificial intelligence (AI) classifiers (numerical fingerprints generated by AI trained on databases of known child sexual abuse material to find analogous material) for new child sexual abuse material; and*
- *(iii) natural text patterns for solicitation of children.*

10) Neither the EU Centre nor service providers are granted any law enforcement task or power under the proposal.

The EU Centre does not assess the criminal law nature of the items of online child sexual abuse received. Its function is to filter out obvious false positives, detected by mistake, and prevent them from reaching law enforcement authorities. All other reports will be forwarded to the competent national law enforcement authorities and assessed by them as to their criminal relevance. It is for each authority to verify, in accordance with the applicable law, whether an item corresponds to child sexual abuse and is, in fact, illegal. In addition, the proposal provides for a mechanism ensuring that, where such authorities establish that a new reported item constitutes child sexual abuse material, they communicate the result of their assessment to the EU Centre, so that a corresponding indicator can be added to the database of indicators of known child sexual abuse.

Thus, the assessment of the criminal law nature of the content reported by service providers is conducted entirely by competent authorities at national level. The EU Centre does not have enforcement powers either. In particular, orders such as those for the detection or removal of child sexual abuse may only be issued by the competent national authorities.

Similarly, service providers are not required to perform any assessment of the criminal law nature of the potential child sexual abuse identified when implementing a detection order. They are simply required – upon reception of a detection order – to implement and operate on the relevant services the technology needed to check against the database

of indicators and to subsequently report any match, via the EU Centre, to the competent law enforcement authorities.

It should be noticed that some service providers already report potential child sexual abuse material detected voluntarily to the US Centre for Missing and Exploited Children (NCMEC), which forwards relevant reports to Europol. The proposal introduces an obligation to detect and report, requiring providers to take responsibility for keeping their services free from this type of very serious illegal activities.

Compared to the current system of voluntary detection, the Commission considers that the new system of mandatory and targeted detection orders will further lower any risk of misuse or erroneous reporting. Currently, service providers decide themselves whether to engage in activities for the detection of child sexual abuse, in accordance with their own assessment of what is necessary and proportionate and without a complete legal framework regulating those decisions and activities. The introduction of a system of mandatory detection to be ordered only when necessary and proportionate by a judge or independent administrative authority within the EU, with the involvement of data protection authorities and with the safeguards described above, will significantly reduce the risk of any instrumentalisation of detection. The same is true for the involvement of the EU Centre, which, as an EU agency, will have to act in an objective manner and comply fully with EU data protection standards.

11) The Commission considers that effective prevention of child sexual abuse requires the adoption of a holistic approach, which takes due account of both the offline and online dimension of this crime. The proposal is a considerable step forward on prevention for at least three reasons. First, it requires all relevant online service providers, that face a risk of misuse of their services for the purpose of online child sexual abuse, to assess such a risk and adopt safety by design measures with preventive objectives. Secondly, it aims to significantly limit the circulation of child sexual abuse material, which not only prevents re-victimisation but also constitutes an important component of perpetrator prevention (as research shows that a considerable rate of those who view child sexual abuse material online end up committing real-life abuse at a later stage). Thirdly, the proposal requires Coordinating Authorities, service providers and the EU Centre to keep statistics on several aspects of the crime, as well as on reports and their follow-up by national authorities. This information is key to increase the effectiveness of national prevention programmes.

A further point to note is that the 2011 Child Sexual Abuse Directive requires Member States to adopt prevention programmes and to enable law enforcement to use effective investigative tools. The ongoing process of revision of that Directive also entails an assessment of the need to reinforce provisions on prevention and investigations, for example by explicitly requiring Member States to allow for undercover investigations on the 'dark web'. As explained, that Directive is in principle the appropriate place to set out measures of this kind.

12) The Commission considers that only a holistic approach can be effective in the fight against child sexual abuse. Hence, the identification of both victims and perpetrators is key and Member States should avoid investing on one aspect at the expenses of the other.

13) The Commission has no comments on whether it would be more appropriate for the Netherlands to comply with the proposed regulation by means of its administrative law or of its criminal law.

14) When choosing appropriate technologies for the purpose of implementing detection orders on their services, providers are required to comply not only with the requirements of the proposal but also with the requirements of any horizontal EU legislative instrument applicable to them, such as the GDPR but also the e-Commerce Directive[3]. This does not need to be specified in the proposal, which does not purport to entail any derogation from the provisions of the e-Commerce Directive.

15) The proposed regulation is a sectoral instrument, covering only certain forms of child sexual abuse as defined in the 2011 Child Sexual Abuse Directive, which sets the minimum harmonised EU standard in the field. Other forms of online harm to children are not within its scope. The proposal defines what child sexual abuse material or solicitation of children are, for the purposes of the proposed regulation, with reference to the Directive. The proposal is not a criminal law instrument, but an internal market instrument requiring relevant online service providers to take responsibility for keeping their service clear of material and activities that are illegal according to the 2011 Child Sexual Abuse Directive.

16) The establishment of the EU Centre will not lead to delays in the submission of reports to national law enforcement authorities. Currently, in practice, reports are collected and forwarded to Europol by the US Centre of Missing and Exploited Children (NCMEC) when they appear to have EU relevance. With the EU Centre receiving those reports directly, there would be increased speed of processing and effectiveness. The involvement of the EU Centre will help streamline the reporting process, both by making it entirely clear for service providers to whom they need to report and by ensuring that national law enforcement authorities are not unnecessarily burdened by manifestly erroneous reports. The EU Centre will be staffed and structured with the best interest of the children in mind, taking into account the imperative need to ensure expediency and objectiveness. In addition, the proposal already caters for the need to expedite the treatment of urgent reports, by requiring providers to signal the need for urgent action when submitting such reports.

17) The proposal is technology neutral. It is not intended to discourage the use of end-to-end-encryption but rather to ensure that both privacy and child safety are ensured everywhere in the online space, including on end-to-end encrypted services. The

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

proposal does not entail any form of indiscriminate scanning and does not require the systematic decryption of communications of all users, as explained above.

18) The EU Centre is not in place and has no database of indicators nor list of technology yet. It is unclear to what type of indicators, content and detection technology the Eerste Kamer refers when it refers to a 12% error rate. It might be useful to note that the error rate for detection of known child sexual abuse material is extremely low (significantly below 1%). The acceptable error rate for new material is entirely dependent on political choices, as AI classifiers are trained to detect material that corresponds to child sexual abuse material with a pre-defined probability rate, that can be set higher or lower depending on the political choice made in this respect. For example, Thorn's AI Classifier can be set at a 99.9% precision rate. With that precision rate, 99.9% of the content that the classifier identifies as child sexual abuse corresponds to actual child sexual abuse.
