**Comments of the services of the Commission on some elements of the Draft Final Complementary Impact Assessment on the Commission Proposal for a Regulation Laying down Rules to Prevent and Combat Child Sexual Abuse, presented by ECORYS, at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE)**

This non-paper prepared by the Commission's services aims to provide explanations with regard to the proposal for a Regulation on preventing and combating child sexual abuse.
This non-paper is based on the relevant Commission proposal and does not present any new positions with regard to that proposal.

## BACKGROUND

On 11 May 2022, the European Commission published a Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (the 'Proposal')[1].

On 6 April 2023, a consortium headed by ECORYS presented a Draft Final Complementary Impact Assessment on the Commission Proposal for a Regulation Laying down Rules to Prevent and Combat Child Sexual Abuse, prepared upon commission by the European Parliamentary Research Service (EPRS) on behalf of the Committee on Civil Liberties, Justice and Home Affairs (LIBE) (the 'study'), to answer the following questions:

1. Are all dimensions and aspects of the problem covered and adequately analysed? How effective and efficient is the CSA proposal in addressing the problem?
2. What is the likely impact of the CSA proposal on the internet?
3. What is the likely impact of the CSA proposal on fundamental rights?
4. Are the measures foreseen in the CSA proposal necessary and proportionate?
5. How would the detection of new CSAM or grooming respect the prohibition of general monitoring obligations? Are the new obligations and requirements foreseen in the CSA proposal precise enough as to not violate the prohibition of general monitoring obligations?
6. What would be the preferred option among the three retained options for an EU Centre to prevent and counter child sexual abuse?

The study was prepared in a short time frame, between November 2022 and March 2023, and with a targeted mandate based on a number of questions. Aside from the short time frame, as the study acknowledges, it faced a number of key methodological limitations. Given the more limited scope of the exercise, the study is narrow in scope. Secondly, the amount of evidence-based academic research on the impact of the proposal on technology, the quantity and quality of detection, and on behaviour was found to be limited and the authors therefore had to rely on expert opinions. An additional limitation lies in the lack of explicit consideration by the experts interviewed of aspects of the Proposal other than detection orders, as it seems to emerge from references such as "The majority of consulted experts expect a steep increase in reported content as providers of information society services will would [sic] be obliged to detect and report

[1] COM(2022) 209 final.

more, and the CSA proposal covers known material, new material and grooming" [2]. This type of statements does not give account of the differentiated, risk-based approach of the Proposal when drawing conclusions on its expected consequences. In particular, it does not factor into the reasoning the fact that the Proposal only allows for order-based detection as a last resort measure, to be taken when mitigation fails to sufficiently reduce the risk of misuse of a service for the purpose of online child sexual abuse.

The study concludes that "the overall effectiveness of the CSA proposal is expected to be limited. This is caused by a variety of factors that when taken together make it difficult to conclude that the CSA proposal will be effective".

The study also concludes that the Proposal "would result in efficiency gains in the fight against CSA. In particular, the decreased reliance on US databases and services for the detection of CSAM would benefit efficiency," and "the establishment of the EU Centre would positively impact the effectiveness of the combat against CSAM". At the same time, the study notably questions the compatibility of the envisaged measures with fundamental rights to privacy the protection of and personal data, and expresses concerns on the impact that the proposal would have on law enforcement reports.

In response, the following sections provide further details on certain aspects on each of the responses provided in the study to the questions asked by LIBE.

## 1. ON THE PROBLEM DEFINITION

The study questions that fragmented legal frameworks across Member States negatively impact cooperation between public authorities and providers of information society services, stating that "[h]aving national legal frameworks in place might actually improve cooperation between public authorities and providers of information society services on the national level, rather than hamper it. Moreover, it can be questioned whether the fragmentation of legal frameworks across Member States can be considered as the driver that calls for the introduction of an EU-wide approach, or whether the actual problem driver is CSA."

The Commission agrees that the underlying problem is child sexual abuse. Its manifestation online, both through grooming and through the exchange of materials, takes place on online services offered across EU Member States' borders. If each Member State were to adopt its own legal framework for dealing with these services, the service provider would face different rules in each Member State. This creates an obstacle to the internal market. The same logic was also applied recently in the Digital Services and Digital Markets Acts.

## 2. ON THE IMPACT OF THE CSA PROPOSAL ON THE INTERNET

*Impact on technology*

The study argues that, because the technologies to detect new CSAM and grooming have lower accuracy than those to detect known CSAM, that would lead to an increase of reported content and high error rates which would reach law enforcement.

[2] As the study does not include its interview methodology, it cannot be verified which information was provided to interviewees, nor whether the interviews followed a standardised approach.

The study does not reflect the fact that the technologies to detect new CSAM and grooming are already deployed at scale,[3] . For example, last year NCMEC received more than 67000 reports concerning grooming globally (7561 of those reports were related to EU Member States). A majority of the grooming report received by NCMEC, whose global number more than doubled compared to 2021, originated in messaging services via proactive detection by companies.

The Commission, in its impact assessment, has set out in detail which technologies are currently being used, could be potentially used, and could be developed. Annex 8 of the Impact Assessment accompanying the Proposal provides information, examples and research on technologies used to detect CSAM. [4]
On the *already existing technologies*, at least 8 technologies have been described and explained in detail, with information about their uses and accuracy rates being fully shared. For known CSAM, this includes PhotoDNA[5], YouTube CSAI Match[6], Facebook's PDQ and TMK+PDQF[7]. The study also does not take account of the fact that technologies to detect new CSAM and grooming are already deployed at scale, including Thorn's Safer Tool[8], Google's Content Safety API[9], Facebook's AI Technology[10], and Microsoft's Project Artemis[11].

Second, the study also does not take into account the role that the EU Centre would have in (i) providing verified indicators of CSA that would be the only ones permitted to be used in detection, and (ii) preventing manifest false positives from reaching law enforcement, by acting as a filter between content reported by providers and content reaching law enforcement. The human review provided by the EU Centre ahead of any submission to law enforcement further reduces the error rate. Also, the study did not fully consider the fact that companies would be immediately notified by the EU Centre when their tools are producing erroneous notifications, and will be obliged to take steps to fix it.

Finally, the accuracy of the detection technologies for new CSAM and grooming is quite high as set out in the Impact Assessment on the Proposed Regulation to Counter Child Sexual Abuse, according to the providers.[12] For the detection of new CSAM, the accuracy rate lies significantly above 90% and can be set to 99.9% meaning a 0,1% false positive rate. On the detection of solicitation of children in text-based communications, this is typically based on pattern detection. Some of the existing technologies for grooming detection (such as Microsoft's ), have an accuracy rate of 88%, before human review.

---

[3] For example by Meta on its Facebook services, see here.
[4] Impact Assessment Report Accompanying the document: 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, 11 May 2022.
[5] PhotoDNA
[6] YouTube CSAI Match
[7] Facebook's PDQ and TMK+PDQF
[8] Thorn's Safer Tool
[9] Google's Content Safety API
[10] See here and here for more information on Facebook's tool to proactively detect child nudity and previously unknown child exploitative content using artificial intelligence and machine learning
[11] Microsoft Project Artemis
[12] Impact Assessment Report Accompanying the document: 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, 11 May 2022.

It is important to note that the accuracy rate cited here refers to the number of false positives as a percentage of overall messages flagged for review, rather than a percentage of all messages subjected to a check. The accuracy of AI-based technologies such as detection of new CSAM and grooming can be expected to further increase in the near future, given the rate of development of AI technology that we are experiencing at the moment.

*Impact on the quantity and quality of detection*

The study argues that the quality of detection will deteriorate and that the role of the EU Centre will play will not be sufficient to improve the quality of detection, "considering that decades of research and development have, to date, not resulted in high accuracy levels for detecting new CSAM and grooming".

The study does not consider the various points that would instead permit the quality of detection to improve. At present, companies detect when they want, what they want and how they want. For example, they use their own databases of hashes, built without any public oversight.
In the Commission's Proposal, the companies would detect only if prevention measures are not sufficient and if a court or an independent administrative authority mandates it after an extensive process in which the necessity and proportionality of the detection is carefully assessed, in consultation with data protection authorities.

1. If companies receive a detection order, they would need to use the hashes and indicators provided by the EU Centre, which would correspond only to material that is illegal in the EU, as assessed by national Courts. This should significantly reduce the number of reports of materials that are illegal elsewhere but not in the EU.
2. The Proposal provides for detection, reporting and removing templates which were created based on close consultations with law enforcement on the minimum key data to be reported. This standardisation will greatly facilitate the use of reports for law enforcement, while ensuring useful information for investigations.
3. Considering the role of the EU Centre filtering out false positives, this will actually lead to a significant increase in the quality of reports received by law enforcement compared to the current situation.

The Centre will make available for free the technology to detect, which will alleviate the burden on the providers, especially smaller ones, who will be able to engage in detection both in a more easy and precise manner.

Finally, the assertion that "considering that decades of research and development have, to date, not resulted in high accuracy levels for detecting new CSAM and grooming" is misleading, as it suggests that companies have invested heavily on R&D for detection technologies, an assertion that is questionable.

*Impact on behaviour of providers of information society services, children, and users*

In E2EE communications, the study questions the accuracy rates of technology to detect CSAM stating that "it is unlikely that technologies to detect CSAM in E2EE communications develop

rapidly to reach high accuracy levels in the upcoming 2 to 5 years, without undermining the secure nature of E2EE communications and the security at the end devices."

However, it is unclear what factual basis this statement relies on. Experts have in fact stated quite the opposite; in July 2022, technical experts from GCHQ and the National Cyber Security Centre published a paper explaining a range of possible ways that child sexual abuse material could be detected within encrypted services that would still protect user privacy. The paper also indicates the need for a framework that can be used for consistent evaluation of various techniques on specific platforms and services.[13]

The study also recommends other solutions: "solutions that have more potential include analyses of user behaviour and metadata such as network signals." However, research shows that metadata is not an effective tool for detection of child sexual abuse. For example, in a recent survey by Stanford University among companies on the technologies they use to detect CSAM, none of the companies found the detection of CSAM using metadata effective[14]. Detection based on metadata is much less effective in achieving the objective of preventing and fighting against child sexual abuse than content-based detection, as it does not allow for the submission of actionable reports and, therefore, for the identification of victims for the purpose of providing them with support and assistance, and perpetrators, for the purpose of preventing the commission of further crimes. .

Firstly, metadata cannot reliably predict whether someone engages in exchange of child sexual abuse materials. The situation is different from, e.g., spam or mass malware dissemination, where the volume of interactions and of recipients alone or checking of sender IP addresses against blocklists can already provide certain information. By contrast, given the typically private nature of the dissemination of CSAM, it is not possible to tell whether someone exchanges CSAM solely from the metadata.

In addition, content – images and videos – is indispensable for identifying victims depicted: it is not possible to identify who was abused based on the metadata.

Finally, the use of metadata is often justified by its lesser degree of intrusiveness. However, it is not immediately evident why the privacy intrusion of detection using metadata could be considered significantly less invasive compared to content-based detection[15]. Content is detected without regard to user identity, using technologies that solely answer the question "is this likely to be CSA online yes or no?" not the question "what is this content image/video/conversation

---

[13] Thoughts on Child Safety on Commodity Platforms, by Dr Ian Levy and Crispin Robinson, 21 July 2022.

[14] Pfefferkorn, R., Stanford Internet Observatory, Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers, 9 September, 2021. See in particular the table in p.16. See also here Meta's Monika Bickert statement before the House of Commons: «If content is being shared and we don't have access to that content, if it's content we cannot see then it's content we cannot report». Finally, it should be noticed that metadata-based detection requires the collection of a varied set of data concerning the number and frequency of interactions between accounts, the existence of overlaps between the friends' groups of the two account, the location of the users etc. Such data are likely to become less and less available. For example, the recent roll-out by Apple of Private Relay would obscure, for those companies which enable the functionality, any client/server relationships established across the Safari browser. This represents a general trajectory in online standards towards obscuring metadata as well as content.

[15] In joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net, para. 117, ECJ stated in relation to metadata that "that data provides the means of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications".

about?" With metadata, it would be necessary to collect significant amounts of data across multiple online exchanges to determine probabilities that a given online exchange is CSA online.

## 3. IMPACT OF THE CSA PROPOSAL ON THE PROTECTION OF FUNDAMENTAL RIGHTS

Weighing the fundamental rights affected by the measures in the CSA proposal, the study states that "it can be concluded that the CSA proposal would infringe, in respect of users, Articles 7 and 8 of the Charter of fundamental rights". According to the study, this infringement cannot be justified.

The need to balance all the fundamental rights at stake is at the core of the legislative proposal. When it comes to preventing and combating child sexual abuse online, these fundamental rights are, notably:

- the right to physical and mental integrity of children (Article 3 of the EU Charter of Fundamental Rights (the 'Charter')), the prohibition of torture and inhuman and degrading treatment (Article 4 Charter), their right to such protection and care as is necessary for their well-being (Article 24 Charter), their right to respect for their private and family life (Article 7 EU Charter) as well as to protection of their personal data (Article 8 Charter);
- the right to respect for private and family life (Article 7 Charter), to protection of personal data (Article 8 Charter), and the freedom of expression (Article 11 Charter) of the other users of the online services concerned;
- the freedom to conduct a business (Article 16 Charter) of the online service providers that fall within the scope of the proposal.

The study acknowledges that, in the context of the measures set out in the Proposal, not only the fundamental rights of the users are at stake, but also those of the children, including the positive obligations of relevant public parties to protect the children's rights recognised by the Court of Justice, among which is children's right to privacy[16].

Under the case law of the Court of Justice, the seriousness of the reasons to limit the exercise of fundamental rights determines not only *whether* there can be such a limitation (justification), but also *to what extent* such a limitation can take place (proportionality).[17] In other words, the aim of combating particularly serious crime and protecting children against particularly serious interferences with their fundamental rights is key for the proportionality assessment.

Children are a particularly vulnerable category of persons, and the violation of their right to privacy and other rights through the dissemination of child sexual abuse material online is grave and known to have lifelong consequences for the victims. Moreover, tackling the solicitation of children ('grooming') is especially important given that it can help prevent such particularly serious violations of children's rights from taking place.

In light of this, the proportionality assessment of the detection obligation should take account of:

- on the one hand, the limitation of privacy of a larger group of online userswhich may result from a *judicial* or *independent administrative order* issued based on an assessment of

[16] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126-128.
[17] Case C-817/19, *EU PNR*, para. 115-116.

necessity and proportionality – including the balancing of all fundamental rights at stake - to counter a significant risk of child sexual abuse on the service;

- on the other hand, the violation of the privacy of a smaller but particularly vulnerable group of users (i.e. children), who have the right to such protection and care as necessary for their wellbeing according to the EU Charter;
- as well as the significant impact of that violation on the long-term wellbeing of the child victim;
- and also the fundamental rights of service providers (freedom to conduct business). These are particularly important with respect to the determination of measures to be taken, according to the case law of the Court of Justice.[18] The use of open-ended terms such as 'significant risk' or service used 'to an appreciable extent' for the purpose of online child sexual abuse, is criticised in the study, arguing that these might compromise legal certainty. In this respect, it should be borne in mind, however, that Article 16 of the Charter can make it necessary to use open-ended terms, as this allows the service providers to determine the specific measures to be taken in order to achieve the result sought. The Court has also recognised the need to keep pace with changing circumstances as a valid reason for using open-ended terms[19].

## 4. NECESSITY AND PROPORTIONALITY

The study states that the Coordinating Authority **can issue** a detection order when the risk mitigation measures are not sufficient and that the proposal **"does not provide** the coordinating authority with a legal basis **to take other less intrusive measures**".

These statements are factually incorrect. The proposal states clearly in Article 7(1) that the coordinating authority can only **request** a judicial or independent administrative authority the issuance of a detection order, but it is that judicial or independent administrative authority the one that can issue the order.

Also, Article 5(4) clearly states that the coordinating authority can "require the provider to re-conduct or update the risk assessment or to introduce, review, discontinue or expand, as applicable, the mitigation measures", so that the detection orders are indeed a measure of last resort.

In the view of the Commission services, the measures foreseen in the proposal are necessary and proportionate. It is settled case law of the Court of Justice that the fundamental rights to respect for private and family life (Article 7 of the Charter) and to protection of personal data (Article 8 of the Charter) are not absolute, but must be considered in relation to their function in society[20].

Pursuant to Article 52(1) of the Charter, the exercise of these fundamental rights may be limited, provided the limitation:

- is provided for by law (the proposed regulation will be a legislative instrument);
- is justified by an objective of general interest recognised by the EU or to protect the rights and freedoms of others;

[18] Case C-401/19, *Poland v EP and Council*, para. 75.
[19] Ibid, para. 74.
[20] E.g. ibid, para. 120 ; Case C-817/19, *EU PNR*, para. 112.

- respects the essence of the rights in question;
- is proportionate, in that it is *suitable and necessary* to achieve the objective pursued and corresponds to the *least intrusive means* available to reach it and if the risks to the fundamental rights do not outweigh the benefits of the measure.

In the view of the Commission services, the limitation on the exercise of the abovementioned fundamental rights resulting from the proposal is proportionate:

(i) As shown in the Impact Assessment accompanying the proposal[21], detection of online child sexual abuse is *suitable* to achieve the aim of effectively tackling the particularly serious criminal offences at issue and protecting the aforementioned fundamental rights of children, in particular as detection of known CSAM prevents their re-victimisation while detection of new CSAM and grooming can allow the rescuing of children from ongoing or imminent abuse.

(ii) The criterion of *necessity* is respected by framing detection as a last resort measure. All service providers within its scope have to comply with risk assessment and risk mitigation measures. It is only when, notwithstanding the mitigation measures taken, a significant risk of use of the service in question for the purpose of child sexual abuse remains, that they will be ordered to detect online child sexual abuse. Detection orders can only concern providers of publicly available interpersonal communication services and of hosting services, i.e. providers that may present a real risk of misuse of their services for the purpose of grooming or CSAM dissemination and must be issued by a judicial or independent administrative authority.

(iii) Furthermore, for reasons explored in the Impact Assessment accompanying the proposal (see also its Recital 2), the Commission is of the view that imposing obligations on service providers of the type set out in the proposal is the only manner to effectively combat the particularly serious crimes in question and to protect the rights of the children affected, which can justify the taking of more intrusive measures22. Detection obligations are framed in the proposal in a way that ensures that they do not go beyond what is necessary in each case. The procedure to issue a detection order involves compliance with pre-determined criteria, only after several steps and with the involvement of several authorities. The composite nature of the process is directed at ensuring the proportionality of each detection order in terms of interference with the right to data privacy:

- Whenever required by Articles 35 and 36 of the GDPR *and* in any event in all cases of planned detection orders concerning grooming, the provider must carry out a prior data protection impact assessment and ask the opinion of the competent data protection authority on its draft implementation plan.
- The Coordinating Authority has to ensure that its request for a detection order is as targeted as possible (whenever possible, detection orders should only concern sub-components of the service, if the indication of a significant risk only concerns such sub-component and if technically feasible).

---

[21] See point 2.1.1 of the impact assessment, brining evidence in support of the claim that online CSA is often only discovered thanks to the efforts of online service providers to detect CSAM on their services, and to protect children from being approached by predators online.

[22] Cf. Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154.

- Coordinating authorities are also required to obtain the opinion of the EU Centre and are required to take into account the availability of sufficiently reliable detection technologies when determining whether to issue a detection order. The final decision on whether to issue a detection order belongs to a judicial or independent administrative authority. These authorities are expressly required to ensure an objective and unbiased balancing of **all** the fundamental rights involved.
- Grooming detection orders can only concern communications where one of the users is a child below the age of 17 (the highest age of sexual consent in the EU).
- Providers have to report on the way detection is conducted, including in terms of fundamental rights impact, to Coordinating Authorities. Where necessary, the orders have to be adjusted. Also, more generally, Coordinating Authorities are charged with supervising compliance, using their investigative and punitive powers under the proposal where necessary.
- Redress is ensured, both for affected service providers and affected users.

(iv) there are no less intrusive alternative measures to targeted detection orders that can achieve the aforementioned objectives in an equally effective manner.

In particular, with respect to grooming detection in interpersonal communication services, metadata collection and processing also intrudes on a person's private life and right to data protection, while at the same time being insufficiently effective for the present purposes. The limited effectiveness is linked to the fact that grooming interactions are not characterised by behavioural patterns that can be identified through metadata analysis: they are one-to-one conversations and the only way to become aware of their illegal nature is to detect grooming patterns in their content.

Indeed, in a different context related to general and indiscriminate retention of subscriber and user data, the Court of Justice has noticed the potential intrusiveness of metadata collection and recalled that:

> 'traffic and location data may reveal information on a significant number of aspects of the private life of the persons concerned, including sensitive information such as sexual orientation, political opinions, religious, philosophical, societal or other beliefs and state of health, given that such data moreover enjoys special protection under EU law. Taken as a whole, that data may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. In particular, that data provides the means of establishing a profile of the individuals concerned, *information that is no less sensitive, having regard to the right to privacy, than the actual content of communications'*.[23]

[23] Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117 (emphasis added).

Metadata analysis can lead service providers to take measures against 'suspicious' accounts, e.g. by disabling them. However, without any access to the content of the conversation, it does not allow them to verify whether the exchange is likely to be grooming and should be reported. Hence, the objectives of protecting the potential victim from imminent abuse and to bring perpetrator to justice cannot be met through metadata analysis only.

In light of the above, it is important to note as well that any decision concerning the opening of investigations or prosecutions is taken based on a human, individualised assessment of the situation. Not by private parties, but by the competent law enforcement authorities, in accordance with the applicable law. No decision is taken based on the result of the hit/no-hit automated detection carried out and the subsequent reports by the service providers. In fact, this reporting process, too, is subject to specific requirements set out in the proposal (Articles 12-13) and also involves verification by the EU Centre ensuring that the reports to the competent law enforcement authorities are not manifestly unfounded (Article 48).

## 5. PROHIBITION OF GENERAL DATA RETENTION AND GENERAL MONITORING OBLIGATIONS

The study suggests that the detection orders to be issued under the proposal entail measures that are general and indiscriminate in nature. In this context, the following elements should be considered:

1) The obligations are *order-based*. Detection of both (known and new) child sexual abuse material ('CSAM') and grooming can only take place based on a specific order issued by judicial or independent administrative authorities, relating to an individual case of a service falling within the scope of the Proposal that is at a significant risk of being abused for the transmission of CSAM.

2) The obligations are *risk-based*. Detection orders are issued based on an individualised assessment for the service in question of the level of risk of specific types of online child sexual abuse occurring on a specific service. They can be issued only where there is a significant risk of the service in question being misused for the criminal activities in question. Moreover, prior to the possible issuance of a detection order, other mitigation measures have to be considered, including where applicable the ones that have been considered and implemented based on the Regulation (EU) 2022/2065[24] ("DSA"). An order can be issued only once mitigation measures have been determined to be insufficient to lower the risk in question sufficiently.

3) The obligations are *targeted*. The proposal contains an express requirement, whenever possible, to target and specify the obligation as much as possible, inter alia by focusing only on a relevant part or component of the service. Moreover, the detection obligation can only be imposed in respect of a narrow group of (particularly serious) criminal offences, namely, the dissemination of 'known' or 'new' child sexual abuse material as well as grooming. By extension, only some particular aspects of the communications concerned are affected, such as only material constituting child pornography or pornographic performance – meaning in practice: photos and videos – in relation to the dissemination of 'known' and 'new' child sexual abuse material. To note in this respect the role of the EU Centre, which manages and provides a list of indicators concerning the targeting of communications, in accordance with strict

[24] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

requirements set out in law. Furthermore, in respect of grooming, the detection orders concern exclusively communications where one of the users is a child.

4) Fourth, the obligations are *time-limited*. They apply only for a predetermined, limited period of time. And even during that limited period, reporting and review obligations also apply, which could lead to adjustments where necessary.

5) Finally, the obligations are *graduated* in function of the nature of the activities and the risks for the fundamental rights at stake. For instance, what constitutes a 'significant risk' justifying the issuance of a detection order varies depending on whether the obligation in question aims to combat the dissemination of 'known' child sexual abuse material, the dissemination of 'new' child sexual abuse material or grooming.

Rather than entailing obligations that are general and indiscriminate in nature, the detection obligations that may be issued in individual cases under the Proposal are better compared with forms of targeted obligations of the type that the Court of Justice did deem permissible in the context of its data retention case law. In that case law, it clarified that such targeted obligations could, inter alia, affect certain geographical areas objectively considered to be at risk[25]. Rather than relating to a geographic space, in this case it concerns a specific 'online space' objectively considered to be at risk.

## 6. THE EU CENTRE TO PREVENT AND COUNTER CHILD SEXUAL ABUSE

The study supports an EU Centre that is not independent from law enforcement, with some functions under Europol, due to cost considerations.

The independence from law enforcement is essential to ensure that the EU Centre can effectively assume a key role. The creation of an independent body responds to a request from the European Parliament to ensure a meaningful safeguard before reports are shared with law enforcement.

Considering the importance of independence and the minimal cost differences among the various implementation options for the EU Centre (with cost estimates in the Commission proposal that the study itself acknowledges as rather detailed and of high quality), in the view of the Commission services the best option would indeed be that of an independent EU agency, as included in the proposal.

The study states that "the researchers had limited access to documentation supporting the cost-benefit analysis by the European Commission of the EU Centre to prevent and counter CSA." The European Commission provided all information and data requested, including the preliminary study provided by the same contractor, with whom the Commission had worked over a year. The explanations on the cost-benefit analysis are fully present in the text and Annex 4 and Annex 10 of the Impact Assessment accompanying the Proposal for a Regulation to Counter Child Sexual Abuse.[26]

---

[25] See Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 144-150. See also Joined Cases C-793/19 and C-794/19, *SpaceNet,* para. 112.

[26] Impact Assessment Report Accompanying the document: 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, 11 May 2022.

**ANNEX**

**Non-paper prepared by the Commission services:**

**Balancing the rights of children with users' rights**

## Introduction

1. The Council and the Parliament are currently discussing the Commission's proposal for a Regulation to prevent and combat child sexual abuse[27] ('the proposed Regulation'). This non-paper prepared by the Commission services[28] expands on the compatibility with the Charter of Fundamental Rights of the EU ('Charter') of the proposed system of detection orders in respect of interpersonal communication services.[29]

2. In the following, the proposed Regulation and the relevant legal context are first introduced. Next, some general comments are made. Finally, specific comments are made regarding the four main issues raised in the legal debate, that is, concerning the 'quality' of the law; whether the proposed rules are either general and indiscriminate or targeted in nature; the essence of the fundamental rights at stake; and matters relating to proportionality.

## Proposed Regulation and legal context

3. The objective of the proposed Regulation is to tackle child sexual abuse and protect children's rights in relation to the misuse of certain online services provided in the internal market, including interpersonal communications services.[30] One of the measures proposed to that aim entails empowering – but not obliging – national courts or 'court-like' independent administrative authorities to issue detection orders requiring a given service provider to employ certain technologies to detect three specific types of child

[27] COM(2022) 209 final.
[28] This document should not be used for other purposes than the abovementioned one. As a non-paper prepared by the Commission services, it does not contain an official position of the Commission.
[29] On 26 April 2023, the Legal Service of the Council issued an opinion on the matter (reference no. 8787/23). The present non-paper takes account of the arguments raised in that opinion.
[30] Recital 1 and Art. 1(1) proposed Regulation.

sexual abuse on its service.[31] The measures aim to be '*targeted, carefully balanced and proportionate*'.[32]

4. Under the proposed system, detection orders can only be issued where the competent national court, after a diligent and objective assessment involving also several other independent public authorities, considers that: (a) there is evidence of a significant risk that the service is misused for child sexual abuse; *and* (b) the reasons for issuing the order outweigh its negative consequences, having balanced all fundamental rights and other rights and interests at stake.[33] The availability of suitable technologies and the impact on the rights of the users of the service concerned are part of the required assessment and balancing exercise.[34] Whenever possible, the orders must target only identifiable parts or components of the service in question.[35]

5. Detection orders can only be issued after a mandatory prior process of risk assessment and mitigation.[36] They are therefore a measure of last resort, to be issued only if the risks remain significant despite the risk mitigation measures. Public oversight is ensured also at the stage of execution of the detection orders. In particular, detection can only be done using indicators prepared and reviewed by the EU Centre, a newly created independent EU agency.[37] Also, the service provider subject to a detection order must regularly report on the execution and the competent national authority must regularly assess whether any changes to the detection obligation may be required.[38] Other safeguards include rules ensuring effective redress and complaint-handling;[39] specific requirements regarding the technology to be used;[40] rules on purpose limitation and internal oversight and controls;[41] and information provision to users.[42]

---

[31] See in particular Art. 7-10 proposed Regulation. The three types of child sexual abuse covered are the dissemination of 'known' (i.e. previously detected) and of 'new' (i.e. not previously detected) child sexual abuse material, as well as the solicitation of children (known as 'grooming'). See Art. 2(l)-(p) proposed Regulation.
[32] Recital 2 proposed Regulation.
[33] Art. 7(4) proposed Regulation. As regards the significant risk, see also its Art. 7(5), (6) and (7).
[34] Art. 7(8) proposed Regulation.
[35] Art. 7(8) proposed Regulation.
[36] Art. 3, 4 and 5 proposed Regulation.
[37] Art. 10(1) and Art. 44, 46 and 47 proposed Regulation.
[38] Art. 9(3) and (4) proposed Regulation.
[39] Art. 9(1) and Art. 10(4)(d) proposed Regulation.
[40] Art. 10(3) and Art. 50(1) proposed Regulation.

6. It is true that the issuance and execution of a detection order limits the exercise of certain fundamental rights, notably those to privacy (protection of private life) and protection of personal data of the users of the services in question.[43] That finding is however in itself not conclusive. It is settled case law that these are not absolute rights but must be considered in relation to their function in society.[44] Therefore, the finding is the starting point of the analysis, not its end point. The central question is whether the limitation on the exercise of those two fundamental rights is compliant with the requirements of Article 52(1) Charter, which regulates such cases. The balancing exercise to be conducted in this regard must take account of all the circumstances of the case at hand.[45]

7. In the present case, the limitation is necessary to achieve the objectives of preventing and combating the aforementioned child sexual abuse offences, which the Court of Justice of the EU (CJEU) has described as '*inherently and indisputably extremely serious crime*'.[46] Moreover, the CJEU has also recognised that those crimes entail serious violations of the fundamental rights of the children, notably to protection of private and family life and to protection of an individual's physical and mental integrity, as well as the prohibition of torture and inhuman and degrading treatment.[47]

8. Particularly where, as in this case, children's physical and moral well-being is at risk, public authorities – and therefore logically also the EU legislator – are under a positive obligation to enable effective action against such crimes.[48] In this connection, account should also be taken of Article 24 Charter, which safeguards the rights of the child,[49] as well as the UN Convention on the rights of the child, to which all Member States are a party and which forms part of the general principles of EU law. Article 19 of that Convention is explicit on the need to take appropriate measures, including legislative

---

[41] Art. 10(4)(a), (c), (d) and (f) proposed Regulation.
[42] Art. 10(5) and (6) proposed Regulation.
[43] Art. 7 and 8 Charter.
[44] E.g. CJEU Joined Cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, ECLI:EU:C:2020:791, para. 120; CJEU Case C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:491, para. 112.
[45] E.g. CJEU Case C-112/00, *Schmidberger*, ECLI:EU:C:2003:333, para. 81-82.
[46] C-817/19, *Ligue des droits humains*, para. 149 (emphasis added). See also C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154 (speaking of '*particularly serious*' offences).
[47] Art. 7, 3 and 4 Charter, respectively. See C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126.
[48] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 126-128.
[49] See also Art. 3(3) TEU (stating that the EU is to promote protection of the rights of the child).

ones, for the protection of the child from all forms of physical or mental violence, injury, abuse, neglect, maltreatment or exploitation, including sexual abuse.

9. The case at hand is further characterised by the fact that the extremely serious criminal offences at issue and the resulting equally serious violations of the fundamental rights of children inherently centre on the activities that the perpetrators undertake online. They can therefore only be effectively tackled by involving the providers of the relevant online services, including interpersonal communications services.[50] The in principle 'private' nature of these services implies precisely that they tend to be used for said activities, which by their very nature occur covertly, in that they involve typically communications between a limited number of specific persons.

10. That distinguishes the criminal offences at issue from criminal offences that occur offline. In respect of the latter, having access to certain personal data of users held by online service providers can certainly be *helpful* to tackle the crimes, but this is not necessary the *only* means to do so. Furthermore, the criminal offences at issue are also different from other criminal or otherwise unlawful activities that are conducted online, but that by nature tend to be 'public' at least to some extent, in the sense that they tend to involve communications to larger groups of persons in general, for instance terrorist propaganda, hate speech or copyright-infringing file-sharing.

11. Put simply, in the case at hand, the content is the crime.

12. Finally, the operational and legal challenges currently encountered arise against the background of the changes made as part of the introduction of the European Electronic Telecommunications Code,[51] which took effect from 21 December 2020. The adjusted definitions contained therein in effect extended the scope of the rules on the confidentiality of communications, set out in the e-Privacy Directive.[52] As a consequence, providers of interpersonal communications services were precluded from voluntarily detecting child sexual abuse on their services, as some had done.

[50] Recital 2 proposed Regulation.
[51] Directive (EU) 2018/1972, OJ 2018 L 321/36.
[52] Art. 5 and 6 Directive 2002/58, OJ 2002 L 201/37. In particular, because of the changes enacted, providers of (number-independent) interpersonal communications also qualified as 'electronic communications services' within the meaning of the e-Privacy Directive.

13. As a temporary solution to enable continued voluntary detection, the Interim Regulation was adopted.[53] This was done to allow for the necessary time to adopt a new, long-term legal framework.[54] The proposed Regulation is intended to constitute that new legal framework.[55] The proposed system of detection orders resembles the Interim Regulation in various respects, including that it limits the exercise of the rights and obligations under Articles 5 and 6 e-Privacy Directive.[56] However, the proposed system is based on mandatory rather than voluntary detection and it establishes a far more elaborate and stringent framework, including the limits and safeguards mentioned.

14. The Interim Regulation applies only until 3 August 2024.[57] Therefore, in the absence of a solution found by the EU legislator before that date, the detection activities at issue would again be precluded from that date. Apart from the internal market implications, that implies that the aforementioned criminal offences and fundamental rights violations would remain unaddressed.

**General comments**

15. In the first place, it has to be acknowledged that the Court of Justice of the EU (CJEU) has to date never expressed itself on measures of the kind at issue. There is therefore necessarily a degree of uncertainty. Particularly in respect of complex and sensitive matters such as the present ones, no definitive and absolute conclusions can be drawn in either direction when it comes to compliance with the Charter.

16. In the second place, precisely because the CJEU has not yet ruled on the complex and sensitive matter at issue, it is necessary to take a broad perspective. That involves especially taking account of all potentially relevant case law, including on the combating of illegal online content, and therefore not to focus only on the CJEU's data retention case law, that is, the line of case law centred on the judgment in *La Quadrature du Net*.[58]

[53] Regulation (EU) 2021/1232, OJ 2021 L 274/41. See in particular its Recitals 7-10.
[54] Recital 23 Interim Regulation.
[55] Recital 78 Interim Regulation.
[56] Art. 1(4) proposed Regulation.
[57] Art. 10 Interim Regulation.
[58] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*. Other judgments in this line of case law include CJEU Joined Cases C-293/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238; CJEU Joined Cases C-203/15 and C-698/15,

17. Whilst relevant, the *La Quadrature du Net* line of case law is in itself not decisive. That is so already for the simple reason that the proposed rules at issue concern detection orders, not retention obligations. Insofar as that case law relates to particularly intrusive forms of processing other than retention, the situation at issue is not comparable, as explained below. It should also be noted that this line of case law cannot be said to be consolidated yet, the CJEU being asked until this day to reconsider and refine it on important aspects.[59] Moreover, the restrictive elements contained in that case law should not be over-emphasised; as shown below, account should also be taken of the elements that could justify a less restrictive reading.

18. In the third place, and relatedly, the potential broader implications of an expansive reading of the data retention case law should be considered. One concern is the impact that it may have on the possibilities for effective law enforcement, including on the pending EncroChat case.[60] Another concern is the potential impact on other EU legislation, most notably the Interim Regulation which, as mentioned, despite relying on voluntary action and not providing for a similarly elaborate legal framework, resembles the presently proposed measures in certain respects.

19. Finally, the proposed Regulation is obviously still under discussion. Where deemed necessary, adjustments could be made, including to address possible legal concerns relating to detection orders for interpersonal services. At the same time, apart from possible legal questions relating to any such adjustments, regard should be had to considerations of effectiveness. Entirely excluding detection on interpersonal communications may, for example, help address certain possible legal risks on which the current debate focuses. However, this would likely also make much of the proposed Regulation devoid of purpose. As explained, having regard to the nature of the criminal activities at issue, precisely these kinds of services tend to be misused for child sexual abuse. Moreover, without effective detection, many of the other proposed measures –

---

*Tele2*, ECLI:EU:C:2016:970; CJEU Case C-140/20, *Commissioner of An Garda*, ECLI:EU:C:2022:258; CJEU Joined Cases C-793/19 and C-794/19, *SpaceNet*, ECLI:EU:C:2022:702.

[59] See in particular the re-opening of the proceedings and referral to the Full Court in CJEU Case C-470/21, *HADOPI* (pending).

[60] CJEU Case C-670/22, *EncroChat* (pending).

such as reporting and removal obligations – also risk losing much of their practical significance.

**'Quality' of the law**

20. The first key issue is whether the proposed rules on detection orders meet the requirements as to the 'quality' of the law, that is, whether the rules are sufficient clear, specific and complete to justify the conclusion that the limitation on the exercise of the fundamental rights at issue are 'provided for by law' within the meaning of Article 52(1) Charter. The Commission services are of the view that they are and, consequently, that any doubts raised in this respect are unfounded.

21. There is no debate that the proposed Regulation, in itself, provides a 'law' as required under Article 52(1) Charter. It is true that the proposed rules contain certain open norms, which leave a degree of flexibility and some scope for interpretation. However, that does not mean that the 'quality of the law' requirements are not met.

22. First, the CJEU has held – with reference to case law of the Court of Human Rights (ECtHR)[61] – that said requirements do not preclude the legislation containing the limitation on the exercise of the relevant fundamental rights '*from being formulated in terms which are sufficiently open to be able to keep pace with changing circumstances*'.[62] In fact, the CJEU has noted that precisely the need to respect fundamental rights – and in particular to strike a fair balance between *all* fundamental rights at stake, including the freedom to conduct a business of the service providers involved[63] – may make it necessary to leave it to those service providers '*to determine the specific measures to be taken in order to achieve the result sought*'.[64]

23. Second, other examples such as the Copyright in the DSM Directive[65] and the Digital Services Act[66] (DSA) show that such an approach is not unusual when regulating online

[61] ECtHR Application no. 64569/09, *Delfi v. Estonia*¸*CE:ECHR:2015:01616JUD006456909*, para. 121 (with further references).
[62] CJEU Case C-401/19, *Poland v. EP and Council*, ECLI:EU:C:2022:503, para. 74 (with further references).
[63] Art. 16 Charter.
[64] C-401/19, *Poland v. EP and Council*, 75 (with further references).
[65] Directive (EU) 2019/790, OJ 2019 L 130/92. See e.g. the references to '*best efforts*', '*a sufficiently substantiated notice*' and '*high industry standards of professional diligence*' in Art. 17(4) of this Directive.

services, including in respect of tackling illegal content and activities online.[67] The area is characterised by relatively fast technological and commercial developments, whilst almost by definition involving activities that are sensitive from a fundamental rights perspective. Tellingly, the abovementioned relatively permissive case law of the CJEU and ECtHR relates precisely to measures taken in this area.

24. Third, it is important not to overlook that, in the case at hand, any such discretion and flexibility would be exercised within a detailed framework set out in the proposed Regulation, which includes, as mentioned, many important limits and safeguards. One of the safeguards is that the detection orders are issued by courts or independent administrative authorities and are prepared by, and are executed under the supervision of, other independent public authorities, notably the Coordinating Authority, the EU Centre and national data protection authorities.[68] These public authorities are all legally bound to ensure compliance with the Charter.[69] Their decisions are open to redress,[70] which may lead to preliminary references being made to the CJEU. In addition, the Commission will provide guidance.[71]

25. Thus, on the one hand, in situations like the one at issue, it is permissible and even necessary to leave a degree of discretion and flexibility. On the other hand, there is no question of the service providers being given a free hand. The discretion and flexibility are primarily to be exercised by relevant public authorities, subject to the Charter. Any 'residual' exercise thereof by the service providers concerned occurs under the control of those public authorities and ultimately the CJEU. Only in this manner can the matters at issue be regulated in a manner that is technologically neutral and future-proof and that allows for proportionate, case-specific solutions.

**General and indiscriminate or targeted**

---

[66] Regulation (EU) 2022/2065, OJ 2022 L 277/1. See e.g. the references to '*a criminal involving a threat to the life or safety of a person or persons*', '*promptly inform*' and '*all relevant information*' in Art. 18(1) and to '*a reasonable period of time*', '*frequently*' and '*manifestly illegal content*' in Art. 23(1) of this Regulation.
[67] For another example, see the Interim Regulation.
[68] See in particular Art. 7(1), (2) and (3) and Art. 9(3) and (4) proposed Regulation.
[69] Art. 51(1) Charter. The requirement of fair balancing has been made explicit in Art. 7(4) proposed Regulation.
[70] See in particular Art. 9(1) proposed Regulation.
[71] Art. 11 proposed Regulation.

26. The second key issue relates to the nature of the detection orders contained in the proposed Regulation. In essence, the question here is whether these instruments and the processing of personal data required thereunder is to be qualified as general and indiscriminate, or rather targeted, in nature.

27. That question should be answered in the light of all circumstances of the case at hand. In the view of the Commission services, there are in the present case strong grounds to believe that the proposed measures are not general and indiscriminate like the measures at issue in the data retention case law, but are rather targeted in nature. That is so especially considering that:

- a detection order would be targeted at only a specific service, whenever possible even only to an identifiable part or component thereof,[72] rather than at all electronic communications services collectively;
- the detection obligation would result from an order tailored to the case at hand, including an assessment of the potential impact on fundamental rights, the availability of suitable technologies and the need for any additional safeguards that may be necessary,[73] rather than from generally applicable legislation not involving any case-specific assessment and measures;
- a detection order would only be issued where justified in the light of the existing risks of child sexual abuse, as a measure of last resort, namely where a significant risk of child sexual abuse remains despite the mandatory prior risk assessment and mitigation process;[74]
- a detection order would be subject to strict limits in time,[75] rather than applying without any such limits under generally applicable legislation;
- a detection order would be targeted at certain specific material and conversations entailing specific criminal offences violating children's fundamental rights,[76] rather than a broad list of crimes or threats to national security in general.

[72] Art. 7(8) proposed Regulation.
[73] Art. 7(1), (4) and (8) proposed Regulation.
[74] Art. 3 and 4, as well as Art. 7(4), proposed Regulation.
[75] Art. 7(9) proposed Regulation.

28. It has been suggested that, nonetheless, the proposed detections orders would be general and indiscriminate in nature. Any such view may well affect various aspects of the broader analysis, including regarding the degree of seriousness of the interference with the aforementioned fundamental rights, the possible effects on the essence of those rights and proportionality. In other words, should this view not prove correct, then the concerns that might exist on those points lapse altogether or at least appear to be considerably less serious.

29. In this regard, reference is sometimes made to the position taken by the CJEU on the system of automated analysis provided for in the national legislation at issue in certain parts of *La Quadrature du Net.*[77] However, the national system at issue in that case is different from the detection orders contained in the proposed Regulation. That national system involved the *retention and automated analysis* of certain personal data.[78] That is not at issue under the proposed rules on detection orders, which operate based on a 'hit/not hit' model. That system was also much broader in scope – for instance, focusing on '*links that might constitute a terrorist threat*'[79] – and not subject to the limits and safeguards provided for in the proposed Regulation. Moreover, whilst that system involved general and indiscriminate processing, that is not the case under the proposed Regulation.

30. Furthermore, the abovementioned view could only be based on a very expansive reading of the data retention case law properly speaking, which the Commission services deem neither merited nor convincing.

31. First, any such view fails to acknowledge the differences between retention, at issue in that case law, and detection, at issue in the case at hand. General and indiscriminate retention creates a large pool of personal data, which can subsequently be accessed and analysed. This, in turn, implies that a serious risk may exist of drawing very precise conclusions regarding the private lives of individuals, which is the main driving force

[76] Art. 2(l)-(p) proposed Regulation.
[77] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172-180.
[78] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172.
[79] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 43

behind the strict line taken in the CJEU's data retention case law.[80] Similar risks can arise in respect of other particularly intrusive forms of processing of personal data, such as the automated analysis on a general and indiscriminate basis of the kind referred to above. Although detection can still be intrusive, in the absence of retention or similar processing of the kind mentioned, no similar risk exists. That is especially so given that the detection would function on a 'hit/no hit' basis rather than involving any actual analysis.

32. Second, the aforementioned view appears to assume that solely the *personal scope* of the measures in question – that is, the persons subject to the measures in question – is decisive when determining whether the measures are targeted. However, the CJEU's case law shows that other elements can be relevant too, such as any *limit in time*.[81] Moreover, the case law expressly leaves scope for the use of *other* criteria to prevent the measures from being general and indiscriminate. The CJEU has held that this is, in principle, a matter to be decided by the legislator.[82] This underlines the relevance of the factors listed above which, especially when considered together, clearly point to the targeted nature of the proposed rules.

33. Third, even if we were to focus solely on the persons affected, it follows from the CJEU case law that an indirect connection to the possible crimes may suffice.[83] It is essential to take account of also this aspect in the analysis. The requirement of a 'connection' should not be taken to mean that something akin to an actual *suspicion* in respect of each person concerned is required. Besides seeming not feasible in practice, the case law does not support such an assumption. The CJEU's own example relating to the retention of personal data of persons present in certain geographical spaces, including those involving a '*very high volume of visitors*',[84] illustrates that such an indirect connection could be a rather loose one.

[80] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117. See also C-293/12 and C-594/12, *Digital Rights Ireland*, para. 27; C-203/15 and C-698/15, *Tele2*, para. 99.
[81] C-793/19 and C-794/19, *SpaceNet*, para. 75.
[82] C-793/19 and C-794/19, *SpaceNet*, para. 112.
[83] C-793/19 and C-794/19, *SpaceNet*, para. 105.
[84] C-793/19 and C-794/19, *SpaceNet*, para. 110.

34. To be more concrete, when it comes to the geographical space at which targeted measures may *inter alia* focus, the CJEU gives the example of an airport.[85] Major airports tend to handle millions, if not tens of millions of passengers per year each. Cumulatively, the number of persons affected is logically much greater still. This shows that, whilst any measures entailing an interference should always be as targeted as possible, it is not excluded that they affect large parts of the EU population.

35. If that can hold true for a *geographical* space, it can in principle also hold true for a digital space, such as a specific online service or a part or component thereof. That is especially so if – as in this case – the measures are justified by the need to effectively tackle extremely serious crimes and fundamental rights' violations, multiple factors ensure the targeted nature of the measures, and adequate limits and safeguards are provided for. Thus, there are in this case objective criteria that establish a connection between the processing of the personal data concerned and the objective pursued.[86]

36. Finally, there is no reason to consider that the need for a connection should be appreciated in a fundamentally different manner, depending on whether the personal data at issue concerns metadata or content data. The case law available to date simply does not offer any support for an argument to that effect.

**Essence of the rights**

37. Pursuant to Article 52(1) Charter, if a limitation on the exercise of fundamental rights compromises the essence of those rights, the measures in question would violate the Charter *per se*, that is, irrespective of any proportionality assessment. In the view of the Commission services, there is however no reason to believe that this would be the case here or that serious risks in this respect would exist.

38. First of all, that it is true that the CJEU has in certain cases alluded to the sensitivity of content data, which is indeed affected to some extent by the proposed measures.[87] However, this was done in connection to measures that are general and indiscriminate in

[85] C-793/19 and C-794/19, *SpaceNet*, para. 108.
[86] E.g. C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 133; C-817/19, *Ligue des droits humains*, para. 118 (both with further references).
[87] E.g. CJEU Case C-362/14, *Schrems,* ECLI:EU:C:2015:650, para. 94.

nature. As explained above, that is not the case here. The proposed measures are targeted in nature. By extension, there is no question under the proposed Regulation of giving certain private parties or public authorities access, on a generalised basis, to the content of electronic communications.

39. Furthermore, the approach whereby such a fundamental distinction is drawn between interferences involving metadata and content data finds no support in the case law. For instance, in *La Quadrature du Net* the CJEU held that information derived from metadata can be '*no less sensitive having regard to the right of privacy, than the actual content of communications*'.[88] Thus, whilst the nature of the personal data is not irrelevant, the principal question is what is *done* with the data.[89]

40. The case law also suggests that it is not so much the interference with the content of communications as such that may be problematic, but rather whether it '*permit[s] the acquisition of knowledge of the content*' of the communications.[90] Given especially the technology and indicators to be used under the proposed Regulation,[91] no such knowledge of the content could be acquired, certainly not on a generalised basis.

41. It should also be noted that in other case law the CJEU has applied different standards. In *Ligue des droits humains*, it has for instance held that measures that might reveal very specific information on the private lives of individuals did not affect the essence of the fundamental rights at issue. That was because the information in question, having regard to the limits and safeguards enacted, did not allow for '*a full overview*' of those private lives.[92] Nothing even resembling a full overview could be obtained through the proposed detection orders.

42. Finally, once more, regard should be had to the specifics of the case at hand. As mentioned, the proposed Regulation aims to tackle certain specific forms of extremely serious criminal offences and violations of children's fundamental rights carried out

[88] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 117 (with further references; emphasis added).
[89] Note also that the system established under the national law at issue in -511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 172-180 was not deemed to violate the essence of the fundamental rights at stake.
[90] C-293/12 and C-594/12, *Digital Rights Ireland*, para. 39 (emphasis added).
[91] See in particular Art. 10(3)(b) proposed Regulation.
[92] C-817/19, *Ligue des droits humains*, para. 120 (emphasis added).

*online*. This is yet another important difference with the data retention case law, which mostly seeks to contribute to tackling criminal activities and activities entailing threats to national security that are carried out *offline* and that could, generally speaking, therefore also be tackled through other means.[93] As explained above, the particular criminal offences at issue are different even from must other crimes or otherwise unlawful activities committed online.

43. As noted, simply put, in the case at hand, the content is the crime.

44. Where that is so, the measures taken must necessarily affect the content, at least to some extent, for them to be effective. It is likely for this reason that the CJEU has deemed measures of this kind acceptable and even necessary in its case law on illegal online content, for instance to tackle online copyright infringement[94] and online defamation.[95] There is no reason to think that this would be fundamentally different for the measures contained in the proposed Regulation.[96] Arguably rather the contrary, having regard to the extremely serious nature and consequences of the crimes at issue, the likelihood of the crimes being carried out in a covert manner, as well as the expansive set of limits and safeguards provided for. Thus, in addition to the nature of the personal data at issue and the question what is done with the data, the questions *why* and *how* it is done are relevant too.

45. In the light of the above, the Commission services acknowledge that interferences involving the content of communications tend to be sensitive and intrusive. A strong justification and adequate limits and safeguards are therefore required. However, the available case law, properly assessed, provides no ground to conclude that, in a situation such as the one at issue, the fact that content data is processed affects the essence of the fundamental rights at stake and is therefore precluded *per se*.

**Proportionality**

[93] Cf. e.g. C-793/19 and C-794/19, *SpaceNet*, para. 96.
[94] C-401/19, *Poland v. EP and Council*.
[95] CJEU Case C-18/18, *Facebook Ireland*, ECLI:EU:C:2019:821.
[96] Note that whereas the case law cited deals essentially with hosting services (that is, services turning around the online storage of third-party information), such services do not necessarily involve information that is publicly available; they can also involve communications of an in principle 'private' nature. Hosting services and interpersonal communications services are not mutually exclusive legal concepts.

46. The fourth and last key issue to be addressed relates to the proportionality assessment required under Article 52(1) Charter. In practice, this is often the central element in the review conducted by the CJEU.

47. The Commission services are of the view that there are numerous elements that, especially when considered in their totality, likely justify the conclusion that the proposed system of detection orders is proportionate.

48. As a first point, it is important to recall, once more, that the proposed detection orders do not entail processing that is general and indiscriminate in nature, within the meaning of the CJEU's case law available to date. Any proportionality assessment based on the premise that they are, therefore does not seem correct.

49. In addition, it is important to distinguish between the retention generally at issue in the data retention case law, the analysis required under the aforementioned particular national legal system at issue in some parts of the *La Quadrature du Net* judgment, and the detection actually at issue in the case at hand. It goes without saying that precisely identifying the nature of the activities causing the interference is of great importance when assessing their proportionality. That means that any conclusions articulated by the CJEU in cases involving the former two types of processing cannot simply be applied one-to-one to the activities at issue here.

50. Furthermore, proportionality is essentially about the relationship between the means employed to achieve the objective pursued. It is generally recognised that combating child sexual abuse is an objective of general interest within the meaning of Article 52(1) Charter. Moreover, the fact that, as has been seen, the crimes and violations of the fundamental rights of children at issue are extremely serious, and that relevant public authorities are under a positive obligation to act in this respect, is of crucial importance precisely on this point. These circumstances, which are specific to the present case, should be placed at the very heart of the proportionality assessment.

51. It may be true that the CJEU has held that such positive obligations cannot justify the imposition of *general and indiscriminate* obligations to *retain* personal data of *practically the entire population*, and also that only the purpose of safeguarding *national*

*security* and not tackling *serious crime* are able to justify those kinds of measures.[97] However, that does not mean that these positive obligations, as well as the other specific circumstances mentioned, are to be ignored when assessing the *proportionality* of *targeted* measures for the *detection* of the criminal offences at issue in the present case.

52. Far from it. In fact, ignoring them would go against two considerations that are central to much of the case law. Namely, firstly and most generally, that in situations like these, where several fundamental rights conflict with each other, a fair balance must be struck between them.[98] And secondly and more specifically, that the more serious the objectives pursued by the measures entailing an interference are, the more serious the interferences they can justify, and *vice versa*.[99] The extremely serious nature of the crimes and the violations of children's fundamental rights at issue are therefore highly relevant when assessing the proportionality of the proposed rules.

53. In line with what has been said above, interferences with the content of communications may be sensitive, but it does not follow that they are necessarily disproportionate. Particularly not where, as in the present case, the interferences occur with the objective of tackling certain specific, extremely serious criminal offences and violations of the fundamental rights of children, which – as was noted earlier – by virtue of their nature can only be effectively tackled in that manner.

54. In the data retention case law, the CJEU has accepted that the fact that a particular measure may be the only means of effectively tackling certain crimes can mean that it is compatible with the Charter, including as a matter of proportionality.[100] That is so even when the measure constitutes a serious interference with fundamental rights.[101] That decision by the CJEU may have related to intrinsically less sensitive personal data (namely source IP addresses), but that is counterbalanced by the fact that that data is

[97] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 145; C-793/19 and C-794/19, *SpaceNet*, para. 92-94.
[98] E.g. C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 127.
[99] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 131; C-140/20, *Commissioner of An Garda*, para. 53. See also CJEU C-207/16, *Ministerio Fiscal*, ECLI:EU:C:2018:788, para. 55; C-817/19, *Ligue des droits humains*, para. 116.
[100] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 154.
[101] C-511/18, C-512/18 and C-520/18, *La Quadrature du Net*, para. 153.

retained in a general and indiscriminate matter, which is inherently more intrusive than targeted detection. The latter aspect should not be ignored. That argues in favour of taking account of this circumstance also in this case.

55. Precisely on this point – that is, the '*risk of systemic impunity for offences committed exclusively online*' – the data retention case law may be subject to further refinement.[102]

56. Finally, it is settled case law that, in situations like the present one, account must be taken of the system in its entirety, in particular the applicable limits and safeguards.[103] Therefore, when conducting the proportionality assessment, it is imperative that account is taken of the extensive system of limits and safeguards that the proposed Regulation would establish for the issuance and execution of detection orders. As observed earlier, these safeguards include the following: issuance by a court or independent administrative authority based on a case-by-case balancing exercise; involvement and oversight by other independent public authorities at all stages; prior risk assessment and mitigation; only issued in case of an objectively evidenced significant risk of child sexual abuse, graduated in function of the degree of intrusiveness; mandatory targeting; strict limits in time; regular reporting and review; effective redress and complaint-handling; information provision to users; purpose limitation and internal oversight and controls; specific requirements regarding the technology to be used; detailed safeguards regarding the indicators to be used; and safeguards stemming from Commission guidance.

**Conclusion**

57. In conclusion, the system allowing for the issuance, under certain conditions, of detection orders to be employed in respect of interpersonal communication services contained in the proposed Regulation is novel and relates to a complex and sensitive area of law. Questions as to the compatibility with the Charter therefore arise and cannot be answered with absolute certainty. However, the Commission services consider that the proposed rules and the case law available to date, seen in their entirety and properly construed, provide no reasons to conclude that on this point the proposed Regulation is incompatible with the Charter.

[102] See Opinion AG Szpunar, Case C-470/21, *HADOPI*, para. 68-88.
[103] See e.g. C-401/19, *Poland v. EP and Council*, para. 82-98.