Prevention and combating CSA: a path toward a privacy consensus

23 April 2024

Mikołaj Barczentewicz[1]

Jan Bednarski[2]

Michał Czarnuch[3]

Legal opinion commissioned by DOT Europe. This opinion presents the views of the authors and does not necessarily represent the position of DOT Europe or of its members.

1. EXECUTIVE SUMMARY

- **Purpose and scope**
  - This opinion analyses the Child Sexual Abuse (CSA) Regulation Proposal's[4] implications for interpersonal communications services (ICS), focusing on alignment with the Charter of Fundamental Rights and overall effectiveness. Our analysis covers both the European Commission's initial Proposal and the LIBE Report,[5] and seeks to provide an analysis how to enhance the Proposal's efficacy by enabling proactive CSA prevention and combating by ICS providers, while ensuring conformity with the Charter (Section 3.1).
- **Main conclusions**
  - The CSA Proposal can be significantly improved to enable proactive CSA prevention and combating by ICS providers while ensuring conformity with the Charter.

---

[1] Associate Professor of Law, University of Surrey School of Law; Research Associate, University of Oxford; Senior Scholar, International Center for Law & Economics.
[2] Associate, Rymarz Zdort Maruta law firm.
[3] Partner, Rymarz Zdort Maruta law firm.
[4] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 11 May 2022, COM(2022) 209 final (CSA Proposal).
[5] Committee on Civil Liberties, Justice and Home Affairs (LIBE), Report of 16 November 2023 on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (LIBE Report).

RYMARZ ZDORT MARUTA
ul. Prosta 18
00-850 Warsaw
+48 22 520 4000
www.rzmlaw.com

- Our key recommendations include introducing enhanced risk mitigation measures and adopting a layered approach. The layered approach would allow for a proportionate gradation of intrusiveness and safeguards. With appropriate conditions, voluntary CSA detection could be a part of this solution.
- We also propose an alternative that would address only some concerns: to grant ICS providers a right to request the initiation of mandatory detection orders procedures.
- These solutions aim to leverage the unique capabilities of ICS providers and provide effective alternatives to mandatory detection orders, ultimately strengthening the Proposal's prevention framework and compatibility with fundamental rights.

- **Background and context**
  - Until late 2020, ICS providers relied on existing legal frameworks like the GDPR[6] to process data for CSA prevention and detection. The expanded scope of the ePrivacy Directive[7] then necessitated a derogation to provide legal certainty for uninterrupted CSA prevention and detection activities, leading to the Interim Regulation[8] (Section 3.2).
  - The Interim Regulation, with its initial sunset clause set for 3 August 2024, currently permits ICS providers to detect, remove and report CSA material and solicitation. Its sunset clause is now extended until 3 April 2026 due to the anticipated delay in adopting a new CSA framework. The scope of the Interim Regulation is limited, covering detection, removal, and reporting without fully addressing CSA prevention through risk mitigation measures, thereby being partially hindered by the ePrivacy Directive (Section 3.3).
- **Key features of the CSA Proposal** (Section 3.4)
  - Introduces a structured approach transitioning from voluntary to mandatory CSA mitigation and detection by service providers.
  - Emphasizes flexibility for providers in selecting prevention and detection measures.
  - Does not permit voluntary processing of interpersonal communications or related traffic data for CSA prevention or detection, given the prohibitions in the ePrivacy Directive.
- **Concerns regarding compatibility with the Charter of Fundamental Rights** (section 4)
  - The Proposal's compatibility with the Charter has been questioned, particularly the proportionality of restrictions on privacy and data protection rights.
  - Key issues include implications for end-to-end encryption (E2EE), clarity on substantive limitations of fundamental rights interferences, and the degree of interference.
  - The authors of this paper are concerned with the privacy implications that detection within E2EE spaces may pose, and thus welcome the LIBE Report's amendments which remove E2EE services from the scope of detection orders. (Section 4.1).

---

[6] Regulation 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.

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[8] Regulation 2021/1232/EU of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse.

- We point out that the distinction between known/new CSAM and solicitation is crucial, with concerns about the accuracy of detection technologies for new CSAM and solicitation (section 4.4).
- While we recognize that mandatory detection orders are designed in the Proposal as a measure of last resort, we believe the current approach overlooks less intrusive alternatives that could reduce the need for more intrusive mandatory detection orders (section 4.5).

- **Recommendations to leverage voluntary efforts of ICS providers** (section 5)
  - A shift from voluntary to mandatory efforts will limit proactive measures by ICS providers, despite their unique insights and capabilities. We also highlight two additional reasons that make voluntary efforts both desirable and proportionate for ICS providers.:
    - Avoiding potential delays or inaction by Coordinating Authorities in initiating detection order procedures (section 5.1.1).
    - Enabling effective CSA prevention measures, not necessarily involving detection, that are currently restricted by the ePrivacy Directive (section 5.1.2).
  - Proposed solutions:
    - Introduce 'enhanced' risk mitigation measures with a derogation from the ePrivacy Directive, subject to oversight by Coordinating Authorities and Data Protection Authorities (section 5.2.1).
    - Adopt a layered approach with gradation of intrusiveness and safeguards for enhanced mitigation measures. Procedural safeguards for content-based measures could include prior and fast-tracked approvals by an authority, with judicial permission for the most intrusive measures like CSA detection (section 5.2.2).
    - An alternative that would address only some concerns would be to grant ICS providers a right to request initiation of detection order procedures, with enforceability subject to judicial review (section 5.2.3).

2. TABLE OF CONTENTS

3. INTRODUCTION

3.1. The scope of this opinion

This opinion examines how the proposed Child Sexual Abuse (CSA) Regulation[9] would impact interpersonal communications services (ICS), considering both the European Commission's original Proposal and the LIBE Report.[10] We assess the Proposal's conformity with the Charter of Fundamental Rights and its overall effectiveness. Our analysis aims to provide recommendations on enhancing the Proposal's efficacy by enabling proactive CSA prevention and combating by ICS providers, while ensuring alignment with the Charter.

3.2. The Interim Regulation and the need for derogation from the ePrivacy Directive

Until late 2020, interpersonal communications services (ICS) providers had been allowed to take measures to prevent and combat child sexual abuse (CSA) on their services while complying with generally applicable legal rules, like the General Data Protection Regulation (GDPR).[11] However, at that time, the scope of the ePrivacy Directive[12] was extended to ICS.[13] The ePrivacy Directive protects the confidentiality of communications by prohibiting certain activities otherwise allowed under EU law, including the GDPR. Thus, without an intervention by the EU legislators, ICS providers' CSA combating activities, including the voluntary detection of CSA, would have been largely prohibited by the ePrivacy Directive.[14] To avoid that, the Interim Regulation was adopted.[15]

The Interim Regulation permits ICS providers to detect child sexual abuse material (CSAM) and solicitation of children in their services and to report both to law enforcement authorities and to organisations acting in the public interest against CSA. The Interim Regulation contains a sunset clause and is meant to apply only until 3 August 2024. Initially, in the

[9] See n 4.
[10] See n 5.
[11] See n 6.
[12] See n 7.
[13] This change came due to Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.
[14] The ePrivacy Directive permits Member States to adopt legislative measures to restrict the scope of its prohibitions, but leaving this to the Member States would have negatively affected the internal market due to lack of harmonization (see Recital 13 of the ePrivacy Directive).
[15] See n 8.

Proposal for a CSA Regulation, the European Commission proposed to replace the Interim Regulation with a new framework, but it became clear that the Proposal is unlikely be adopted in time. Hence, the Commission proposed to amend the Interim Regulation by extending its application to 3 August 2026.[16] The negotiators from the Parliament and the Council agreed to extend it to 3 April 2026.[17]

3.3. Limitations of the Interim Regulation

Aside from being limited in time, the Interim Regulation is also significantly limited in scope. It allows for detection and reporting of CSAM and solicitation of children, but does not permit some potentially effective CSA mitigation measures that do not involve detection. As a result, such mitigation measures are currently significantly hindered in the EU by the ePrivacy Directive. In other words, while the Interim Regulation contributes to combating CSAM by allowing its detection, it does not fully enable CSA prevention through risk mitigation measures that do not involve detection.

3.4. The CSA Proposal

For the purposes of our opinion, the key features of the European Commission's Proposal for a CSA Regulation are its (1) CSA mitigation and detection framework, (2) limited provision for voluntary efforts of service providers, and (3) concern with CSA prevention. The LIBE Report shares those general features.

Regarding the first two points, the CSA Proposal shifts the balance from voluntary efforts under the Interim Regulation to a mandatory system. Even though CSA prevention and combating efforts are meant to be in principle mandatory, the Proposal acknowledges the need for flexibility in the choice of specific measures by service providers.

In a departure from the Interim Regulation, the Proposal does not allow ICS providers to voluntarily process any communications or related traffic data for detection purposes. Moreover, the Proposal does not give ICS providers even a right to request the initiation of the procedure that could lead to the making of a detection order (Article 7).

The obligations of service providers to prevent and combat online CSA are included in Chapter II of the Proposal. They include obligations for: risk assessment and mitigation (section 1), detection (section 2), reporting (section 3), removal (section 4), and blocking (section 5). In this opinion, we focus on mitigation and detection obligations.

Under the Proposal, it would be up to the providers to choose what mitigation measures to adopt and which detection technologies to use. This flexibility is limited by the general rules set in the Proposal setting out the requirements for mitigation measures (Article 4) and for detection technologies (Article 10), as well as by potential future guidelines (e.g., Article 11). Regarding mitigation measures, the flexibility may also be limited by individual decisions of the relevant Coordinating Authorities (Article 7(4)).

In the Commission's Proposal, mitigation measures are meant to include adapting the provider's content moderation, recommender systems, decision-making processes, service operation and functionalities, or terms and conditions (Article 4). This would be done through appropriate technical and operational measures and staffing. Mitigation measures are also

---

[16] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2021/1232 of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC for the purpose of combating online child sexual abuse, 30 November 2023, COM(2023) 777 final.

[17] 'Child sexual abuse online: agreement on extending current rules until April 2026' (15 February 2024) < https://www.europarl.europa.eu/news/en/press-room/20240212IPR17636/child-sexual-abuse-online-agreement-on-extending-current-rules-until-april-2026 >.

meant to include reinforcing the provider's internal processes or supervision of the service's functioning.

The LIBE Report aimed to make the definition of mitigation measures more concrete by adding specific examples like 'limiting users, by default, to directly share unsolicited content with other users directly, in particular through private communications' (Amendment 131). The LIBE Report also proposed to stress that the 'decision as to the choice of mitigation measures shall remain with the provider' (Amendment 129; see also Recital 17 of the original Proposal). The key limitation of mitigation measures is that they cannot involve the processing of communications or related traffic data in accordance with the prohibition from the ePrivacy Directive. We consider this issue in Section 5.1.2.

In the Proposal, mandatory detection is understood as 'installing and operating technologies to detect the dissemination of known or new child sexual abuse material or the solicitation of children' (Article 10(1)). The LIBE Report proposes to modify this description by specifying that the technologies are 'available, secure and privacy-friendly,' as well as by removing the reference to solicitation (Amendment 209). Like the Interim Regulation, the Proposal would permit some processing of communications or related traffic data, otherwise prohibited by the ePrivacy Directive, for the purposes of CSA detection, reporting, and removal (Article 1(4), LIBE amendment 85). ICS providers would be obligated to implement detection through detection orders (Article 7) and would not be allowed to do so voluntarily. Detection orders would be drafted by the national Coordinating Authority and issued by a designated judicial authority or independent administrative authority. The LIBE Report proposes to limit this to just judicial authorities (Amendment 168). The orders would be addressed to service providers. Whether to request the issuance of a detection order would be in the relevant Coordinating Authority's discretion, creating the possibility that such authorities would fail to act in a timely manner or at all. There would be no right for service providers to request the initiation of the procedure for the issuance of a detection order.

As we discuss in section 5.1.2, there is a significant gap in the Proposal's approach to prevention in ICS, which risks undermining the overall prevention framework. Although the Proposal expressly aims to address CSA prevention, not just combatting CSA, it lacks any derogation from the ePrivacy Directive for CSA prevention measures that do not involve CSA detection. This is despite prevention being stressed in the Proposal's title, which refers to 'laying down rules to prevent and combat child sexual abuse,' whereas the Interim Regulation's title only referred to combating CSA.

4. LAWFULNESS OF DATA PROCESSING UNDER THE CSA PROPOSAL

The debate about the lawfulness of processing interpersonal communications and related traffic data under the Interim Regulation and the CSA Proposal has often centred around the need for a 'legal basis.' However, the term 'legal basis' can be ambiguous, as it may refer to at least four different concepts:

(1) a 'legal basis' for personal data processing required by Article 6 of the GDPR;

(2) an exemption from the prohibitions on the processing of communications and related traffic data, including non-personal data, in the ePrivacy Directive;

(3) compatibility of legal rules permitting or mandating data processing with the Charter of Fundamental Rights;

(4) a general 'legal basis' under the EU Treaties for the enactment of legislation like the CSA Proposal (the Commission relied on Article 114 of the Treaty on the Functioning of the European Union (TFEU)).

In this opinion, we focus on currently the most contentious aspects, related to the ePrivacy Directive and to the Charter of Fundamental Rights.

The GDPR. However, we also note the need for the law to address more directly the first issue, i.e., which of the 'legal bases' in Article 6 GDPR applies. The Proposal achieves that by imposing legal obligations on ICS providers, and thus providing them with a legal ground referred to in Article 6(1)(c) GDPR.[18]

The ePrivacy Directive. Regarding the ePrivacy Directive, as an ordinary piece of secondary EU legislation, it does not bind future EU laws such as the proposed CSA regulation. The EU legislature has the authority to enact any limitations or derogations from the ePrivacy Directive that it deems appropriate, so long as they are compatible with EU primary law, especially the Charter.[19] In other words, the Directive itself does not limit what can be included in a new CSA Regulation. However, in the absence of rules that limit or derogate from it (such as the Interim Regulation), the Directive significantly restricts what ICS providers can do to prevent and combat CSA. Therefore, to ensure the effectiveness of the CSA prevention and combating framework, careful consideration must be given to the relationship between CSA-specific rules and the ePrivacy Directive, to avoid the latter unduly undermining the former. As argued below, the Proposal does not currently provide a similar derogation needed for voluntary CSA detection as the Interim Regulation does, nor does it enable providers to implement additional prevention measures that do not involve CSA detection (Section 5.1.2), thus potentially limiting the Proposal's effectiveness, especially for CSA prevention.

Notably, unlike the Interim Regulation, the Proposal does not expressly *derogate* from the ePrivacy Directive but it purports to limit 'the exercise of the right and obligations provided for in 5(1) and (3) and Article 6(1)' of the Directive. Shifting from a derogation to a 'limitation of the exercise of rights' is not required by EU primary law and may be inadvisable, as it risks creating significant interpretative difficulties and uncertainty for authorities, courts, and service providers. The EU legislature has the freedom to enact a clear derogation, thereby clarifying that only EU primary law, including the Charter, is dispositive for the interpretation of the future CSA Regulation.

The Charter of Fundamental Rights. There is no question that a law that mandates the processing of user data for the purposes of CSA mitigation or detection is likely to interfere with some of the rights protected by the Charter of Fundamental Rights, especially the rights to privacy and to the protection of personal data (Articles 7 and 8 of the Charter). However, interferences with fundamental rights are not by themselves unlawful and they may be justified in accordance with Article 52(1) of the Charter.

The Commission's Proposal has been criticized for violating Article 52(1) of the Charter by imposing disproportionate restrictions on fundamental rights protected by the Charter, primarily the rights to privacy and the protection of personal data. Some critics argue that the Proposal may even compromise the essence of certain rights. [20] The criticism is mainly directed at the proposed mechanism of mandatory detection orders.

---

[18] COM(2022) 209 final, 4.

[19] In particular, the EU legislature is not bound by Article 15(1) of the ePrivacy Directive, which is directed to Member States.

[20] EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, issued on 28 July 2022 (EDPB-EDPS Opinion 4/2022); Opinion of the Council Legal Service from 26 April 2023 on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse (CLS Opinion); Christopher Vajda, 'Legal opinion commissioned by MEP Patrick Breyer on the 2022 Proposal for an EU Regulation laying down rules to prevent and combat child sexual abuse', 19 October 2023 (Vajda Opinion).

It has been argued that the originally proposed mechanism of detection orders is not sufficiently limited to ensure that it would be applied in a proportionate way, or even to ensure that it would not lead to compromises of the essence of fundamental rights. In particular, the concern was that the Proposal did not ensure that detection orders would be targeted, as opposed to being general and indiscriminate, in the meaning of CJEU case law.[21]

In general, we agree with the Commission that the CJEU has not ruled on measures exactly like the ones proposed in the Proposal, so there is some uncertainty on how the Court would approach such legislation.[22] Nevertheless, certain features of the Commission's Proposal raise doubts about their Charter compatibility. However, we believe those concerns can be addressed by introducing additional amendments in the final text.

4.1. End-to-end encryption

The authors who evaluated the Proposal noted that, unlike the Interim Regulation, the Proposal appears to at least allow that compliance with it may involve breaking end-to-end encryption (E2EE). This has been seen, we believe justifiably, likely to be a significant limitation of fundamental rights, including the rights to privacy and to the protection of personal data. The EDPB-EDPS Joint Opinion rightly pointed out security risk related to both client-side and server-side scanning and highlighted the chilling effect that undermining E2EE by the Proposal could have on freedom of expression and the legitimate private use of electronic communication services.[23] Similarly, the Council Legal Service noted that weakening E2EE would create stronger interference with fundamental rights.[24]

Furthermore, in the recent case of *Podchasov v. Russia*, the European Court of Human Rights (ECtHR) acknowledged the importance of preserving E2EE integrity.[25] The ECtHR accepted that in cases where it is technically impossible to provide authorities with encryption keys associated with specific users, weakening E2EE as a whole would indiscriminately affect all users.[26]

The LIBE Report proposed a solution to this concern, by adding, among other provisions:

> Nothing in this Regulation shall be interpreted as prohibiting, weakening or undermining end-to-end encryption. Providers shall not in particular be prohibited to offer end-to-end encrypted services.[27]

4.2. Clarity on the substantive limitations of interferences with fundamental rights

Insofar as the CSA Proposal interferes with the rights protected by the Charter, the limitations on the exercise of those rights 'must be provided for by the law' (Article 52(1) of the Charter).[28] Both the Commission and the commentators noted that the CJEU allows some flexibility in this respect,[29] not precluding the limitations 'being formulated in terms which are sufficiently open to be able to keep pace with changing circumstances.'[30] Vajda noted:

> On one view, the Regulation could be said to comply the application of this principle as set out in *Poland v Council* on the basis that detection of CSAM is constantly

---

[21] See e.g. C-793/19, SpaceNet, paras. 75, 105-113, 131; C-511/18, La Quadrature du Net, paras. 143-151, 168; C-203/15, Tele2, paras. 105-112.
[22] European Commission, 'May 2023 Non-paper', para. 15.
[23] EDPB-EDPS Opinion 4/2022, paras. 100 - 101. See also Harold Abelson and others, 'Bugs in our Pockets: The Risks of Client-Side Scanning' (2024) 10 Journal of Cybersecurity.
[24] CLS Opinion, para. 51.
[25] *Podchasov v. Russia* App no 33696/19 (ECtHR, 13 February 2024).
[26] *Podchasov v. Russia*, para. 57.
[27] Article 1(3a) proposed in LIBE amendment 83; see also LIBE amendments 9, 26, 168, 216, 265; IMCO amendments 23, 131.
[28] See also European Commission, 'May 2023 Non-paper', paras. 20-25; Vajda Opinion, paras. 63-66.
[29] Id.
[30] Case C-401/19, Poland v Parliament and Council, para. 74.

> evolving in the light of technological developments. On the other hand, the interference with the rights to privacy and data protection in the present case is much more serious than that of the interference with the right to freedom of expression in *Poland v Council*.[31]

Vajda thought that the risk of undermining end-to-end encryption weighs heavily against concluding that the Proposal meets the standard.[32] Hence, removing that risk, as proposed in the LIBE Report, would address Vajda's key argument.

However, even setting aside the issue of encryption, it remains the case that at least the most intrusive measure potentially possible under the CSA Proposal (e.g., a detection order requiring detection based on content of all communication in a very large ICS) could be seen as more serious interference than what the CJEU considered in *Poland v Parliament and Council.* The Commission's own examples of recent legislation that relies on general language in defining the limits of interferences with fundamental rights are the Digital Services Act[33] and the Copyright in the Digital Single Market Directive,[34] neither of which purports to derogate from the rules on the protection of confidentiality of communications.[35]

Given this uncertainty, it is advisable to add more clarity on the substantive limitations of interferences with fundamental rights in the text of the Proposal. This should contribute significantly to reducing the risk of an adverse finding from the CJEU.

One significant way in which the potential scope of detection orders could be made clearer is by making more robust the provision on mitigation measures that ICS providers are obligated and permitted to implement to reduce the risk of CSA in the first place, thereby reducing the need for mandated detection orders at a later stage. The LIBE Report proposed some solutions in this direction.[36] However, as we argue below ('Less intrusive alternatives'), their proposals are insufficient for a different reason, i.e., that they exclude more effective mitigation measures that are less intrusive than a mandatory detection order. We propose other solutions in Section 5.

The chief solution adopted in the LIBE Report was to further specify the conditions for the issuance of a detection order in Article 7 (Amendments 168-169). However, we don't believe that the specific amendments proposed in the LIBE Report are required to ensure conformity with the Charter. Notably, the LIBE solution did not even fully satisfy the EDPB.[37]

4.3. Degree of interference

Even if the legislation *clearly* outlines the limitations on potential interferences, the *degree* of interference may still be disproportionately high when weighed against counterbalancing considerations, potentially leading to a violation of Article 52(1) of the Charter.

The CJEU has imposed particularly strict limits on *general and indiscriminate* data processing for law enforcement purposes, albeit predominantly in a somewhat different context related

---

[31] Vajda Opinion, para. 66.
[32] Id., paras. 66-69.
[33] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act).
[34] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
[35] European Commission, 'May 2023 Non-paper', para. 40.
[36] LIBE amendments 129-151.
[37] EDPB, 'Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse' (13 February 2024) 3. The EDPB expressed doubts that the LIBE Report 'appears ambiguous as to how detection orders should be "targeted" and when "reasonable grounds of suspicion" should be deemed to exist.'

to proactive retention of subscriber and traffic data over a longer period of time.[38] The Proposal states that any measures taken should be 'targeted' (e.g., recitals 2 and 23), and in the case of detection orders, independent authorities would determine whether a measure is sufficiently targeted on a case-by-case basis. Therefore, it is difficult to argue that the text of the Proposal would permit general and indiscriminate data processing. A more natural interpretation of the text is that the authorities applying the rules would only be empowered to mandate targeted data processing.

Nevertheless, there is likely to be uncertainty as to what kind of processing would be 'targeted' (allowed under the Proposal) and what 'general and indiscriminate' (not allowed under the Proposal). The view expressed by the commentators is well-exemplified by Vajda's concern that a detection order

> may well require monitoring the actual content of all electronic communications made by every user of that Provider's electronic communications network, including encrypted communications.[39]

To our knowledge, the Commission did not dispute this interpretation of the Proposal. However, they appear to contest the notion that it would constitute 'general and indiscriminate' data processing, i.e. a situation analogous to the kind of processing the CJEU restricted to the most exceptional circumstances. The Commission emphasized that the proposed rules are intended to be 'targeted, carefully balanced, and proportionate.'[40] Furthermore, they underscored the substantive and procedural safeguards included in the Proposal.[41]

In essence, the Commission seems to argue that Vajda's example could be compatible with Article 52(1) of the Charter, considering the substantive and procedural safeguards in place. If the Court disagrees with this view, it need not invalidate the future regulation. In fact, we see invalidation as unlikely (see below). In such a situation it is more likely that the Court would rule that the regulation must be interpreted in a way that precludes the Commission's reading.

This situation could lead to temporary uncertainty regarding the correct interpretation of the future regulation. There is a risk that some national authorities, including Coordinating Authorities and those designated to issue detection orders, will adopt the Commission's interpretation while others will not. This risk underscores the need to further specify the conditions for imposing measures that interfere with rights, such as those we discuss below in the sections 'Types of CSA' and 'Less intrusive alternatives.'

---

[38] See e.g. C-793/19, SpaceNet, paras. 75, 105-113, 131; C-511/18, La Quadrature du Net, paras. 143-151, 168; C-203/15, Tele2, paras. 105-112. It is true that in *La Quadrature du Net,* the CJEU also considered as 'general and indiscriminate processing' 'automated analysis of traffic and location data' which was 'independent of the subsequent collection of data' (i.e. retention); *La Quadrature du Net*, paras. 172-182; Vajda Opinion, paras. 90-92. However, while the processing in question was independent of the *subsequent* retention of data, it was not independent of the *prior* legally mandated retention—the automated analysis in question was meant to be applied to data already retained under a legal obligation; *La Quadrature du Net*, para 43,

[39] Vajda Opinion, para. 61.

[40] European Commission, 'Non-paper prepared by the Commission services: Balancing the rights of children with users' rights' (16 May 2023) < https://home-affairs.ec.europa.eu/system/files/2023-06/Non-paper%20prepared%20by%20the%20Commission%20services%20on%20balancing%20the%20rights%20of%20children%20with%20users'%20rights_en_0.pdf > ('May 2023 Non-paper'), para. 3.

[41] European Commission, 'Comments of the services of the Commission on some elements of the Joint Opinion of the European Data Protection Supervisor and the European Data Protection Board (EDPS-EDPB) on the proposal for a Regulation laying down rules to prevent and combat child sexual abuse at the request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and the Council Law Enforcement Working Party (LEWP)' (3 May 2023) < https://home-affairs.ec.europa.eu/document/download/05f459f6-7b82-4d01-ac8c-2e263382bd93_nl?filename=Comments%20EDPS-EDPB%20opinion.pdf > ('Comments on the EDPB-EDPS Joint Opinion'), 2-3.

However, we disagree with the stronger claim that the Proposal itself is necessarily incompatible with the Charter due to this uncertainty. Adopting such a standard would likely result in many EU legislative acts being found invalid, which is emphatically not what we observe in CJEU case law. In fact, invalidation is exceptional, and the CJEU typically favours an interpretation that preserves the validity of EU legislative acts.[42] As the CJEU recently reiterated:

> … in accordance with a general principle of interpretation, an EU measure must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter. Thus, if the wording of secondary EU law is open to more than one interpretation, preference should be given to the interpretation which renders the provision consistent with primary law rather than to the interpretation which leads to its being incompatible with that law …[43]

4.4. Types of CSA (known material, new material, solicitation)

The Proposal addresses 'online child sexual abuse,' which is defined in Article 2 as 'the online dissemination of child sexual abuse material and the solicitation of children.' The Proposal further categorizes 'child sexual abuse material' into 'known' and 'new' material. In the Commission's original Proposal, all three categories (known material, new material, and solicitation, also referred to as 'grooming') are subject to risk assessment, mitigation measures, and detection orders. However, the LIBE Report suggests removing solicitation from the scope of detection orders.[44]

As has been noted by the Commission and by the commentators, different technologies and operational measures are likely to be used for the prevention and combating of each of the types of CSA.[45] There is a broad agreement that the available methods to detect known CSAM are highly accurate in the sense of having a very low probability of producing false positives.[46] Moreover, detection of known CSAM typically involves processing only images and videos, which is considered less privacy intrusive.[47] The question of accuracy of the methods to detect new material and solicitation (grooming) is more controversial.[48]

Regarding solicitation, the Explanatory Memorandum to the Proposal stated that '[d]etection technologies have also already acquired a high degree of accuracy, although human oversight and review remain necessary.'[49] However, the assertion that detection of solicitation and unknown CSAM has a 'high degree of accuracy' is disputed.[50]

---

[42] For example, in *Digital Rights Ireland* the Court found that the Directive 2006/24 imposed the kind of measure that the Court found incompatible with the Charter 'without any differentiation, limitation or exception'; Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, para. 56. Whereas in the case of the Proposal, there are limitations and only on a certain interpretation of those limitations the most controversial measures could be taken.
[43] C-401/19 Poland v Parliament and Council, para. 70.
[44] LIBE amendments 168 and 188.
[45] See, e.g., EDPB-EDPS Opinion 4/2022, 21-23; Vajda Opinion, para. 28; European Commission, '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)' (8 June 2023) < https://home-affairs.ec.europa.eu/document/download/df3805f0-60fe-4c9b-96fc-00a0d37a198a_en?filename=Comments%20from%20the%20Commission%20to%20the%20European%20Parliamentary%20Research%20Service%27s%20impact%20assessment_en_0.pdf > ('Response to ECORYS'), 3.
[46] Id.
[47] See, e.g., EDPB-EDPS Opinion 4/2022, para. 69.
[48] Id.
[49] COM(2022) 209 final, 14.
[50] EDPB-EDPS Opinion 4/2022, para. 73; DOT Europe, 'DOT Europe position paper: Regulation laying down rules to prevent and combat child sexual abuse (December 2022)' < https://doteurope.eu/library/ >, 12-13.

Given the significant differences in accuracy between methods used to detect known CSAM versus new CSAM and solicitation, the Proposal should more clearly specify limitations on mandating the detection of unknown CSAM and solicitation compared to known CSAM.

The solution to this concern could involve imposing further safeguards on detection of new CSAM and solicitation, if not removing them entirely from the scope of mandatory detection orders. It may also be advisable to rely more on voluntary efforts of ICS providers, including risk mitigation measures (see Section 4.2), allowing ICS providers to further develop the methods to prevent and combat unknown CSAM and solicitation.

Given that there are significant doubts whether there currently are, or there will be soon, any 'sufficiently reliable' technologies for detection of new CSAM and of solicitation, mandating such measures through detection orders may be disproportionate. The LIBE Report's removal of solicitation from the scope of mandatory detection orders remedies this partially but does not address the analogous question regarding new CSAM.

4.5. Less intrusive alternatives

Article 52(1) of the Charter requires that interferences with fundamental rights be necessary to achieve the intended objective. The Commission argues that the Proposal satisfies this necessity requirement by positioning detection as a measure of 'last resort',[51] stating:

> 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.[52]

However, the Proposal omits some less intrusive measures that could reduce the need for detection orders or at least allow for more limited detection orders. This is not remedied in the LIBE Report. The omission of these less intrusive measures undermines the argument that detection orders are necessary and proportionate.

For example, as we discuss below (Section 5.1.2), due to the lack of a suitable derogation from the ePrivacy Directive, ICS providers would not be able to use non-content data (e.g., metadata, traffic data) for CSA mitigation. With appropriate safeguards, mitigation measures relying on non-content data would be less intrusive than content detection under detection orders. Even if mitigation using non-content data is less effective for some purposes than content detection,[53] it may be sufficiently effective to reduce the risk of CSA use of the service, perhaps even to the extent that would make detection orders inapplicable under the Proposal (i.e., below the level of 'significant risk'). Moreover, non-content data may be available for analysis in end-to-end encrypted services where content data is not available and thus where detection orders may be ineffective (assuming that they would not allow undermining end-to-end encryption).

With appropriate substantive limitations, even the use of communications content data for CSA mitigation could constitute a less intrusive and proportionate alternative to mandatory detection orders. The example we give below (Section 5.2.2) is the use of content data in a way that does not by itself have any adverse consequences for the persons involved. This

---

[51] European Commission, 'Comments on the EDPB-EDPS Joint Opinion', 5.
[52] Id.
[53] Though the differences in effectiveness should not be overstated. For example, in one of the documents the Commission inaccurately presented the results of a Stanford study by summarizing it as having found that 'none of the companies found the detection of CSAM using metadata effective,' whereas the study found that the companies did not consider metadata as 'most useful' (i.e., more useful than automatic content scanning and user reports) for the purpose of CSAM detection, without making any findings on metadata being ineffective in absolute terms; European Commission, 'Response to ECORYS', 5; Riana Pfefferkorn, 'Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers' (Stanford Internet Observatory, 9 September 2021) < https://ssrn.com/abstract=3920031 >.

could be done, for instance, for the purposes of developing CSA prevention measures or for the purpose of assessing the statistical prevalence of CSA use on a service.

5. LEVERAGING VOLUNTARY EFFORTS OF ICS PROVIDERS

As we noted in the Introduction, the Proposal shifts the balance from *voluntary* efforts of ICS providers under the Interim Regulation to a *mandatory* system. Understandably, the EU legislature may prefer a system where the decision to engage in prevention and combating CSA is not left to a free choice of service providers. However, that legislative decision does not require discarding voluntary efforts of service providers. What is more, discarding those efforts risks undermining the effectiveness of the overall framework. Notably, the Proposal's CSA prevention and combating framework puts emphasis on risk assessment conducted by service providers. The Proposal also already recognises the need for giving service providers the flexibility in the choice of technologies and measures for risk mitigation and for detection. Allowing the service providers to play a more proactive role would thus be consistent with the Proposals overall scheme.

5.1. Reasons for broader recognition of voluntary efforts of ICS providers

The general reasons that support giving ICS providers flexibility in the choice of technologies and measures include their first-hand knowledge of the functioning of their services, their likely superior understanding of technology and capacity to experiment with and develop organisational and technological solutions, and their clear interest in preserving their business reputation as well as offering safe services to their users.

However, there are also more specific reasons for a broader recognition of voluntary efforts in the Proposal:

5.1.1. The risk that Coordinating Authorities will not act in a timely manner and in a way that ensures maximum effectiveness of CSA prevention and combating

According to both the Commission's Proposal and the LIBE Report, service providers would be disabled from implementing CSA detection measures prohibited by the ePrivacy Directive until they receive a detection order. Service providers would not even be able to initiate the procedure for the making of such an order. This may mean significant delays or not receiving an order at all due to immaterial reasons, given the lack of any time limits or even an enforceable duty for the relevant Coordinating Authorities to act.[54]

The Proposal appears to be based on an implicit assumption that to the extent any derogations from the ePrivacy Directive will be needed, the Coordinating Authorities will identify such needs on their own and quickly proceed to request detection orders, so that there will be no risk of significant gaps in coverage by CSA combating measures.[55] Given the inevitable administrative limitations, the assumption that no gap would be left is highly doubtful. The broad scope of the ePrivacy Directive's data processing prohibitions could significantly hamper the effectiveness of the overall CSA prevention and combating framework if Coordinating Authorities experience delays or inaction due to administrative limitations such as staffing, expertise, or coordination with third parties.

5.1.2. The need for effective CSA prevention, which may not involve detection

As we noted in the Introduction, the Proposal expressly aims to address not only combating child sexual abuse, but also its prevention. However, neither the Commission's Proposal nor

[54] Under the Proposal, Coordinating Authorities are the only ones competent to request the issuance of a detection order from a judicial authority.

[55] Moreover, that any needed derogations will be covered by detection orders, which is also highly doubtful, especially regarding CSA prevention measures.

the LIBE Report clearly permits ICS providers to implement any CSA prevention measures that do not involve CSA detection but are still covered by the broad scope of the confidentiality-protecting rules from the ePrivacy Directive (Articles 5, 6, and 9). Thus, important risk mitigation measures mandated in the Proposal risk being ineffective if not based on information ICS providers cannot process due to the ePrivacy Directive.

The absence of provisions for such mitigation measures also undermines the argument that detection orders are necessary and proportionate because these measures could potentially serve as less intrusive alternatives. If less intrusive alternatives are possible, but they are not made available, then it is difficult to claim that detection orders will only be applied if truly necessary.

(a) Breadth of the prohibitions on data processing in the ePrivacy Directive

The ePrivacy Directive limits otherwise lawful processing of communications and traffic data by ICS providers in Articles 5, 6, and 9. Article 5(1) protects the confidentiality of communications and related traffic data. Article 5(3) limits storing or accessing information already stored on user devices. Article 6 limits the processing of traffic data, while Article 9 does so for location data other than traffic data.

Both the CJEU and other institutions like the EDPB have interpreted those provisions broadly.[56] For example, the CJEU stressed, that Article 5(1)

> applies to the measures taken by all persons other than users, whether private persons or bodies or State bodies. As confirmed in recital 21 of that directive, the aim of the directive is to prevent unauthorised access to communications, including 'any data related to such communications' in order to protect the confidentiality of electronic communications.[57]

According to the definition in the ePrivacy Directive, 'communication' 'means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service' (Article 2(d)). Recital 15 of the ePrivacy Directive explains that a 'communication' 'may include any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication.' On the other hand, 'traffic data' is defined as potentially including any translation of this communication information by the network over which the communication is transmitted for the purpose of carrying out the transmission.

Due to the broad scope of these prohibitions, an ICS provider is likely to find that nearly all information they could access related to a user falls under one of the ePrivacy Directive's restrictions.

(b) Effective mitigation measures fall under the scope of the ePrivacy Directive

The breadth of the cited provisions of the ePrivacy Directive means that some of the possibly most effective and proportionate CSA prevention measures are currently hampered, if not rendered entirely out of bounds.

Consider the example of a measure aiming to impose additional precautions in situations where one adult is in contact with many minors on an ICS. At first glance, the following mitigation measure specified in the LIBE Report might seem to address this issue:

> limiting users, by default, to establish unsolicited contact with other users directly, in particular through private communications, by asking for user confirmation before

---

[56] See e.g. C-793/19 SpaceNet AG paras. 52–58, C-511/18 La Quadrature du Net para. 117, C-203/15 Tele2 para. 77, C-207/16 Ministerio Fiscal para. 77; EDPB Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive.
[57] C-203/15 Tele2 para. 77.

> allowing an unknown user to communicate and before displaying their communications.[58]

However, within a single ICS, minors may initiate or accept interactions with adults, particularly if the initial interaction began on a different service or in a more public area of the same service. A general limitation suggested in the LIBE Report would not address such cases.

If permitted to use traffic data, including messaging patterns, an ICS provider could implement additional preventative measures. These measures could include limiting an adult user's ability to find minors on other parts of the service, displaying a customized warning to the minor to reconsider the contact, and potentially applying other suitable preventative measures.

The example above illustrates just one of many mitigation measures that could be significantly more effective, or even feasible in the first place, if they were allowed to use the kinds of data processing currently prohibited by the ePrivacy Directive.

Another potential mitigation measure would be for ICS providers to analyse patterns of interactions among users who subscribe to groups or threads with titles or descriptions containing keywords suggestive of CSA interest. Our understanding is that this type of analysis could be conducted without compromising end-to-end encryption of messaging content.

(c) Necessary derogations are absent from the Proposal

The question to what extent the Proposal allows for exceptions to the prohibitions from the ePrivacy Directive is addressed in Article 1(4). As amended in the LIBE Report, this provision states:

> This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC ***with the sole objective of enabling relevant information society services to use specific technologies for the processing of personal and other data to the extent strictly*** necessary ***to detect and report online child sexual abuse and remove child sexual abuse material from their services*** for the execution of the detection orders issued in accordance with Section 2 of Chapter 1 of this Regulation.

The second part of the emphasised text replaced the phrase 'insofar as' in the original Proposal.

As we noted earlier, unlike the Interim Regulation, the Proposal does not expressly *derogate* from the ePrivacy Directive but it purports to 'limit the exercise of the right and obligations provided for in 5(1) and (3) and Article 6(1)' of the Directive. This departure from the Interim Regulation may be inadvisable because it risks creating significant interpretative difficulties and uncertainty for the authorities, the courts, and the service providers.

Like the Interim Regulation, Article 1(4) of the Proposal allows for exceptions to the prohibitions from the ePrivacy Directive solely to the extent strictly necessary 'to detect and report' (or simply 'for the execution of detection orders,' in the original Proposal[59]). There is no mention of the purpose of CSA prevention and no mention of applicability of the derogation to mitigation measures under Article 4 of the Proposal.

---

[58] LIBE amendment 131 to Article 4(1)(aa) (new).

[59] Moreover, Article 10 of the Commission's Proposal, which specified what detection orders are, provided in its paragraph 4(a) that the provider shall 'take all the necessary measures to ensure that the technologies and indicators, as well as the processing of personal data and other data in connection thereto, are used *for the sole purpose of detecting* …' (emphasis added).

Considering the tendency to interpret the prohibition from the ePrivacy Directive broadly and any exceptions narrowly, it may be difficult to argue that detection orders would permit the preventative mitigation measures discussed above. At the very least this is significantly unclear and risks divergent interpretations.

5.2. Potential solutions and their conformity with the Charter

We now turn to potential solutions aimed at addressing the concerns raised above. The second solution introducing 'layers' is a variant of the first solution introducing 'enhanced' risk mitigation measures that would benefit from a derogation from the ePrivacy Directive. The third solution, addressing the concern about inaction of Coordinating Authorities, is a more limited self-standing option, and does not address the other concerns.

5.2.1. Enhanced risk mitigation measures

All the reasons presented above could be addressed by extending the derogation, or at least elements of it, from the ePrivacy Directive to risk mitigation measures in Article 4 of the Proposal. This extension would allow ICS providers to process communications data (including content data) and related traffic data to minimize the risk of CSA use of their services, based on risk assessments conducted under Article 3. Such risk mitigation measures could span the full scope of CSA prevention and combating measures, including CSA detection.

This would not be a mere continuation of the current situation under the Interim Regulation. The ICS providers, and the risk assessments they conduct, would additionally be subject to the oversight of the Coordinating Authorities, in accordance with Article 5.

Like under the Interim Regulation, measures involving data processing covered by the GDPR would continue to be under the oversight of relevant Data Protection Authorities.

This solution would address the risk of inaction or insufficient actions from the Coordinating Authorities. ICS providers would be allowed to begin or continue existing mitigation measures without needing a prior decision from a Coordinating Authority, subject to stronger safeguards than those currently under the Interim Regulation.

It would also address the concern about ICS providers being allowed to use effective prevention (mitigation) measures that do not involve detection. This is because Articles 3 and 4 of the Proposal refer more broadly to minimising the risk of CSA use of services.

Compatibility with the Charter. Even though it is hard to predict how the CJEU would approach such a situation, the simple solution of extending the derogation from the ePrivacy Directive to Article 4 of the Proposal may raise concerns as to conformity with Article 52(1) of the Charter due to insufficient safeguards. This risk could be reduced by augmenting the procedural and substantive safeguards for 'enhanced' risk mitigation measures, i.e. those benefiting from an ePrivacy derogation.

The additional safeguards could include reference to or copying the substantive limitations that apply to detection orders (Articles 7 and 10). They could also include the requirement to obtain a prior permission of the Coordinating Authority, while requiring the Authority to issue a reasoned decision in a limited time and subjecting the Authority's decision to effective redress.

The risk of a finding of invalidity under the Charter could be further reduced by adopting a layered solution that we discuss in the next subsection.

5.2.2. A layered solution with a gradation of intrusiveness and of safeguards

The Proposal involves a wide range of information types and technological and organizational measures, which adds complexity that may not be readily apparent. The legislative approach taken in the Proposal is to employ more general rules to encompass a broader spectrum of situations. However, this approach makes it more challenging for stakeholders to ascertain the probable impact of the law and the boundaries of permissible interferences with Charter-protected rights. Consequently, there is an increased likelihood that the framework could be deemed in breach of Article 52(1) of the Charter. Conversely, overly casuistic legislation is also undesirable, as it may compromise the effectiveness (due to inflexible detailed rules) and clarity (excessive text may be more difficult to comprehend) of the law.

The measures prescribed by the Proposal's rules would impact several fundamental rights, notably the right to privacy, the right to personal data protection, freedom of expression and information, and the freedom to conduct business. These measures would, to varying degrees, both safeguard and restrict the exercise of these rights. In some cases, they may simultaneously protect and limit the same right, such as the privacy rights of minor ICS users. Given this complexity, we believe a more 'layered' approach is preferable, seeking to strike a balance between the concerns surrounding the generality and predictability of the legislative framework.

Thus, enhanced mitigation measures could be expressly divided in several ‘layers’ or ‘steps,’ with a gradation of intrusiveness which would come with a gradation of safeguards. The ICS providers may be allowed or required to use some or all of them, depending on the risk assessment of their service.

The layers could include, for example, measures that:

1. Use only non-content data (metadata, traffic data) and have limited consequences for users' experience of a service. In the latter respect, they could be limited to minimal ‘nudging’ effects.

As noted earlier, ICS providers could rely on information about patterns of interactions among users who subscribe to 'groups' or 'threads' with certain keywords in their titles or descriptions that indicate an interest in CSA. This, we understand, is possible without interfering with end-to-end encryption of messaging. Based on this information, providers could improve their CSA prevention tools or include 'nudges' in user interfaces that do not block functionality. For example, messages from a flagged user account could be directed into a separate 'inbox' for other users, similar to how spam emails are handled.

By not severely limiting the service's functionality, such a measure would be unlikely to raise serious concerns under Article 11 of the Charter,[60] as users would not be restricted in their communication methods, and there would be a low risk of a 'chilling effect.'

2. Use only non-content data (metadata, traffic data) but might be used to ground more than minimal effects on what a user can do with the service, including ‘hard’ limits on contacts with other users (within a framework allowing for recourse, as appropriate and required by EU law like the DSA[61]).

3. Use content data, but in a way that does not by itself have any adverse consequences for the persons involved. For example, only for the purposes of developing CSA prevention measures or for the purpose of assessing the statistical prevalence of CSA use on a service.

---

[60] Compare e.g. with C-401/19 Poland v Parliament and Council, paras. 84-86. See also Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, para. 28.
[61] Regulation 2022/2065.

4. Use content data for the purpose of CSA detection and reporting.

Gradation of safeguards. The first kind of measure carries a particularly low risk of adverse consequences for users, especially when weighed against the critical interests it helps protect. Therefore, it may be appropriate to employ more experimental tools, tools with higher error rates, or low-confidence matches from highly reliable tools.

The more significant consequences should come with more stringent requirements of reliability of the tools used. The measures of this kind should have low levels of errors. However, it may be possible to achieve such high reliability through human review.[62]

Similarly, stronger procedural safeguards may be appropriate. Measures that use content data could require prior approval by an authority. Furthermore, it may be advisable to require permission from a judicial authority for enhanced mitigation measures that use content data for CSA detection and reporting.

Compatibility with the Charter. By dividing enhanced mitigation measures into layers as suggested above, the Proposal could demonstrate more clearly than it does now that its framework for CSA prevention and detection is proportionate and conforms with Article 52(1) of the Charter. Moreover, implementing enhanced mitigation measures would significantly strengthen the argument that detection orders are necessary as a last resort where mitigation is insufficient (i.e., that there are no less intrusive measures available than detection orders).

5.2.3. A right to request the initiation of the procedure of making of a detection order

A more limited solution, not mutually exclusive to proposals discussed in sections 4.2.1-2, could target the risk that Coordinating Authorities may fail in a timely manner and in a way that ensures maximum effectiveness of CSA prevention and combating. This solution would involve vesting service providers with an enforceable right to request the initiation of the procedure for the making of a detection order, and to receive a reasoned decision in case the Coordinating Authority refuses to request a detection order.

At a minimum, this would help ensure that the current level of CSA combating efforts is preserved under the new framework. This is because those service providers who currently voluntarily detect CSA can be expected to strive to ensure that their efforts can continue.

This solution could be implemented through a modification of the proposed Article 7 by allowing service providers to request the initiation of the procedure through which a Coordinating Authority would independently decide whether to request a detection order.

The Coordinating Authority's decision whether to request a detection order should be made within a specified time limit and be subject to judicial review. Otherwise, there will be a risk that coordinating authorities will fail to act, even without any reason.

In addition, given that some service providers are currently engaged in voluntary detection efforts, it may be advisable to provide a temporary extension of the derogation from the ePrivacy Directive for those voluntary efforts. This could come with an imposition of a duty on Coordinating Authorities to review those efforts as a matter of priority and in sufficient time to ensure that those voluntary efforts that merit it will be able to receive detection orders before the expiry of the temporary extension.

---

[62] The LIBE Report explicitly invokes Article 8 of Regulation 2022/2065 (DSA) which contains the prohibition on general monitoring obligation (Amendment 189). This amendment only concerns detection orders. However, if our suggestion of a derogation for prevention orders were to be considered, it may be inadvisable to follow LIBE's approach. This is because the CJEU sees the prohibition of general monitoring as adding an otherwise inapplicable condition, which also does not directly follow from primary law, that automated tools must avoid errors on their own, without human intervention; see C-401/19, Poland v Parliament and Council, paras. 87-90.

Compatibility with the Charter. Allowing service providers to request the initiation of the procedure for making a detection order would not, by itself, constitute an interference with any Charter provision. This is because it would not involve any reduction in substantive or procedural safeguards: merely a right for service providers to request the initiation of the procedure.

In fact, this would allow the Proposal to better comply with Article 52(1) and Article 16 of the Charter. Given the business risks (e.g., reputational risks) of being perceived as insufficiently preventing and combating CSA, ICS providers have a significant interest in being permitted to obtain a detection order. The possibility that a Coordinating Authority could fail to act to request the issuance of an order, without procedural safeguards, is concerning. These safeguards should include the service provider's right to request the initiation of the procedure, time limits, and effective judicial redress. The absence of these safeguards is arguably itself an additional and unnecessary interference with Article 16 of the Charter, thus a violation of Article 52(1) of the Charter.