Position Paper on the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Introduction

ISPA Belgium (Internet Service Providers Association) brings together the entirety of the Internet industry ecosystem in Belgium, representing the collective voice of the Internet community. ISPA members are committed to making the digital space a safe space for everyone and to protecting children online in particular, and support the EU strategy for a more effective fight against (online) child sexual abuse. ISPA therefore shares the objectives of the proposed Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (CSAR).[1] This legislation is timely given that the ePrivacy Directive Interim Derogation, that currently provides us with a legal basis to detect child sexual abuse material (CSAM) in private communications, will expire in April 2026.[2]

Moreover, ISPA favors harmonization and an EU-led approach on the matter, rather than many national approaches, as fragmentation of rules only leads to more inefficiency.

However, ISPA members are concerned about the operability of the Regulation, as well as the possible regulatory duplications and conflicts of law it can create.

End-to-end encryption (E2EE)

In the Danish compromise text[3], the Regulation would extend the Temporary Regulation for up to 72 months after the CSAR enters into force, thereby preserving the legal basis for voluntary detection during the transition. Over the longer term, however, the system reverts to mandatory detection orders, which may be imposed on high-risk services under defined conditions. Detection orders once again become the sole legal basis for authorizing the scanning of user content and are limited to known and newly identified CSAM.

The new Danish compromise text for the Regulation states that "nothing in this Regulation should be interpreted as prohibiting, weakening or circumventing, requiring to disable, or making end-to-end encryption impossible"[4] and goes on by saying that "in interpersonal communications services using end-to-end encryption, those technologies shall detect the dissemination of child sexual abuse material prior to its transmission"[5]. However, requiring detection tools to identify CSAM before transmission, effectively points toward client-side scanning. Detecting material and generating reports cannot be done without compromising encryption. E2EE, however, is

[1] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse.

[2] Regulation (EU) 2021/1232 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.

[3] Presidency compromise texts on Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 24 July 2025, link: https://cdn.netzpolitik.org/wp-upload/2025/07/2025-07-24_Council_Presidency_LEWP_CSA-R_Compromise-texts_11596.pdf.

[4] Recital 26 Presidency compromise text.

[5] Article 10 Presidency compromise text.

fundamental to protecting user data, maintaining trust in online services, and safeguarding privacy. While encrypted services can, like any technology, be misused, weakening E2EE would jeopardize the security of the internet, erode privacy protections, and introduce severe cybersecurity risks.

For these reasons, ISPA believes that services offering end-to-end encryption should be explicitly exempted from scanning obligations and permitted to address the risks of child sexual abuse material through approaches that do not compromise the confidentiality of private communications. As currently drafted, the proposal still creates mechanisms that threaten to break E2EE.

Prevention-led approach

The proposed compromise text heavily focuses on the detection of CSAM. As noted, the Temporary Regulation would be prolonged for up to 72 months after the CSAR takes effect, allowing voluntary detection to continue during the transition. In the longer run, however, the framework shifts back to mandatory detection orders.

ISPA believes a more prevention-led approach should be at the forefront of the Regulation, based on the proportionality principle. Child sexual abuse must be prevented from happening in the first place, not just reported and detected once it has happened. Detection orders should be measures of last resort, as they hold a risk of contradicting the prohibition of general monitoring, a core tenet of European law recently reaffirmed in the Digital Service Act (DSA).[6]

ISPA supports the inclusion of voluntary measures, in particular an explicit legal basis for the voluntary detection of child sexual abuse (CSA), similar to what exists under the ePrivacy derogation. This approach was reflected in the earlier Polish Presidency compromise text, which replaced mandatory detection with voluntary measures. Providers should be able to develop approaches to tackle CSA that are effective, proportionate and appropriate for their service, adapted to the technical realities and the business of the provider. Allowing and incentivizing voluntary measures will allow operators to develop and use the type of mitigations that will be most effective to combat CSAM based on their business model.

Several ISPA members have tools in place for voluntary detection of CSAM and prevention of CSA within their own systems. ISPA believes that providers should be enabled to (further) develop preventive approaches and measures, and that should be done by creating an express legal basis to process communications metadata for the purposes of prevention and detection with appropriate safeguards in the text.

Cloud computing services providers should be regarded as the location of last resort to disable access to CSAM

A core principle of this legislation must be that illegal content, in this case CSAM, is removed or disabled as close to the source as possible. This approach not only safeguards the confidentiality of communications, but also ensures that the framework remains proportionate and targeted while improving the overall effectiveness of the measures.

[6] 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).

For this reason, providers of cloud computing services should be regarded as a last resort when it comes to disabling access to CSAM. As LIBE underlined in its final report, the specific nature of cloud computing and web-hosting services, when functioning as infrastructure, means that imposing the same obligations as on hosting service providers could have a far broader impact on users of cloud-hosted services. Detection and removal orders should therefore be directed primarily to hosting providers and interpersonal communications services that can reasonably be expected to have the technical and operational capacity to act directly against CSAM.[7]

Number-based interpersonal communication services (NB-ICS) and Business to business (B2B) services

Extending the scope of this legislation to number-based interpersonal communication services (NB-ICS) is neither practical nor justified, as these services are not commonly used to distribute image or video content. In most EU Member States, subscribing to NB-ICS requires users to present official identification, such as a passport, ID card, or driver's license, under national Know-Your-Customer (KYC) rules. These checks mean that the identity of NB-ICS users is already verified. This existing framework serves as a strong deterrent against the circulation of CSAM on such services.

Moreover, both the European Parliament's Complementary Impact Assessment[8] and the Council Legal Service's Opinion[9] highlight that applying the proposal to NB-ICS would be disproportionate to its purpose.

Equally, as they do not hold a risk of transmitting CSAM, also B2B services should be exempted from the scope of the Regulation.

Conclusion

The European Parliament and the Council have laid down rules to prevent and combat child sexual abuse (CSA). ISPA members are committed to making the digital space a safe space for everyone, and thereby share the objectives of this proposed Regulation.

However, ISPA is concerned about the protection of E2EE, the absence of a prevention-led approach and the current role of could computing services, NB-ICS and B2B services in the Regulation. Furthermore, once passed, this legislative proposal will be immediately applicable in Belgium and impact its active providers.

Our sector association is happy to welcome the opportunity to further explain our views at a physical meeting.

---

[7] Amendment 30, Report on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, Committee on Civil Liberties, Justice and Home Affairs – European Parliament, 16 November 2023, link: https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html.

[8] Proposal for a regulation laying down rules to prevent and combat child sexual abuse – Complementary impact assessment, European Parliament, April 2023, link: https://www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf.

[9] Opinion of the Legal Service on Proposal for a Regulation laying down rules to prevent and combat child sexual abuse – detection orders in interpersonal communications – Articles 7 and 8 of the Charter of Fundamental Rights – Right to privacy and protection of personal data – proportionality, Council of the European Union, 26 April 2023, link: https://cdn.netzpolitik.org/wp-upload/2023/05/2023-04-26_Council_Legal-Service_CSAR_8787_Agence-Europe.pdf.