Council of the European Union

Brussels, 8 April 2026
(OR. en)

8048/26

**Interinstitutional File:**
**2022/0155 (COD)**

**LIMITE**

**ENFOPOL 124**
**JAI 436**
**CRIMORG 90**
**IXIM 92**
**DATAPROTECT 112**
**CYBER 156**
**COPEN 128**
**FREMP 123**
**TELECOM 156**
**COMPET 407**
**MI 318**
**CONSOM 113**
**DIGIT 93**
**CODEC 612**



**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse<br>- Considerations regarding detection |

## 1. The Commission's proposal and the co-legislators' positions on detection

The **Commission's proposal** contains provisions allowing for the issuance of detection orders concerning known and new child sexual abuse material (CSAM) or grooming. These orders, which could be issued upon request of a Coordinating Authority by a competent judicial or independent administrative authority, would be addressed to providers of hosting services or interpersonal communications services in the event that the Coordinating Authority concludes, after taking account of all relevant facts and circumstances of the case at hand, that there is evidence of a significant risk of the service being used for the purpose of online child sexual abuse and the reasons for issuing the detection order outweigh the negative consequences for the rights and legitimate interests of all parties affected.

The mandates of both the European Parliament (EP) and the Council significantly depart from the Commission's proposal.

The **most relevant changes introduced by the EP** are the following:

a. Detection orders may concern **known and new child sexual abuse material. Grooming** and interpersonal communications to which **end-to-end encryption** "is, has been or will be applied" are **excluded** from the scope.

b. These orders should be issued **only by a competent judicial authority** to providers of hosting services or number-independent interpersonal communications services and they "shall be **targeted, specified and limited to individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication, in respect of whom there are reasonable grounds of suspicion for a link, even an indirect one, with child sexual abuse material**."

c. **Three preconditions** must be met before detection orders can be issued:

   1. there must be "reasonable grounds of suspicion";

   2. the impact of the risk mitigation measures taken by the provider does not suffice or the provider fails to put in place effective mitigation measures;

   3. the issuance is necessary and proportionate and outweighs negative consequences on the rights and legitimate interests of all parties affected, without jeopardising the security of communications.

d. As a rule, detection orders should be **addressed to the service provider acting as controller** under the General Data Protection Regulation[1]. Only where the controller cannot be identified or where addressing the controller would be detrimental to an ongoing investigation, the orders can be addressed to the service provider that stores or otherwise processes the data on the controller's behalf.

e. Detection orders should also contain **information about the right to appeal to a court** according to national legislation.

[1] Regulation (EU) 2016/679.

f. A **review clause** was added for the Commission to assess, within three years, the feasibility of including grooming in the scope of detection orders in the future.

In addition to detection orders, the European Parliament has added a task for the **EU Centre** to - proactively and on its own initiative - conduct **searches on publicly accessible content on hosting services for known child sexual abuse material,** based on guidelines to be issued by the European Data Protection Board.

The **Council has deleted all provisions on detection orders.** However, a **review clause** was added with the obligation for the Commission to assess within three years after the entry into force of the Regulation the necessity and feasibility of including detection obligations in the future, including an evidence-based assessment of the reliability and accuracy of the relevant available technologies.

Furthermore, the Council mandate foresees that providers of **number-independent interpersonal communications services** should be allowed to carry out **voluntary activities to detect** known and new child sexual abuse material and grooming.

The Council has added a provision to clarify that **"this Regulation shall not prohibit, make impossible, weaken, circumvent or otherwise undermine […] encryption, including end-to-end encryption, implemented by the relevant information society services or by the users [or] create any obligation that would require a provider of hosting services or a provider of interpersonal communications services to decrypt data or create access to end-to-end encrypted data, or that would prevent providers from offering end-to-end encrypted services."**

**2. Way forward for discussions on detection**

In order to move the negotiations forward and try to find common ground with the EP, the Presidency suggests breaking down the different elements of the co-legislators' positions on detection, which could be combined in different ways – without the necessity to cover all of them - to come to a solution that is acceptable for both co-legislators.

Distinctions could be made alongside the following axes:

| | | |
|---|---|---|
| Providers of **hosting services** | ⇆ | Providers of **interpersonal communications services** |
| Content **publicly** accessible | ⇆ | Content **not publicly** accessible |
| **Known** child sexual abuse material | ⇆ | **New** child sexual abuse material |
| Detection **orders** to providers | ⇆ | **Voluntary** detection by providers |
| Detection targeted to **(parts of) services** | ⇆ | Detection targeted to **(groups of) persons** |

One useful avenue would be to first **distinguish** between **detection on hosting services** (i.e. on content that is largely publicly accessible) and on **interpersonal communications services** (i.e. content that is private).

*Detection on hosting services*

A number of possibilities could be explored in this context – for example, voluntary detection on hosting services by providers as a mitigation measure. Alternatively, detection orders could be issued to providers if certain conditions are met.

As far as publicly accessible content on hosting services is concerned, the meaning of the term 'publicly accessible' would need to be clearly defined to ensure legal certainty. Moreover, consideration should be given to Article 8 of the Digital Services Act (DSA)[2] in terms of avoiding imposing obligations of generalised scanning on providers:

*"No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers."*[3]

Consideration should also be given as to whether detection on publicly accessible content would be for known and/or new CSAM and/or grooming.

[2] Regulation (EU) 2022/2065.
[3] Under the DSA, there is no obligation for providers to scan their services. However, if they become aware of illegal content, they must report it or else they will become liable.

*Proactive scanning by the EU Centre*

The EP's position for the **EU Centre to conduct scanning on its own initiative for known CSAM** on publicly accessible content might also be considered (or built upon) as a complement to possible detection orders or voluntary scanning in publicly accessible content.[4]

*Detection on interpersonal communications*

Scanning of interpersonal communication services could be done either following a **detection order** on providers ***or*** **voluntarily** by providers (as a mitigation measure).

To the extent that **detection orders on interpersonal communications** would be considered, safeguards would have to be applied to ensure the protection of privacy. The conditions under which detection would take place could be explored further, e.g. whether detection orders could be **targeted to (groups of) persons** and/or **limited to specific parts of the provider's system that present a specific risk** and/or **to specific type of content.**

Finally, the positions of both co-legislators **exclude end-to-end encrypted interpersonal communications** from the scope of detection. Therefore, the Presidency expects that an agreement could be found between the Council and the EP on encryption.

**3. Questions for delegations to consider**

In preparation of the trilogue on 16 April 2026, the Presidency invites delegations to provide feedback to the following questions by Monday, 13 April 2026, COB.

a) The Presidency intends to explore the possibility of having distinct approaches to detection of content that is publicly accessible on hosting services and detection on interpersonal communications services. Would the delegations agree with this approach?

b) As regards detection of publicly accessible content, the Presidency intends to explore the possibility of (a) detection orders; (b) voluntary detection; and (c) scanning by the EU Centre, with appropriate limitations. Would you agree with this approach?

[4] In the Commission's proposal and the Council position, the EU Centre would already be tasked to conduct such searches at the request of a national authority or a person that has been subjected to child sexual abuse (see Article 49).

c) As regards detection on interpersonal communication services, the Presidency intends to explore the possibility of (a) detection orders; and (b) voluntary detection, with appropriate limitations. Would you agree with this approach?

d) In relation to the axes mentioned above, are there any elements that the delegations cannot accept as part of a compromise under any circumstances?