Council of the European Union

Brussels, 4 March 2025
(OR. en)

6475/25

LIMITE

JAI 229
ENFOPOL 60
CRIMORG 37
IXIM 41
DATAPROTECT 41
CYBER 51
COPEN 31
FREMP 41
TELECOM 60
COMPET 83
MI 96
CONSOM 26
DIGIT 30
CODEC 166

Interinstitutional File: 2022/0155(COD)

NOTE

From:	Presidency
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Exchange of views on the approach suggested by the Presidency

The Presidency provided delegations at the LEWP-P meeting on 5 February 2025 with a compromise text suggesting a new approach as outlined in doc. 5352/25. Based on the feedback from delegations received during and after that meeting, the Presidency has prepared this discussion paper for the LEWP-P meeting on 11 March 2025.

The Presidency noted agreement among delegations that when Regulation (EU) 2021/1232, the ”Interim Regulation”, expires on 3 April 2026, there should be no legal void obliging providers to discontinue their current detection and reporting activities. The Presidency also noted that delegations are willing to continue working on the proposed Regulation with a view to reaching a partial mandate for negotiations with the European Parliament as soon as possible.

As the views expressed by delegations differ significantly on several substantial issues, the Presidency intends to focus the discussion on the following topics: (1) Obligations for providers, (2) Scope and design of the derogation from certain provisions of Directive 2002/58/EC, (3) Use of technologies by providers, (4) Reducing complexities and administrative burden, (5) Review clause.

1. **Obligations for providers**

In Article 1, the Presidency has introduced in paragraph 1 the obligation on providers to make their best efforts to prevent the use of their services for child sexual abuse (CSA). In Articles 3 and 4, the Presidency aimed at strengthening the prevention measures to be undertaken by providers, as in particular outlined in Article 4(1) and (2). If providers do not comply with their obligations, penalties may be imposed on them in accordance with Article 35.

In Articles 5 and 5a, the Presidency proposed to adapt the text to the absence of mandatory detection, maintaining the obligation for providers of high-risk services to effectively contribute to the development of relevant detection technologies, while the adjusted or additional risk assessment or prevention measures would need to be done by providers on a recommendation basis only. In Article 12, the Presidency put an emphasis on the notification by the users. Providers of high-risk services would be obliged to provide an effective user notification mechanism and to give feedback to users.

The Presidency's intention is to shift the focus of the proposal towards prevention, comprising beyond the obligations of providers also the preparation of dedicated national strategies by the Member States and a comprehensive communication and outreach strategy by the EU Centre. Therefore, the Presidency has chosen to use the term "prevention" instead of "risk mitigation" throughout the text.

There seems to be a common view among delegations that it is essential to make the providers more accountable to ensure an effective prevention of CSA. Some proposed to oblige the providers to effectively prevent the use of their services for CSA, while others remarked that a service provider in reality cannot fully prevent the misuse of its services and therefore cannot be required to do so. Some delegations advised the Presidency to move back to the wording "risk mitigation" as proposed by the Commission as this term provides more clarity and is easier to assess and measure. Another issue to keep in mind is that in absence of detection orders, detection should remain voluntary for providers. Therefore, the obligation to prevent or to mitigate the risk of CSA in their services should not result in a de facto detection obligation for providers.

Several delegations asked the Presidency to reinstate the text in Article 5a to avoid a limitation of the powers of national authorities to ensure that providers comply with their obligations. They request that the Coordinating Authority should have the power to request additional or adjusted prevention/risk mitigation measures and to enforce necessary improvements as appropriate, if it considers that those measures initially suggested and carried out by the provider were not sufficient.

Some delegations asked the Presidency to expand the obligation to establish a user notification mechanism in line with Article 12(3) to all relevant providers. In addition, it was proposed to ensure that reporting mechanisms are always available to users and that user notifications should be promptly reported to the competent authorities.

Questions to delegations:

- How do you see the best way to make providers accountable to prevent or mitigate the risk of CSA in their services without triggering a de facto detection obligation for providers?
- Do you agree to keep the term "prevention" throughout the text as suggested by the Presidency or do you prefer to revert to the term "risk mitigation" as in the Commission proposal?
- Do you prefer to keep the Presidency text or to reinstate the previous text in Article 5a (1) and (2) regarding adjusted or additional risk assessment or prevention/risk mitigation measures?
- Do you prefer to limit the user notification mechanism laid down in Article 12(3) to high-risk services or should this obligation apply to all relevant providers?

2. Scope and design of the derogation from certain provisions of Directive 2002/58/EC

The derogation from certain provisions of the e-privacy Directive 2002/58/EC was added by the Presidency as a new prevention measure in Article 4a. The incorporation of the text of Regulation (EU) 2021/1232 reflects its current scope: derogation from Articles 5(1) and 6(1) of the e-privacy Directive for 'number-independent interpersonal communication services ' and covering all three types of CSA. The text of Regulation (EU) 2021/1232 has been followed to the extent possible. Additions proposed include in paragraph 3 (a) the reporting to the EU Centre, (b) the use of the indicators provided by the EU Centre, (c) the use of technologies made available by the EU Centre including additional cyber security safeguards and (d) mitigation measures against cybersecurity risks and provisions on keeping logs. The reporting by providers has been aligned with the other reporting obligations under this Regulation, taking into account the standard reporting form established by implementing act 2024/2916. In paragraph 4, it is clarified that the use of technologies provided by the EU Centre does not affect the responsibility of providers regarding the use of technologies.

In Article 88, the Presidency suggests extending Regulation (EU) 2021/1232 for 3 years after the entry into force of this Regulation until the EU Centre is established and the databases of indicators are available for being used by providers under Article 4a.

The Presidency suggested integrating the derogation from certain provisions of Directive 2002/58/EC in this Regulation rather than providing a permanent basis for Regulation (EU) 2021/1232 as a self-standing legislative act in order to benefit from the features of this Regulation for the voluntary activities of the providers as outlined above.

Concerning legal aspects, some delegations wondered about the alignment of Article 4a with the General Data Protection Regulation (GDPR), and in particular its Article 22 with regard to the use of automated detection technologies and the need of human intervention where necessary, and the legal possibility to permanently establish the provisions of Regulation (EU) 2021/1232. Concerns were also expressed with regard to the wording "suspected online child sexual abuse" and the exemption for the "scanning of audio communications" which would require clear definitions.

Regarding the scope of the derogation, some delegations expressed the view that the voluntary activities of providers should include prevention measures that require accessing metadata or other stored data. Therefore, they suggested expanding the scope of the derogation to Article 5(3) of the e-privacy Directive as initially foreseen in Article 1(4) of the Commission proposal for the purpose of detection orders. Other delegations wondered whether the scope of the derogation should not be limited to known CSA material (CSAM), and how the singling out of 'number-independent interpersonal communication services ' in Article 4a would affect other provisions of this Regulation.

Some delegations asked to add safeguards under Article 4a, in particular on the rights of the data subject to be made aware of the nature of the measures undertaken by providers. Some delegations pleaded for effective and clearly defined reporting channels avoiding duplications and wondered about the legal basis for "organisations acting in the public interest against CSA" to receive reports.

Questions to delegations:

- How do you see the best way of designing the derogation from certain provisions of the e-privacy Directive so that it is effective, provided with sufficient safeguards and properly embedded in the functioning of this Regulation?
- Do you agree to have the derogation integrated in this Regulation as Article 4a as suggested by the Presidency or do you prefer to keep Regulation (EU) 2021/1232 as a separate legislative act to be amended and made permanent through this Regulation?
- Do you agree to keep the scope of the derogation as suggested by the Presidency, analagous to the scope of Regulation (EU) 2021/1232? If you do not agree, please indicate which deviations from the scope you want to see implemented.

3. Use of technologies by providers

In the text proposed by the Presidency, comprehensive safeguards for cybersecurity including encryption apply for the entire Regulation under Article 1(5). Upload moderation is no longer possible due to the deletion of Article 10(1). Even though not explicitly indicated in the current text, the possibility and feasibility of the detection in encrypted environments in the future might be subject to the assessment by the Commission (see review clause below). Article 1(6) makes clear that there should be no obligation on providers to detect in a generalised and indiscriminate manner.

The requirements for the use of technologies by providers performing activites under Article 4a are outlined in paragraph 3, letter (c) of this article. In paragraph 4, it is clarified that the use of technologies provided by the EU Centre does not affect the responsibility of providers regarding the use of technologies.

The scope of Article 50 is broadened in the Presdiency proposal so that the EU Centre can make available technologies to providers to prevent the dissemination of CSA. In Article 66, the Presidency proposed to keep the Technology Committee with the task to support the EU Centre's activities related to developing technologies to prevent CSA.

With regard to cyber security and the protection of privacy, some delegations asked the Presidency to delete the first sentence of Article 1(5) as the current wording would de facto exclude encrypted services from the scope of the Regulation as well as discourage the initiative of providers who, without endangering the encryption of communications, decide to implement innovative technologies to detect CSAM and grooming, including on a voluntary basis. Other delegations welcomed the protection of encryption as suggested by the Presidency and insisted to keep excluded from this Regulation any measures which lead to the scanning of encrypted inter-personal communications or which break, weaken, modify or circumvent end-to-end encryption including through client-side scanning or upload moderation. One delegation asked to clarify whether the encryption safeguards apply only to communication in transit or also to stored previous communication. Another delegation asked the Presidency to make clear in Article 1(6) that generalised and indiscriminate detection should not be allowed.

Some delegations asked for more information about the technologies currently used by the providers under the derogation regime. In particular, they asked for more insight into what technologies exist that allow for the scanning of text with the purpose of the detection of grooming without it leading to the deduction of the substance of the content, but which has the capacity to detect recurring patterns only.

One delegation suggested that the European Data Protection Board and the EU Centre's Technology Committee should provide an opinion before the EU Centre makes technologies available to providers under Article 50.

Questions to delegations:

- How do you see the best way of regulating the use of technologies by providers including those made available by the EU Centre, also with a view to protecting cyber security?
- Do you agree to invite the Commission to prepare an updated overview of the technologies currently used by the providers under the derogation regime and to provide information about the existing technologies to detect grooming without it leading to the deduction of the substance of the content?

4. Reducing complexities and administrative burden

During the work of the Council on the proposed Regulation, several elements have been added that could undergo a thorough analysis given the changed scope of this Regulation with regard to detection. This concerns in particular the risk categorisation in Article 5 and the sign of reduced risk in Article 5b. While the necessity and proportionality of the risk categorisation could be questioned in absence of detection orders, some delegations flagged that the sign of reduced risk could even have a counterproductive effect.

Some delegations asked the Presidency to discuss the role and tasks of the EU Centre to prevent and combat child sexual abuse. One delegation called for the EU Centre being replaced by a network of experts and organisations (organisations acting in the public interest against CSA, providers, specialised law enforcement agencies) to carry out victim support, share best practices and provide research. While Europol could be entrusted with hosting the databases of indicators, the EU Innovation Hub for Internal Security could assist the Commission in assessing the maturity and accuracy of technologies with regular studies on this subject.

The Presidency stressed in its compromise text the additional role for the EU Centre to act as a knowledge hub, tasked the Centre to develop a communication strategy and promote the dialogue with and among stakeholders, reflected the strengthening of prevention aspects and the EU Centre's support to the providers' activities under Article 4a, and included the possibility for Member States to request the EU Centre to verify the effectiveness of prevention measures. The EU Centre would still receive the reports from providers and sort out false positives before forwarding them to law enforcement.

Questions to delegations:

- How do you see the best way of reducing complexities and administrative burden in this Regulation?
- Do you agree to keep the risk categorisation and the sign of reduced risk as proposed by the Presidency or do you prefer to disregard or amend these elements?
- Do you agree to keep the EU Centre with the revised role and tasks proposed by the Presidency, do you propose to amend the role and tasks of the EU Centre or do you prefer to replace the EU Centre by different structures?

5. Review clause

In Article 85, the Presidency adapted the review clause so that the Commission is invited to assess the necessity and feasibility of possible mandatory detection within three years after entry into force of this Regulation. As the development of technologies is going on at a high pace, this period of time appears reasonable for the Commission to assess whether technological developments require the tabling of a legislative proposal to amend this Regulation. If this is not the case, another 3-year period would apply. In parallel, the Presidency text includes obligations for the providers of high-risk services and a task to the EU Centre supported by the Technology Committee to contribute to the development of technologies to prevent CSA.

Delegations welcomed in general the inclusion of a review clause in the Presidency compromise text to balance the deletion of the detection order from the scope. It was also suggested that the Commission's assessment should cover the possibility and feasibility of detection of interpersonal communications services using end-to-end encryption, and the evolution of CSA after the entry into force of this Regulation. One delegation asked to clarify with what activities and to what extent the providers of high-risk services would be expected to contribute to the development of technologies.

Questions to delegations:

- How do you see the best way of designing the review clause for the Commission to possibly propose new legislation within 3 years after entry into force of this Regulation?
- How do you see the roles and responsibilities for providers, the EU Centre and its Technology Committee and possible other structures to contribute to the development of new technologies to prevent CSA?