Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 14 June 2024

WK 8634/2024 INIT

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

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 - Explanatory note of the Presidency

The Presidency informs delegations in this explanatory note about the changes made to the previous compromise text 9093/24, outlined in the ANNEX to this note[1], in preparation of the partial negotiation mandate with the European Parliament:

1. The wording on the protection of cyber security and in particular encryption was strengthened in Art. 1(5) following a request by the French delegation.
2. A definition of "visual content" in Art. 2(y) supported by recital 23a was added, following a request by the Czech delegation for clarifications.
3. A definition of a hit for the detection of new CSAM in Art. 2(z) was added to meet the request for more clarity raised by several delegations. Recital 23a was cleaned to avoid duplications with the operational provisions in Art. 7(6a).
4. The possibility for the Commission to increase the number of hits required for triggering the reporting through delegated acts, where necessary, was introduced in Art. 7(6a) and Art. 86 to increase the accuracy of detection.

5. A clarification was made in Art. 8(1a) that independent administrative authorities should act free from any external influence when exercising their duties, following a request by the Swedish delegation.
6. A clarification was made in Art. 10(2) that the technologies used for upload moderation also have to be vetted through an implementing act by the Commission.
7. Additional safeguards were added for detection technologies that are intended to be used in services using end-to-end encryption, following a request by the French delegation. A specific testing and technical certification of those technologies by the EU Centre with the involvement of its Technology Committee is introduced before those technologies are subject to the vetting procedure in line with Art. 10(2)). These changes are reflected in Arts. 10(3), 43(9) and 66(6), supported by recital 26a.
8. A clarification was made in Art. 10(4) that the obligation for providers of interpersonal communications services to limit functionalities to prevent the transmission of visual content and URLs absent the user consent would be applied only when a detection order is received. This change follows a request by the Swedish delegation.

[1] New changes to the Commission proposal in comparison to document 9093/24 are marked in **bold underline** and ~~strikethrough underline~~.

(23a) To further avoid undue interference with fundamental rights and ensure proportionality, detection orders should cover only visual content, which should be understood as images and the visual components of videos, including charts, infographics, logos, animations, iconography, gifs, stickers or the visual components of livestreaming, and URLs, while the detection of audio communication and text should be excluded. Despite that limitation of detection to images and the visual components of videos, the solicitation of children could still be identified to some extent through the detection of visual material exchanged. To increase the accuracy of detection, the reporting by providers of hosting services and providers of publicly available interpersonal communications services on potential online new child sexual abuse material should be limited to that material either notified to them by a user or detected repeatedly on their services. ~~The first detection of potential new child sexual abuse material should be stored by the providers as a hit and preserved for at least twelve months or, if the detection has been issued for a duration of more than twelve months, for the duration of a detection order. The stored hit should be deleted thereafter.~~ As an additional safeguard to protect privacy, the reporting to the EU Centre of potential new child sexual abuse material detected in the service of a provider, should be done in a pseudonymized way, so that the personal data cannot be attributed to a specific data subject prior to ~~Only after~~ human verification ~~by the EU Centre, the providers should share the report with the EU Centre including the personal data attributable to a data subject~~.

(26a) While end-to-end encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society, the European Union needs to ensure the effective prevention of and fight against serious crime such as child sexual abuse. Providers should therefore not be obliged to prohibit or make impossible end-to-end encryption. Nonetheless, it is crucial that services employing end-to-end encryption do not inadvertently become secure zones where child sexual abuse material can be shared or disseminated without possible consequences. Therefore, child sexual abuse material should remain detectable in all interpersonal communications services through the application of vetted technologies, when uploaded, under the condition that the users give their explicit consent under the provider's terms and conditions for a specific technology ~~functionality~~ being applied to such detection in the respective service. Users not giving their consent should still be able to use that part of the service that does not involve the sending of visual content and URLs. This ensures that the detection mechanism can access the data in its unencrypted form for effective analysis and action, without compromising the protection provided by end-to-end encryption once the data is transmitted. To avoid the weakening of the protection provided by the encryption, technologies intended to be used for detection in services using end-to-end encryption should be certified by the EU Centre and tested with the support of its Technology Committee before undergoing the vetting procedure foreseen for all detection technologies.

Article 1

Subject matter and scope

5. Without prejudice to Article 10a, this Regulation shall not prohibit, make impossible, <u>weaken, circumvent or otherwise undermine cybersecurity measures, in particular encryption, including</u> end-to-end encryption, implemented by the relevant information society services or by the users. This Regulation shall not 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.

Article 2

Definitions

For the purpose of this Regulation, the following definitions apply:

<u>(y) 'visual content' means images and the visual components of videos;</u>

<u>(z) 'hit' means a match established by comparison between the indicators to detect the dissemination of new child sexual abuse material and the visual content subject to detection.</u>

Article 7

Issuance of detection orders

6a. Providers of hosting services and providers of interpersonal communications services shall carry out the detection orders concerning the dissemination of new child sexual abuse material in a way that the material is reported in accordance with Articles 12 and 13 under the conditions outlined in sub-paragraphs 2 to 4.

The detection of potential new child sexual abuse material shall result in a hit to be flagged in the affected service, without the provider getting knowledge of, or control over, that information. Providers shall preserve the information about the existence of the hit for at least twelve months or the duration of the respective detection order, whatever is longer.

Once potential new child sexual abuse material has been flagged in a service twice, or once a user has notified the provider about potential new child sexual abuse material within a service, the provider shall report that material to the EU Centre in such a manner that the personal data cannot be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separate and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Where the EU Centre considers, after human verification, that a report on potential new child sexual abuse material submitted by a provider is not manifestly unfounded, it shall require the provider to re-submit the report without the limitations outlined in sub-paragraph 3.

<u>The Commission shall be empowered to adopt delegated acts in accordance with Article 86 in order to increase, where necessary, the number of hits required to trigger the reporting of potential new child sexual abuse referred to in sub-paragraph 3.</u>

Article 8

Additional rules regarding detection orders

1a. **If a detection order is issued by an independent administrative authority or by the Coordinating Authority of establishment with the prior authorisation by an independent administrative authority, that independent administrative authority must have a status enabling it to act objectively, impartially and free from any external influence when carrying out its duties ~~and must, for that purpose, be free from any external influence~~.**

Article 10

Technologies and safeguards

1. Providers of hosting services and providers of interpersonal communications services that have received a detection order shall execute it by installing and operating technologies **approved by the Commission** to detect the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable, using the corresponding indicators provided by the EU Centre in accordance with Article 46.

2. **The Commission shall adopt implementing acts to approve the technologies referred to in paragraph 1 and Article 10a, after consulting the EU Centre, using the criteria set out in paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87.**

   The provider shall be entitled to acquire, install and operate, free of charge, technologies made available by the EU Centre in accordance with Article 50(1), for the sole purpose of executing the detection order.

   ~~The provider shall not be required to use any specific technology, including those made available by the EU Centre, as long as the requirements set out in this Article are met.~~ The use of the technologies **referred to in paragraph 1 and Article 10a approved by the Commission** ~~made available by the EU Centre~~ shall not affect the responsibility of the provider to comply with ~~those~~ **the** requirements **set out in this Article** and for any decisions it may take in connection to or as a result of the use of the technologies.

3. The technologies shall ~~be~~:

   (a) **be** effective **and suitable** in detecting the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable;

   (aa) not introduce cybersecurity risks for which it is not possible to take any effective measures to mitigate such risk;

   (ab) if applied in services using end-to-end encryption, be certified by the EU Centre following tests conducted with the support of its Technology Committee, that their use could not lead to a weakening of the protection provided by the encryption;

   (b) **be limited to detect visual content and URLs, and** shall not be able to **deduce the substance of the content of the communications nor to** extract any other information from the relevant communications than the information strictly necessary to detect, using the indicators referred to in paragraph 1, patterns pointing to the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable;

(c) **be** in accordance with the state of the art in the industry and the least intrusive in terms of the impact on the users' rights to private and family life, including the confidentiality of communication, and to protection of personal data;

(d) **be** ~~sufficiently~~ reliable **and accurate**, in that they limit to the maximum extent possible the rate of errors regarding the detection **and, where such errors occur, enable the correction of errors without undue delay**.

4. The provider shall:

(a) 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 the dissemination of known or new child sexual abuse material ~~or the solicitation of children~~, as applicable, insofar as strictly necessary to execute the detection orders addressed to them. **In particular, the provider shall:**

(i) diligently identify, analyse and assess the cybersecurity risks that could be introduced by the technologies used for the execution of the detection orders;

(ii) take all reasonable mitigation measures, tailored to the possible cyberscurity risk identified, to minimise that risk;

(aa) upon receiving a detection order in interpersonal communications services, limit the functionalities of that ~~the~~ service to prevent the transmission of visual content and URLs absent the user consent pursuant to paragraph 5(aa);

(b) establish effective internal procedures to prevent and, where necessary, detect and remedy any misuse**, including misuses caused by breaching cybersecurity measures,** of the technologies, indicators and personal data and other data referred to in point (a), and unauthorized access to, and unauthorised transfers of, such personal data and other data;

(c) ensure regular human oversight as necessary to ensure that the technologies operate in a sufficiently reliable manner **and, where necessary, in particular when potential errors are detected, human intervention**;

(d) establish and operate an accessible, age-appropriate and user-friendly mechanism that allows users to submit to it, within a reasonable timeframe, complaints about alleged infringements of its obligations under this Section, as well as any decisions that the provider may have taken in relation to the use of the technologies, including the removal or disabling of access to material provided by users, blocking the users' accounts or suspending or terminating the provision of the service to the users, and process such complaints in an objective, effective and timely manner;

(e) inform the Coordinating Authority, at the latest one month before the start date specified in the detection order, on the implementation of the envisaged measures set out in the implementation plan referred to in Article 7(3);

(f) regularly review the functioning of the measures referred to in points (a), **(aa),** (b), (c) and (d) of this paragraph and adjust them where necessary to ensure that the requirements set out therein are met, as well as document the review process and the outcomes thereof and include that information in the report referred to in Article 9(3).

5. The provider shall ~~inform~~ **request the consent of** users **to detect the dissemination of known or new child sexual abuse material for the purpose of executing detection orders after informing them in the terms and conditions of use** in a clear, prominent and comprehensible way of the following:

(a) the fact that, **upon receiving a detection order, the provider** ~~it~~ operates technologies to detect online child sexual abuse **material** to execute the detection order, the ways in which it operates those technologies, **meaningful information about the logic involved**, and the impact on the confidentiality of users' communications;

(aa) the fact that, upon receiving a detection order in interpersonal communications services, it is required to limit the functionalities of the service to prevent the transmission of visual content and URLs absent the user consent;

(b) the fact that **the provider** ~~it~~ is required to report potential online child sexual abuse to the EU Centre in accordance with Article 12;

(c) the users' right of judicial redress referred to in Article 9(1) and their rights to submit complaints to the provider through the mechanism referred to in paragraph 4, point (d) and to the Coordinating Authority in accordance with Article 34.

The provider shall not provide information to users that may reduce the effectiveness of the measures to execute the detection order.

6. Where a provider detects potential online child sexual abuse through the measures taken to execute the detection order, it shall inform the users concerned without undue delay, after ~~Europol or~~ the national law enforcement authority of a Member State that received the report pursuant to Article 48 has confirmed that the information to the users would not interfere with activities for the prevention, detection, investigation and prosecution of child sexual abuse offences.

Article 43

Tasks of the EU Centre

The EU Centre shall:

9. certify technologies that are intended to be used to detect the dissemination of known or new child sexual abuse material in services using end-to-end encryption following tests conducted with the support of its Technology Committee that their use could not lead to a weakening of the protection provided by the encryption in accordance with Article 10(3)(ab).

Article 66

Establishment and tasks of the Technology Committee

6. The Technology Committee shall

(ac) contribute to the EU Centre's activities related to the testing of technologies that are intended to be used to detect the dissemination of known or new child sexual abuse material in services using end-to-end encryption with a view of excluding that their use could lead to a weakening of the protection provided by the encryption in accordance with Article 10(3)(ab).

Article 86

Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

2. The power to adopt delegated acts referred to in Articles 3, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a**, **83** and 84 shall be conferred on the Commission for an indeterminate period of time from [*date of adoption of the Regulation*].

3. The delegation of power referred to in Articles 3, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a, 83** and 84 may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day after the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.

4. Before adopting a delegated act, the Commission shall consult experts designated by each Member State in accordance with the principles laid down in the Inter-institutional Agreement of 13 April 2016 on Better Law-Making.

5. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

6. A delegated act adopted pursuant to Articles 3, **4, 5, 5b**, **7,** 8, 13, 14, 17, **18b**, 47, **47a, 83** and 84 shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.