Council of the
European Union

Brussels, 22 February 2024
(OR. en)

6850/24

LIMITE

JAI 312
ENFOPOL 93
CRIMORG 34
IXIM 67
DATAPROTECT 98
CYBER 53
COPEN 89
FREMP 96
TELECOM 74
COMPET 208
MI 201
CONSOM 70
DIGIT 54
CODEC 568

**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 – New approach suggested by the Presidency

The Presidency has prepared this note to discuss with delegations a possible refined approach for the proposed Regulation laying down rules to prevent and combat child sexual abuse. In response to concerns expressed by some delegations regarding the proportionality and targeting of detection orders and related to cyber security, the Presidency suggests focusing the first discussion on two interlinked building blocks: (1) risk categorisation of services for more targeted detection orders and (2) protecting cyber security and encrypted data, while keeping services using end-to-end encryption within the scope of detection orders. Based on the contributions from delegations to each of the building blocks, the Presidency is planning to further develop the concept, and to assess the consequences on other parts of the proposal, including the functioning and tasks for the envisaged EU Centre and will finally reflect an agreed concept in the legislative text.

1. More targeted detection orders

The Presidency proposes a combination of measures to increase the targeting of the detection orders. These include the categorisation of (parts of) services of providers of hosting services and of interpersonal communications services according to their risk level based on objective and non-discriminatory parameters. Depending on the categorisation of the (parts of the) service, they would subsequently be subject to obligatory or recommended risk mitigation measures and, as a measure of last resort, to detection orders.

The proposal includes the following two steps:

(1) Risk categorisation

The Presidency suggests developing a methodology for determining the risk of specific services or parts thereof. The risk categorisation should be based on a set of objective parameters (related to the type of service, the core architecture of the service, the provider's policies and safety by design functionalities and user tendencies). During the risk categorisation process, service providers could already apply additional risk mitigation measures to be possibly classified in a better category.

The scoring could be based, for example, on yes/no questions related to the core architecture of the service, on the extent to which policies and functionalities are in place to address the risk of child sexual abuse material being disseminated or grooming activities on the service or on the sampling and analysis of specific data (or a combination of all these scoring methodologies and criteria).

The methodology and the main parameters to determine in which category a service would fall, could be included in the operative part of the regulation, whereas a template including more specific descriptions and details per parameter could possibly be established through delegated or implementing acts. It is also relevant to keep agile regarding adapting the risk categorisation to future technological developments.

Following the outcome of this risk categorisation process, systems or parts thereof are classified as ‘high risk’, ‘medium risk’, low risk’ or ‘negligible risk’.

With reference to Recital 18b and Article 3(4) of the most recent compromise text, the categorisation of service providers could be reassessed more or less frequently depending on their category.

(2) Risk mitigation and detection orders

Depending on the risk category of the (part of the) service, the provider can be subjected by the Coordinating Authority to implement obligatory risk mitigation measures, tailored to the risks identified in the risk assessment. If the implementation of these measures is deemed not sufficient, a detection order could be requested by the Coordinating Authority. To make the issuing of detection orders more targeted and tailored to the situation of the specific service provider, the Presidency proposes establishing two different types of detection orders, aligned with the risk categories identified above.

a) Services categorised as “high risk” could be subject to obligatory risk mitigation measures and a standard detection order.

b) Services categorised as “medium risk” could be subject to obligatory risk mitigation measures and a limited detection order.

c) Services categorised as “low risk” could receive a list of recommended mitigation measures.

d) Services categorised as “negligible risk” would not receive a list of recommended mitigation measures (but should take voluntary mitigation measures based on their risk assessment).

The difference between standard and limited detection orders would be implemented in terms of criteria such as (1) maximum duration, (2) the detection technologies used, (3) whether only public information or also inter-personal communications are subject to the order, and (4) whether they can only apply to parts of the service, (5) if they should cover services using end-to-end encryption.

The Presidency also suggests granting providers of ‘high risk’ and ‘medium risk’ services with the possibility to ask the coordinating authority on their own initiative for the authorization to detect (parts of) their service, based on a detection order issued by a competent authority. This would allow providers to take more responsibility in the process of detection on their own services. The Coordinating Authority would still decide whether to request the issuance of the detection order to a competent judicial or independent administrative authority.

The above approach could be combined with other measures to make the detection orders more targeted, including those already specified in the current text, such as limitation to an identifiable part or component of the service, specific types of channels of a publicly available interpersonal communications service, or to specific users or specific groups or types of users, provided that such measures effectively address the risks identified.

2. Protecting cyber security and encrypted data

While some delegations have expressed concerns that providers could be obliged to break into end-to-end encrypted (E2EE) inter-personal communication when executing detection orders or introduce cyber security vulnerabilities , other delegations were of the opinion that technical solutions can be found that do not break E2EE and do not introduce cyber security vulnerabilities, and that excluding services using E2EE from the scope of detection orders would make the regulation less effective in achieving its objectives as a significant portion of CSA would not be covered.

The Presidency therefore proposes in a spirit of compromise to include services using E2EE in the scope of standard detection orders issued to high-risk services, under the condition that a detection order should not create any obligation that would require a provider to create access to end-to-end encrypted data and that the technologies used for detection are vetted with regard to their effectiveness, their impact on fundamental rights and risks to cyber security.

As some delegations have expressed concerns that the current wording on safeguarding cyber security and encryption (Recital 26 and Article 10(3)(e)) is not sufficient, the Presidency considers adding further safeguards to protect cyber security in the operative part of the text and the recitals.

3. Questions to delegations

1. Do you support the idea of developing a risk categorisation for (parts of) services of providers and classifying them into four categories, and do you have suggestions regarding the methodology and the parameters to be applied?

2. Do you support the approach that risk mitigation measures and detection orders should be linked to the risk categorisation?

3. Do you support the establishment of two different kinds of detection orders depending on the risk level of a service?

4. Do you agree that there should be a possibility for providers of hosting services and of interpersonal communications services, under certain conditions, to request to the co-ordinating authority, on their own initiative, the authorization to detect (parts of) their service, based on a detection order issued by a competent judicial or independent administrative authority?

5. Do you agree to include high-risk services using E2EE- in the scope of standard detection orders, under the condition that a detection order should not create any obligation that would require a provider to create access to end-to-end encrypted data and that the technologies used for detection are vetted with regard to their effectiveness, their impact on fundamental rights and risks to cyber security?

6. Do you support the addition of further safeguards to protect cyber security in the operative part of the text and the recitals as suggested by the Presidency?

7. Do you have any additional remarks that the Presidency should consider when further developing the concept and working on consequential changes to other parts of the proposed regulation, including on the EU Centre, resulting from the new approach related to more targeted detection orders and protecting cyber security and encrypted data?