Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2022/0155 (COD)

Brussels, 15 July 2022

WK 10409/2022 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.

MEETING DOCUMENT

From:	General Secretariat of the Council
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

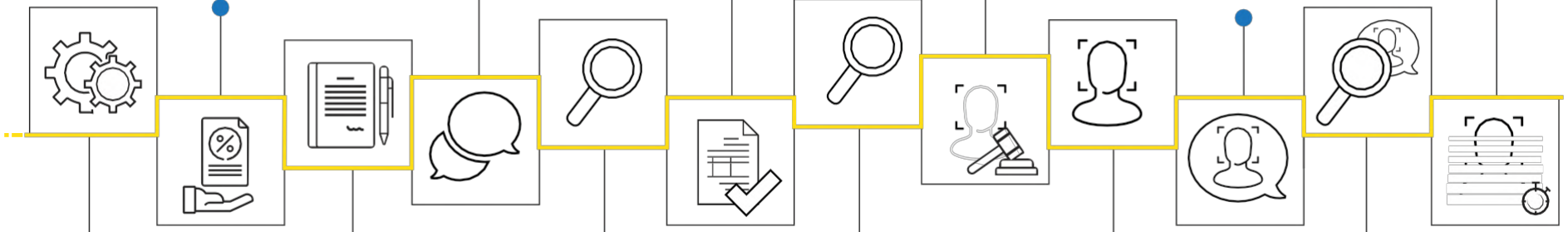
Delegations will find in annex two documents from the Commission services:

- A flowchart of the CSA detection process

- A document outlining the relations between the CSA proposal and the Digital Services Act (DSA), the Terrorist Content Online (TCO) Regulation, the GDPR and the Interim Regulation.

Process for detection orders

PUBLIC



Risk assessment and mitigation
providers assess the risk and implement mitigation measures

Risk reporting
providers report on risk and mitigation measures to Coordinating Authority (CA)

CA check #1
If risk still significant, CA prepares draft detection order

Comments on draft detection order
by the provider & EU centre (4 weeks)

CA check #2
of comments on draft detection order. If necessary, CA requests provider to draft implementation plan for the possible detection order

Implementation Plan
by the provider (including data protection impact assessment) + DPA opinion

CA check #3
of implementation plan. If necessary, CA requests judicial or independent administrative authority to issue detection order

Detection order
issued by judicial or independent administrative authority to start in min 3 months*

Detection
by providers using indicators from the EU centre

Reporting
by providers to the EU centre

Review of reports
by EU centre: stop false positives and forward relevant reports to law enforcement

Removal Orders
(if needed)
issued by judicial or independent administrative authority on request by CA, providers to remove within 24 hours*

* Appeal/redress possibilities

RELATION BETWEEN CHILD SEXUAL ABUSE (CSA) PROPOSAL AND OTHER RELEVANT LEGISLATIVE TEXTS

PUBLIC

This paper describes the relations between the CSA proposal and the legislative instruments most relevant to it, i.e. the Digital Services Act (DSA), the Terrorist Content Online (TCO) Regulation, the GDPR and the Interim Regulation.

1. DSA Proposal (COM (2020) 825 final)[1]

1.1. General

The DSA and CSA proposals share the same legal basis, TFEU article 114.

The DSA proposal is a *horizontal instrument* applicable to providers of intermediary services offered to recipients of the service that have their place of establishment or are located in the Union. Among other things, it creates asymmetric due diligence obligations for providers of intermediary services, including obligations aiming at tackling illegal content. Illegal content under the DSA is defined broadly, as 'any information that in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law'(Article 2(g)). The definition therefore also covers child sexual abuse material (CSAM).

The CSA proposal is a *sectoral instrument* applicable to the relevant providers of information society services, whose services present a risk of being misused for the purpose of online child sexual abuse. It builds on the horizontal framework provided by the DSA, but goes further to impose (i) more specific due diligence obligations with respect to the protection of children from online sexual abuse (in particular, Articles 3 to 6) and (ii) more specific obligations concerning the tackling of a specific type of illegal content, i.e. online child sexual abuse (in particular, Articles 7 to 18). Online child sexual abuse is defined as 'the online dissemination of child sexual abuse material and the solicitation of children' (Article 2(p)). This definition covers known and new CSAM as well as grooming. The CSA proposal defines what constitutes CSAM or grooming by reference to the relevant definitions enshrined in Directive 2011/93.

1.2. Scope of Application

The geographical/territorial scope of the DSA and CSA proposals is identical, while the personal scope (i.e. the type of service providers concerned) and the material scope (i.e. the type of content concerned) differ.

In particular:

[1] Political agreement has been reached on the DSA proposal, but the text of new Regulation has, at present, not yet been finalised and adopted. Therefore, this document is based on the text of the DSA as proposed. The final text of the DSA is unlikely to substantially deviate on the points relevant for the present assessment.

- geographical/territorial scope: EU Digital Single Market – both instruments apply to providers of relevant services as defined in the respective texts, to the extent that they are *offering such services in the Union*, *irrespective of their place of main establishment*.
- personal scope: although there is a degree of overlap, the definition of relevant services differs in the two texts, by virtue of their different aims. The DSA applies to providers of intermediary services (mere conduit, caching, hosting) and most of its provisions apply to providers of online platforms (which is a subcategory of hosting services and which does not include interpersonal communications services), whilst the CSA proposal applies to certain providers of information society services (publicly available interpersonal communications, hosting services, software applications stores, internet access services). The reason for this differentiation is that the CSA proposal only imposes a (differentiated) set of obligations on those information society services that, in principle and by virtue of their nature, either
    - present a risk of misuse for the purpose of online child sexual abuse (this is the case of publicly available interpersonal communications and hosting services), or
    - present a risk of being used as facilitators to online child sexual abuse (this is the case of software applications stores and internet access services);
- material scope: the illegal content relevant for the purpose of the two instruments is different. The DSA refers to all 'illegal content' as (broadly) defined therein, while the CSA proposal refers only to a specific type of illegal content, namely CSAM and grooming (jointly defined as online child sexual abuse). On this, see also the further explanation in section 1.1.

1.3. Risk Assessment, mitigation and risk reporting

The DSA provides for a process of risk assessment, risk mitigation and risk reporting, including independent auditing of risk management for very large online platforms (i.e. reaching at least 45 million of recipients of service). This risk management process will be overseen by the Commission.

The CSA proposal provides for a process of risk assessment, risk mitigation and risk reporting for publicly available interpersonal communication services and hosting services. If a provider is already undertaking a risk assessment under the DSA (Article 26), it will be able to build on it (rather than necessarily having to re-start from the beginning) for the purpose of the risk assessment under the CSA proposal, without prejudice to the need to meet the specific requirements of the CSA proposal. This process under the CSA proposal is overseen by Coordinating Authorities, which are authorities of the Member States conceived as the expertise hub and coordination point for all matters related to the fight against online child sexual abuse at the national level and which are therefore best placed to evaluate the service providers' risk assessment and risk mitigation measures.

1.4. Detection, removal and reporting of illegal content

Although it contains rules on certain orders issued on the basis of national law or other acts of Union law (Articles 8 and 9), the DSA does not provide for the legal basis for orders on the

detection and removal of illegal content in interpersonal communications or hosting services neither in any other type of intermediary services.

Conversely, the CSA proposal does provide for a legal basis for the issuance of orders for the detection and removal of a specific type of illegal content, namely online child sexual abuse.

As regards reporting, both the DSA (Article 21) and the CSA proposal contain certain obligations. However, the main differences are that the CSA proposal's obligations are specifically focused on online child sexual abuse, contains more detailed reporting requirements and couples those requirements with rules on the further processing of such reports.

1.5. Establishment of contact point and legal representative

Both the DSA and the CSA proposal contain rules on contact points and legal representatives of the relevant service providers. To the extent that a provider has already established a point of contact and a legal representative under Articles 10 and 11 of the DSA, there is no need for duplication under Articles 23 and 24 of the CSA proposal.

1.6. Notice and action mechanism

Notice and action mechanisms are regulated by the DSA (Articles 14 to 19 in particular), which provides for a horizontal set of obligations concerning the establishment and functioning of such mechanism by the providers of relevant intermediary services. The relevant framework applies to all illegal content, including CSAM. Hence, it would not have been appropriate to regulate the matter again in the CSA proposal.

Against this framework, the CSA proposal (Article 32) simply enables Coordinating Authorities to notify CSAM. In practice, that can be done through the mechanisms provided for in the DSA.

Where Coordinating Authorities notify CSAM on the basis of Article 32 of the CSA proposal (as opposed to the issuance of a removal order issued under Article 14 of the CSA proposal), this does *not* create any obligation on the notified provider to remove the content. Nonetheless, if the notice allows the provider to identify the illegality of the content without a detailed legal examination (and therefore could lead to the provider acquiring actual knowledge of illegal content on its services), the combined application of both legal frameworks (DSA and CSA) will normally encourage removal, for not doing so can have the effect of making inapplicable the protection granted by the conditional liability exemption under the DSA, in particular for providers of hosting services (Article 5 DSA).

1.7. Level of penalties

The level of penalties envisaged under the CSA proposal is aligned with that under the DSA, including periodic penalty payments, not exceeding 6% of the annual income or global turnover of the preceding business year and penalties relating to the provision of information and submission to on-site inspections not exceeding 1% of the annual income or global turnover of the preceding business year.

1.8. Prohibition of general monitoring obligation

Article 7 DSA states that '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'. This provision essentially reiterates the content of Article 15 of the e-Commerce Directive (Directive 2000/31/EC), which must be read in conjunction with its Recital 47 and in light of case law of the Court of Justice of the EU ('CJEU').

The prohibition of general monitoring concerns obligations of a general nature. As Recital 47 of the e-Commerce Directive clarifies, it does not concern monitoring obligations in a specific case and, in particular, does not affect orders issued by national authorities in compliance with Union law, as interpreted by the CJEU.

This has already been interpreted by the CJEU as not precluding the court order imposing detection and removal of specific items of content confirmed to be illegal, as well as, under certain conditions, the content which is identical or equivalent to content already found to be illegal, provided that the monitoring of and search for the information concerned is limited to information properly identified in the order and does not require the provider to carry out an independent assessment of that content (C-18/18). The case law of the CJEU clarifies that the prohibition of general monitoring obligation reflects the balance, which the Union legislator seeks to strike between the various rights and interests at stake, in the light of the principle of proportionality (C-682/18 and C-683/18).

Against this framework, the assessment of the compliance of the CSA proposal with the fundamental rights to which the prohibition of general monitoring obligations gives expression should take into account, in particular, that under the CSA proposal:

- Detection obligation is not imposed as a generally applicable obligation but can be imposed on a service provider only on a case-by-case basis, and only as a measure of last resort, when risk mitigating measures implemented by the service provider, e.g. safety by design, are not sufficient to achieve the objective at stake.
- Detection is imposed only on those services at risk of misuse of online child sexual abuse or, whenever possible, sub-components of these services. The scope of the detection order must be as targeted as possible.
- Detection is embedded in a series of safeguards (on which see below section 3) and it is ordered, taking into account all the individual circumstances of the specific case, by a judge or independent administrative authority.
- The CSA provisions allowing the issuance of detection orders do not impose excessive obligations, in particular taking into account the objectives pursued, i.e. the fight against a particularly serious crime and the protection of a particularly vulnerable category of victims against very serious harm. The court or independent administrative authority issuing the detection order will also have to comply with the principle of proportionality.
- Detection concerns content that is normally clearly illegal: the illegality of CSAM is in principle not context-dependent, unlike most other types of illegal content.

2. TCO (Regulation (EU) 2021/784)

2.1. General

- Both the TCO and the CSA proposal are sectoral instruments to address different forms of illegal content.
- Both provide for the setting up of national competent authorities with important monitoring and enforcement functions.
- The different nature of the illegal content in question in the two texts (i.e. terrorist content and online child sexual abuse) justifies the need for differentiated approaches on specific questions, as discussed more in detail below.
- Both instruments are consistent with the DSA as a horizontal instrument addressing all forms of illegal content. Each of these three instruments remain at early and different stages of development, i.e. the TCO has recently started to apply, the DSA has been recently agreed at political level, and the CSA proposal is under discussion by the EU legislator.

2.2. Scope

The geographical/territorial scope of application of the two instruments is identical. However, the personal scope of application differs, notably because only the CSA proposal applies to publicly available interpersonal communication services. This is due to the different dissemination model of terrorist content, which is in many cases shared publicly to reach as broad an audience as possible, when compared to online child sexual abuse, which tends to be shared on a one-to-one or one-to-few basis, rather than on public platforms.

2.3. Geographical reach of removal orders and removal deadline

Under the TCO, competent authorities of each Member State has the power to issue removal orders (Article 3), there being a special procedure for cross-border removal orders (Article 4). Under the CSA proposal, the Coordinating Authorities can only request removal orders to be issued against service providers within their jurisdiction (Article 14).

The CSA proposal adopts this model to ensure coherence with the mechanism for risk assessment, mitigation and reporting and for the issuance of detection orders: the Coordinating Authority of establishment is the point of reference for all obligations imposed by the CSA proposal on service providers falling within its jurisdiction. In any event, service providers that have received a removal order will have to remove (or disable access to) the CSAM in all Member States.

As to the deadline given to the relevant service providers for removal (1h under the TCO and 24h under the CSA proposal), this is once again linked to the different dissemination model (typically, much faster for terrorist content).

PUBLIC

2.4. Involvement of judicial or independent administrative authority in issuance of removal order

Under TCO, removal orders are issued by national competent authorities, whilst under the CSA proposal they are requested by Coordinating Authorities, but ultimately issued by judicial or independent administrative authority. This is linked to the higher level of interference with the relevant fundamental rights that is likely to arise in connection to a removal order concerning CSAM (especially when shared through interpersonal communication services).

3. GDPR (Regulation (EU) 2016/679)

3.1. General

The GDPR lays down rules relating to the protection of natural persons with regard to the processing of their personal data. It elaborates a specific fundamental right in the EU Charter, namely the right to the protection of personal data (Article 8 EU Charter).

The CSA proposal aims at protecting several fundamental rights of children, including their right to the integrity of the person (Article 3 of the EU Charter) and their right to data protection (Article 8 of the EU Charter), to the extent that they are threatened by online child sexual abuse.

The CSA is without prejudice to the GDPR (Article 1(3)(d)). The CSA proposal leaves the GDPR unaffected and aims to ensure that the level of data protection required by the GDPR is always guaranteed in connection to matters falling under that proposal.

3.2. Involvement of data protection authorities

Data protection authorities are closely involved throughout process of detection and, in particular, at the stage of:

- Selection of the detection technologies made available through the EU Centre, which will also be subject to a compulsory opinion from the EDPB on each technology (Article 50 CSA proposal)
- Application of the technologies to a specific case:
    - In relation to detection orders concerning known and new CSAM, Articles 35 and 36 of the GDPR apply in the absence of a specific framework set up under the CSA proposal itself. This means that, before implementation of a detection order, the provider will have to conduct a data protection impact assessment and, if the processing to be undertaken is a 'high risk' one, ask for the DPA opinion on its conformity with the GDPR.
    - In relation to detection orders concerning grooming, which involve the highest level of interference with the right to privacy and protection of personal data, the CSA proposal goes beyond the GDPR by requiring the controller to always undergo the prior consultation procedure set out in Article 36 GDPR– in addition to what is required under Articles 35 and 36 of the GDPR - the opinion of the competent DPA *before* a detection order can even be requested. The DPA can provide written advice or utilise any of its powers. The opinion is requested on the

draft implementation plan prepared by the provider. This must be provided to the Coordinating Authorities that have to decide whether or not to request a detection order, as well as to the judicial or independent administrative authorities that have to decide whether to issue such an order when requested.

In addition, given that the CSA proposal is without prejudice to the GDPR, the CSA proposal's rules on supervision and enforcement should not be understood as affecting the powers and competences of the data protection authorities under the GDPR (Recital 54). In other words, those powers and competences remain unaffected and the above only adds to what already follows from the GDPR (and other rules of EU data protection law).

3.3. Automated processing

Article 22 GDPR protects individuals from decisions based solely on automated processing, including profiling, that produce legal effects concerning them (or similarly significantly affect them). The CSA proposal is fully in line with this provision.

Automated processing under the CSA proposal does not lead to any decision based solely on automated processing that produces legal effects concerning individuals. Under the CSA proposal, automated processing by service providers occurs with human oversight and only leads to the submission of a report to the EU Centre. From that point on, i.e. from the point where decisions of the type covered by Article 22 GDPR can be made, including decisions on the launch of investigations or criminal proceedings in respect of a given individual, all such decisions are taken by humans.

4. Interim Regulation (Regulation (EU) 2021/1232)

4.1. General

The Interim Regulation is a temporary instrument, designed to avoid the creation of a protection gap in the fight against online child sexual abuse by providing temporary and strictly limited rules derogating from certain obligations laid down in Directive 2002/58/EC (Article 5(1) and 6(1)).. Before its entry into force (and still today), detection of online child sexual abuse by providers offering their services in the Union occurred on a purely voluntary basis. As a result of the entry into force of an amended version of the European Electronic Communications Code (Directive 2018/1972/EU) broadening the scope of application of the e-Privacy Directive (Directive 2002/58/EU), and in the absence)[2], as of 21 December 2020, providers of

[2] Directive 2002/58/EC applies to the processing of personal data in connection with the provision of publicly available electronic communication services. Until 21 December 2020, the definition of 'electronic communication service' set out in Article 2, point (c), of Directive 2002/21/EC of the European Parliament and of the Council (5) applied. On that date, Directive (EU) 2018/1972 of the European Parliament and of the Council (6) repealed Directive 2002/21/EC. The definition of 'electronic communications service' in Article 2, point (4), of Directive (EU) 2018/1972 includes number-independent interpersonal communications services as defined in Article 2, point (7), of that Directive. Number-independent interpersonal communications services, which include, for example, Voice over internet Protocol, messaging and web-based email services, were therefore brought within the scope of Directive 2002/58/EC on 21 December 2020.

interpersonal communications services would not be able to continue using specific technologies for the voluntary detection of online child sexual abuse on their services.

Hence, the need for adoption of an interim regulation providing for a temporary derogation from the e-Privacy Directive with a view to enabling the continuation of lawful (in particular, GDPR-compliant) voluntary detection activities. The Interim Regulation does not establish a legal basis for processing of such data. The Interim Regulation being a temporary instrument, it only applies until 3 August 2024. After that date, and in the absence of a long-term framework, there will be no legal basis in Union law for providers of certain interpersonal communications services to detect (and, therefore, report) online child sexual abuse on their services. As a consequence, a long term framework providing a legal basis for detection while, at the same time, embedding it within a series of safeguards to ensure a fair balancing of all fundamental rights involved, is needed.

4.2. Scope

The Interim Regulation only applies to certain number-independent interpersonal communications services, enabling them to continue lawful detection, reporting and removal of online child sexual abuse from their services on a voluntary basis. The limited scope is due to the fact that the Interim Regulation is meant to respond to a punctual change in the scope of application of the e-Privacy Directive, namely its applicability to number-independent interpersonal communications services as well, and consequently lack of a legal basis for certain providers to continue such voluntary activities.

The CSA proposal aims at providing a long-term framework governing the detection of online child sexual abuse by all service providers concerned. Hence, it applies more broadly (to publicly available interpersonal communications, hosting services, software applications stores, and internet access services), is much more extensive in the matters that it covers and applies without a limitation in time.

4.3. Safeguards related to detection

The Interim Regulation enables the continuation of lawful voluntary detection of online child sexual abuse on certain number-independent interpersonal communications services under the following conditions:

- proportionality of the processing;
- well-established, state-of-the-art nature and reliability of the detection technologies used;
- use of relevant key indicators for grooming detection;
- obligations for providers, including transparency (submission of annual reports by the providers, provision of information to users), human oversight and/or human intervention, and establishment of appropriate procedures and redress mechanisms.

These conditions are also included in the CSA proposal, but, as it provides a legal basis for processing and being more extensive, they are accompanied by further limits and safeguards, including:

- detection is a last resort measure, to be ordered by the court or an independent administrative authority only when risk mitigation fails to sufficiently address the risk of online child sexual abuse;
- limitation of detection obligations to services (or sub-components of services) that present a risk of online child sexual abuse as defined in the CSA proposal;
- involvement of data protection authorities in the detection process (see above);
- availability of a list of detection technologies kept by the EU Centre and subject to opinion of the EDPB;
- detection to be performed using *only* the indicators provided by the EU Centre (for known CSAM, these indicators correspond to material confirmed to be illegal in the EU by national authorities, while for new CSAM and grooming, they correspond to material analogous to that confirmed to be illegal in the EU by national authorities);
- possibility of judicial review and redress for all parties involved;
- decision to detect no longer left to the service providers, but taken by judicial or independent administrative bodies that will have to take into account the entirety of the relevant legal framework, including an express obligation to balance the fundamental rights at stake, and that have access to both the request by the Coordinating Authority and the opinion of the competent DPA if available;
- reporting to be centralised at the level of the EU Centre, so that obvious false positives can be filtered before they reach law enforcement and feedback can be sent to service providers on false positives so that the accuracy of the detection and reporting process can be constantly improved;
- transparency: not only service providers, but all actors involved in the implementation of the CSA proposal are subject to express and suitable transparency obligations.

4.4. Voluntary detection and legal basis for detection

The Interim Regulation does not provide a legal basis for detection. The CSA proposal provides a legal basis upon which to ground mandatory detection activities conducted in accordance with the safeguards and procedures enshrined therein; namely, the detection orders issued in accordance with the CSA proposal, including the procedural and substantive safeguards provided for.

As to voluntary detection, once adopted, the CSA proposal repeals the Interim Regulation, meaning that from that point on:

- providers of interpersonal communication services will be unable to detect online child sexual abuse on a voluntary basis insofar as EU law and, in particular, the e-Privacy Directive, which will be applicable, does not allow for such activities. Provided that the CSA proposal is adopted in time, these providers will be able to (only) conduct mandatory detection based on a detection order issued in accordance with such a proposal. For those mandatory detection activities, the CSA proposal provides a limitation of the exercise of the relevant rights and obligations provided in the e-Privacy Directive (Article 1(4)).

- Providers of hosting services, which do not fall under the e-Privacy Directive, will remain free to detect online child sexual abuse on a voluntary basis for publically available content, provided that such detection complies with applicable EU law, in particular the requirements of the GDPR. In addition, those providers could also be obliged to detect online child sexual abuse whenever they receive a detection order issued in accordance with the CSA proposal.

PUBLIC