Written comments submitted by Member States

Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

(9068/22)

Contents

BELGIUM

This document contains preliminary comments and questions of Belgium related to the European Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse. We welcome the hard and thorough work that has clearly been put into this topic by the Commission. The problem and the need for EU action in relation to CSAM is quite obvious and Belgium supports a clear legal basis.

We want to share with you the following more general remarks.

Firstly, we underline that we are in favor of the newly proposed **bínding obligations** for providers, including the very important obligation to report online child sexual abuse material. We look forward to studying the details of the different 'orders' that would be created.

We want to underline that – while respecting the need for end-to-end encryption and recognizing the importance of it – **encryption** should not be able to be used as a technical excuse not to fulfill the obligations posed on providers by this Regulation. The legal provisions should indeed be technology-neutral and futureproof, but should at the same time prevent 'technical excuses' being used to circumvent the effectiveness of the imposed obligations, for example by using those reasons as basis for impossibility or disproportionality. The legal provisions should be clear on this. In this regard for example, we wonder about how Article 7(4), first subparagraph, point (b) should be interpreted.

Furthermore, linked to this aspect, we are interested in the Swedish proposal to have a dedicated discussion on the detection technologies to be used.

We confirm the importance of the necessary new obligations while taking into account sufficient guarantees in relation to **privacy and data protection**. In this regard also, we are looking forward to the opinions of the data protection authorities (EDPB and EDPS) as regards how we can ensure a good balance when it concerns the necessary detection of 'grooming'.

Secondly, we confirm it will be important to have a clear picture of what is already taking place at the operational level – especially within Europol – to make sure there would be no duplication, but also to make sure we are aware of which tasks **Europol** would no longer be performing along the lines of this proposal and how exactly Europol would cooperate with the EU center. For example, we know that Europol today also receives reports from the American NCMEC and uses lists of 'indicators'. We would welcome Europol explaining to the LEWP all its current activities related to CSAM. We would also appreciate it if the French and the incoming Czech presidencies would enable Europol to be present during the discussions on the relevant parts of the proposal, because it will be very important to create a very clear picture of all the necessary cooperation in this field.

Thirdly, a big concern of our experts at the operational level is to avoid that reports of CSAM are received multiple times at the national level. The vast numbers of CSAM are already a challenge, so **duplication** of what is being sent to the Member States by all actors should be avoided at all cost. This should be definitely kept in mind when we design the obligations throughout this regulation later on and in the implementation process.

Fourthly, we support the Portuguese proposal to have a clear outline and comparison of how this Regulation relates to the **DSA**. The compatibility of both instruments should be made sufficiently clear to avoid confusion later on. More specifically already we note the following unclarities we would like to receive further explanation on:

- Recitals 7 and 8 are not sufficient for us to understand when and how the DSA will apply in certain cases. We are considering the relevance of including throughout the text where the DSA is followed, to which extent and with which exceptions. Could the Commission provide us with an exhaustive list of the dispositions where the DSA will apply because a matter is not "fully addressed" by this Regulation?
    - For example, the "notice and action" matter seems to be touched upon/covered by Article 12(3) of this Regulation but certainly not "fully". For example, how do the minimum requirements of the content of the notice in Article 14(2) of the DSA come into play? We would appreciate certain use cases about the application of these articles. Also, in Article 12(3) shouldn't 'notice' be used instead of 'flag'? For more clarity, a link should be made with the notice and action of the DSA here in the text of Article 12(3).
    - In relation to Article 32 of the Regulation we think the coordinating authorities should probably be able to use the notice and action mechanism of the DSA. Is it possible they are awarded "trusted flagger status" (Article 19 DSA)?
    - Furthermore, removal orders in Article 14 of this Regulation are also mentioned in the DSA but in the DSA this has a broader application. What if CSAM is identified directly by the relevant national judicial or administrative authorities? Could they send an order directly to the provider as Article 8 of the DSA regulates? And what if CSAM is identified on a service of a provider established abroad? Article 8 of the DSA allows the relevant national judicial or administrative authorities to send an order directly to the provider, even if established abroad. Will this provision of the DSA still apply?
- We noted that the Commission suggested that the digital service coordinators of the DSA could be designated as coordinating authorities. In this regard we wonder however about Article 26(2)(e) because those digital service coordinators will have horizontal tasks under the DSA of which some might indirectly be "related to the prevention or combating of child sexual abuse" (for example supervision of the obligation of the provider to assess the any systemic risks of dissemination of illegal content (including CSAM) via its services and put in place appropriate measures to mitigate this risk (Articles 26 and 27 of the DSA)). If designating the digital service coordinators of the DSA as coordinating authorities in this Regulation is the intention of the Commission, this probably should be clarified in the recitals. Also, what would be the relation (if any) between coordinating authorities and the digital service coordinators (if they are not the same)?
- The designation of the coordinating authority, whether already existing or not, will require legislative work form the Member States. The 2 months deadline in Article 25 is therefore too short. As an example, digital service coordinators in the DSA should be designated within 15 months from the date of entry into force and this should be aligned with the entry into force and application provisions (currently 6 months for CSA Regulation).

Lastly, we still have doubts about whether the **EU center** in the proposed format is the best way forward. We see a lot of pros and contras and are considering the possible alternatives. We will study this further based on the impact assessment and other relevant considerations. We confirm that we have a study reservation on this point.

In relation to the first two chapters we can already provide you with the following more concrete remarks.

Firstly, we want to ask how the terminology and definitions will relate to those used in the TCO Regulation, such as for example for the definitions of 'hosting service' and 'offer services in the Union'. How will this be streamlined and/or how will be prevented that different understanding arises concerning which providers are meant and how EU legislation applies to them?

Secondly, in relation to the blocking order addressed to the web provider we would like to detail our Belgian situation in order to find out whether also other countries have similar issues and whether amendments in the relevant articles are advisable. On the one hand, we note that in Belgium that currently only the top level URLs (so of the main website and not a specific page) can be blocked by the DNS (domain name system) level. On the other hand, Article 16 states that blocking orders are to be addressed to internet access service providers, while not all of them have their own DNS resolver to reconfigure in order to block a certain URL. In that case, the blocking order will have no effect if it is not (also) addressed to the provider of that DNS resolver. Furthermore we would like some clarification on the meaning of 'blocking', since in practice it concerns more a 'not making visible anymore' by reconfiguration of the DNS resolver and in Article 19 'disabling of access' and 'blocking' seem to be understood as two separate activities. What is understood by these terms in practice?

Thirdly, we want to mention the importance of keeping the overview of all instruments that deal with the rights of victims such as the ones that this Regulation provides for in Articles 20 and 21.

DENMARK

At this point in time, we have the following questions and comments which especially revolves around the interfaces between the draft CSA and the proposal for a Digital Services Act.

According to the CSA, the CSA is coherent with the Proposal for a Digital Services Act ("**DSA**") and will regulate hosting services as defined in the DSA (as well as interpersonal communications services etc.)

Services covered by CSA

1. As the DSA only applies on providers of intermediary services and not for 'mere conduit' and for 'caching' services when the service provider is in no way involved with the information transmitted, it would be interesting to know whether the CSA has the same boundaries in relation to these services, or whether the CSA also will include providers of services of 'mere conduit' and for 'caching' services when it is in no way involved with the information transmitted.
2. The DSA defines intermediary services as (i) mere conduit, (ii) caching, (iii) hosting or (iv) online search engines. Has the CSA regulations about caching services and search engines?

Geographical Scope

The DSA applies to intermediary services provided to recipients of the service that have their place of establishment or residence in the Union, irrespective of the place of establishment of the providers of those services, while the CSA's scope is "relevant information society services offering such services in the Union, irrespective of their place of main establishment."

Is there a material difference between the geographical scopes of each of the DSA and the CSA?

Detection orders

As far as we understand, following certain criteria in the CSA, submission of relevant material and transcripts should be submitted to the EU Centre. Is this in breach with the obligations in the DCA (article 7) stating that there shall not be imposed general obligations to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity?

End-to-end encryption

It is our understanding that some interpersonal encryption services applies end-to-end encryption entailing that the service provider does not have access to decryption, and thereby the service provide cannot comply with the detection orders. How will this be countered in the CSA?

Liability

According to the DSA (article 3-5) there is no liability for the hosting service if the hosting service do not have actual knowledge of illegal activities on its services. However, how will a detection order according to the CSA affect such liability in the DSA?

Please inform whether a service provider could be liable or sanctioned by both the DSA and the CSA or whether there is ranking between the two?

Coordinating Authority

Please advice whether there will possible to connect the Coordinating Authority with the Digital Services Coordinator mentioned in the DSA.

FRANCE

Suite à la présentation du projet de règlement portant sur la prévention et la lutte contre les abus sexuels sur mineurs, les autorités françaises portent à la connaissance de la Commission les interrogations suivantes.

Ce texte, qui s'inscrit dans un contexte général de règlementation des espaces numériques, devra nécessairement **s'articuler avec les textes récemment adoptés ou en cours de négociation visant notamment à formuler des obligations au secteur privé** (DSA, DMA, TCO, IA, CSAM, eIDAS, etc). Aussi, les autorités françaises souhaiteraient voir préciser les points suivants :

- Pour quelles raisons un délai de 24h est-il laissé aux hébergeurs pour retirer des contenus pédopornographiques, alors que le règlement TCO ne leur laisse qu'une heure ? - Why is it that hosts are given 24 hours to remove child pornography content, whereas the TCO Regulation only gives them one hour?
- Quels sont les raisons qui ont conduit la Commission à prévoir un mécanisme différent que celui des injonctions de retrait transfrontières, sur le modèle de TCO ? What are the reasons that led the Commission to provide for a different mechanism than cross-border takedown orders, based on the TCO model?
- Qu'en est-il de la représentation dans une œuvre cinématographique ou audiovisuelle de mineurs se livrant à des actes sexuels ? - What about the depiction in a cinematographic or audiovisual work of minors engaged in sexual acts?
- Les transmissions de contenus visés par le projet de règlement entre pairs mineurs et consentants constituent-ils une infraction couverte par le texte ? - Are transmissions of content covered by the draft Regulation between underage and consenting peers an offence covered by the text?
- A-t-il été envisagé que la procédure prévue par les articles 14 et 15 soit harmonisée avec celle prévue par TCO pour les contenus terroristes, afin d'éviter l'accumulation de textes sectoriels qui seront appliqués par les mêmes structures dans certains Etats membres (PHAROS pour la France) ? - Has it been envisaged that the procedure provided for in Articles 14 and 15 be harmonised with that provided for by TCO for terrorist content, in order to avoid the accumulation of sectoral texts which will be applied by the same structures in certain Member States (PHAROS for France)?
- Les obligations de détection de contenus ASM non-connus ou de sollicitations constituent-elles une exception à l'interdiction d'obligations générales de surveillance prévue par la directive e-Commerce, et demain par le DSA ? - Do the obligations to detect non-known ASM content or solicitations constitute an exception to the prohibition of general monitoring obligations provided for by the e-Commerce Directive, and tomorrow by the DSA?
- En matière de gouvernance, ne serait-il pas utile de confier à la Commission la supervision du respect de certaines obligations prévues par le projet de règlement concernant les plus grands acteurs, sur le modèle du DSA ? A défaut, comment s'articulera la supervision de certaines obligations qui sont similaires dans les deux textes (ex. évaluation/atténuation des risques) ? - In terms of governance, would it not be useful to entrust the Commission with the supervision of compliance with certain obligations provided for by the draft regulation concerning the largest players, on the model of the DSA? Otherwise, how will the supervision of certain obligations that are similar in the two texts (e.g. risk assessment/mitigation) be articulated?

Par ailleurs, les autorités françaises estiment qu'il faudra s'assurer que **les cibles du règlement** sont suffisamment clairement définies :

- les moteurs de recherche ou les acteurs du streaming en direct sont-ils concernés ? (Le déréférencement de contenus pourrait-il être prévu en complément des mesures de retrait et de blocage ?) - Are search engines or live streamers concerned? (Could dereferencing of content be provided for in addition to removal and blocking measures?)
- Les transmissions de contenus visés par le projet de règlement entre pairs mineurs et consentants constituent-ils une infraction couverte par le texte ? - Are transmissions of content covered by the draft Regulation between underage and consenting peers an offence covered by the text?
- La proposition de Règlement vise notamment les fournisseurs de services de communications interpersonnelles. Cela s'applique-t-il à des messageries classifiées ? Cela s'étend-il aux services de communications professionnelles – gouvernementaux (i.e. Tchap) ou commerciaux (i.e. LinkedIn) ? - The proposed Regulation is aimed in particular at providers of interpersonal communications services. Does this apply to classified messaging? Does it extend to professional communication services - governmental (e.g. Tchap) or commercial (e.g. LinkedIn)?

Il conviendra de veiller également à ce que les dispositions du texte sont cohérentes avec **les besoins des autorités compétentes** :

- Dans le cadre d'une obligation de retrait, la durée maximale de 6 semaines pendant laquelle le fournisseur ne doit pas divulguer d'information à l'utilisateur afin de ne pas interférer avec les activités d'une enquête en cours, paraît-elle suffisante ? - In the context of an opt-out obligation, does the maximum period of 6 weeks during which the provider must not disclose information to the user in order not to interfere with the activities of an ongoing investigation seem sufficient?
- Par ailleurs, cette demande de non divulgation peut-elle être étendue aux autres obligations ? - Furthermore, can this non-disclosure requirement be extended to other obligations?
- Les recours sont-ils suspensifs ? Are appeals suspensive?
- Quelle coopération avec les pays tiers – NCMEC, Interpol, ICSE ? What cooperation with third countries - NCMEC, Interpol, ICSE?
- Comment pourrait s'adapter le formalisme imposé par le règlement concernant les obligations de retrait et la volumétrie réceptionnée par les plateformes de signalements nationaux ? How could the formalism imposed by the Regulation concerning the withdrawal obligations and the volume received by the national alert platforms be adapted?

Des questions se poseront également concernant **la nouvelle autorité nationale indépendante de coordination** :

- La nouvelle autorité va-t-elle à la fois collaborer avec les forces de sécurité intérieure et s'articuler avec les mécanismes nationaux existants de détection et de demande retrait et de blocage des contenus en lignes (lien avec PHAROS) ? - Will the new authority both collaborate with internal security forces and link up with existing national mechanisms for detecting and requesting the removal and blocking of online content (link with PHAROS)?

- Comment la Commission envisage-t-elle l'articulation d'un signalement au Centre par un fournisseur et le signalement aux autorités compétentes nationales en parallèle ? N'existe-t-il pas un risque de doublon ? - How does the Commission envisage the articulation of an alert to the Centre by a provider and the alert to the competent national authorities in parallel? Is there not a risk of duplication?
- La Commission a-t-elle des informations supplémentaires sur un éventuel mécanisme de déconfliction ? - Does the Commission have any further information on a possible deconfliction mechanism?
- L'article 25 permettra-t-il de confier à un service de police l'application des demandes de retrait (autorité judiciaire ou administrative) et de blocage et à une AAI les missions relevant de la régulation (sanctions, supervision de l'action des fournisseurs de services en ligne, etc.) ? - Will Article 25 allow the enforcement of takedown (judicial or administrative authority) and blocking requests to be entrusted to a police service and the regulatory tasks (sanctions, supervision of the action of online service providers, etc.) to an AAI?

S'agissant de **la problématique du chiffrement**, les autorités françaises souhaiteraient clarifier les points ci-après :

- L'obligation de détection indiscriminée pour l'ensemble des communications interpersonnelles implique-t-elle pas nécessairement un affaiblissement du chiffrement des communications interpersonnelles ? - Doesn't the obligation of indiscriminate detection for all interpersonal communications necessarily imply a weakening of the encryption of interpersonal communications?
- Comment la Commission envisage la préservation du chiffrement des communications privées et les obligations imposées aux fournisseurs ? - How does the Commission envisage the preservation of encryption of private communications and the obligations imposed on providers?
- Sécurité juridique des fournisseurs de services : selon la présentation, les fournisseurs des services concernés seront appelés à assumer l'équation de mise en conformité du plan d'action sur les mesures de détection avec les exigences du RGPD. Comment envisager la sécurité juridique des opérateurs sur la gestion de ce difficile équilibre ? - Legal certainty of service providers: according to the presentation, providers of relevant services will be called upon to assume the equation of compliance of the action plan on detection measures with the requirements of the RGPD. How to envisage the legal security of operators in managing this difficult balance?

Sur **la question du centre européen dédié**, il sera crucial de veiller d'une part à éviter toute forme de doublon avec les compétences et les missions données à Europol, en particulier à la suite de la révision de son mandat, et d'autre part, d'éviter de multiplier le nombre d'agences européennes. Il sera donc important de déterminer la structure la plus adéquate au regard des missions que l'on souhaite confier à ce centre.

- Quelles raisons ont conduit la Commission à faire ce choix de statut ? - What reasons led the Commission to make this choice of status?
- Quel usage de SIENA ou de la plateforme PERCI sans risque de duplication ? - How can SIENA or the PERCI platform be used without the risk of duplication?

GERMANY

GER thanks COM for the initiative and welcomes COM's effort to prevent and combat child sexual abuse. This is also an objective of the coalition treaty. The CSA draft regulation is an important step towards fighting child sexual abuse in the digital space on a European level and reaching better protection for children.

A common legislation including risk assessment, risk mitigation, risk reporting, clear legal basis and a new European Centre may help strengthening prevention and prosecution of child sexual abuse throughout the EU – while recognizing existing structures of content reporting services.

The confidentiality of communications is an important asset in our liberal societies that must be protected. Based on the Charta of Fundamental Rights, everyone has the right to respect for his or her private and family life, home and communications. All regulatory measures must be proportionate, should not go beyond what is necessary to prevent child sexual abuse in the digital space, and must effectively balance the conflicting interests of protecting children from abuse on the one hand and protecting privacy on the other.

GER will contribute to find clear appropriate and permanent ways for measures to help strengthening prevention and prosecution of child sexual abuse throughout the EU. According to GER's coalition treaty secrecy of communication, a high level of data protection, a high level of Cybersecurity as well as universal end-to-end-encryption is essential for GER. The GER coalition treaty opposes general monitoring measures and measures for the scanning of private communications. GER is reviewing the draft proposal in the light of the coalition treaty. For GER it is important that regulation fighting against and preventing the dissemination of child sexual abuse material is in line with our constitutional standards of protection for private and confidential communication.

Regarding the establishment of an EU Centre the EU strategy had a rather comprehensive approach in mind addressing both online and offline prevention. The current proposal appears to primarily support law enforcement activities, while having no explicit mandate for offline prevention measures. From our view, the EU-Centre should additionally be a hub for awareness raising measures and the support of networks (incl. networks of survivors of child sexual abuse). We are convinced that the EU Centre should focus in particular on the prevention of online CSA. However, within the scope of its competence, it should also focus on offline CSA, , when online offenses are associated with offline violence. . Additionally GER advises to implement an equal structure of active participation of those affected by CSA from the beginning in the design of the EU-Centre. The EU Centre aims to provide support for those affected by CSA. However, the current proposal does not provide information concerning the participation of those affected by CSA in the EU-Centre.

Notwithstanding these substantive comments, we are still examining the current proposal to establish the EU Centre as an independent agency.

Our scrutiny reservation includes also but not only the organizational design of a new European Centre, Article 4, and – very generally speaking – the balancing between fundamental rights especially regarding the confidentiality of communication and end-to-end encryption.

GER would very much welcome the possibility of holding technical expert workshops alongside LEWP. Technical workshops would give MS the opportunity to learn more about the technologies at stake regarding detection orders and help improving a common understanding within MS.

We are intensively reviewing the draft regulation and will further comment on it. At this point GER has numerous questions. We would like to thank the Presidency and COM for the opportunity to transmit our questions and initial observations.

GER kindly asks for clarification regarding the following questions. At this point GER priority lies in the following questions:

1. How does EU CSA support the prevention of offline child sexual abuse? Besides the right for information and deletion of CSAM – what supporting measures are planned for victims and survivors of child sexual abuse?
2. Could the COM please give examples of possible mitigation measures regarding the dissemination of CSAM as well as grooming that are suitable for preventing a detection order?
3. Could the COM please explain how age verification by providers respectively App Stores shall be designed? What kind of information should be provided by a user? With regard to grooming your proposal specifically aims at communication with a child user. Shall the identification of a child user be conducted only via age verification? If a risk has been detected will providers be obliged to implanting user registration and age verification? Will there be also a verification to identify adult users misusing apps designed for children?
4. Does the COM share the view that recital 26 indicating that the use of end-to-end-encryption technology is an important tool to guarantee the security and confidentiality of the communications of users means that technologies used to detect child abuse shall not undermine end-to-end-encryption?
5. Could the COM please describe in detail on technology that does not break end-to-end-encryption, protect the terminal equipment and can still detect CSA-material? Are there any technical or legal boundaries (existing or future) for using technologies to detect online child sexual abuse?
6. What kind of (technological) measures does COM consider necessary for providers of hosting services and providers of interpersonal communication in the course of risk assessment? Especially how can a provider conduct a risk assessment without applying technology referred to in Articles 7 and 10? How can these providers fulfil the obligation if their service is end-to-end encrypted?
7. How mature are state-of-the-art technologies to avoid false positive hits? What proportion of false positive hits can be expected when technologies are used to detect grooming? In order to reduce false positive hits, does COM deem it necessary to stipulate that hits are only disclosed if the method meets certain parameters (e.g., a hit probability of 99.9% that the content in question is appropriate)?
8. Does the proposal establish a legal basis for the processing of personal data <u>for providers</u> in the context of a detection order within the meaning of Article 6 GDPR? Does the proposal establish a legal basis for the processing of personal data <u>for the EU-Centre</u> in the context of a detection order within the meaning of regulation 2018/1725?

Additionally we would already like to raise the following questions:

Risk assessment and risk mitigation:

9. Can COM detail on relevant "data samples" and the practical scope of risk assessing obligations? Especially differentiating between providers of hosting services and providers of interpersonal communications services.
10. Can COM confirm that providers voluntary search for CSAM remains (legally) possible? Are there plans to extend the interim regulation, which allows providers to search for CSAM?

11. In Art. 3 par. 2 (e) ii the proposal describes features which are typical for social media platforms. Can COM please describe scenarios in which for those platforms a risk analysis does not come to a positive result?

Regarding detection orders:

12. Recital 23 states that detection orders should – if possible – be limited to an identifiable part of the service e.g. to specific users or user groups. Could COM please clarify how specific users/user groups shall be identified and in which scenarios a detection order should only be issued addressing a specific user/user groups?
13. Are the requirements set out in article 7 para 5 / para 6 / para 7 to be understood cumulatively?
14. Can COM please clarify "evidence of a significant risk"? Is it sufficient that there are more child users on the platforms and that they communicate to the extent described in Article 3?
15. How detailed does the detection order specify the technical measure required of the provider?
16. Can COM please clarify on the requirements of para 5b, 6a, 7b – which standard of review is applied? How can the likelihood in Art. 7 par 7 (b) be measured? Does the principle in dubio pro reo apply in favor of the hosting service?
17. How are the reasons for issuing the identification order weighed against the rights and legitimate interests of all parties concerned under Article 7(4)(b)? Is this based on a concrete measure or abstract?
18. Has COM yet received feedback by the providers, especially regarding article 7? If so, can you please elaborate the general feedback?
19. How concretely does the identification order specify the measure required of the provider? What follows in this respect from Article 7(8) ("shall target and specify [the detection order]"), what from Article 10(2) ("The provider shall not be required to use any specific technology")?
20. On page 10 of the proposal it says "Obligations to detect online child sexual abuse are preferable to dependence on voluntary actions by providers, not only because those actions to date have proven insufficient to effectively fight against online child sexual abuse(…)" What is COMs evidence proving that these voluntary options are insufficient?
21. How does the draft regulation relate to the rights of data subjects under Art. 12 et seq. of the GDPR, in particular Article 22 GDPR?
22. Regarding data protection supervisory authorities existing tasks under GDPR and other existing or currently negotiated European Acts (such as the DSA) how can effective control of identification orders be reached?
23. Does “all parties affected” in Art. 9 include users who have disseminated CSAM or solicited children but who were nevertheless checked?

Technologies

24. Which technologies can be used in principle? Does Microsoft Photo ID meet the requirements?
25. Should technologies used in relation to cloud services also enable access to encrypted content?
26. How is the quality of the technologies assured or validated? How does the CSA proposal relate to the draft AI-Act?

27. How is the equivalence of providers' own technologies to be assessed under Article 10(2) and how does this relate to providers' ability to invoke trade secrets?
28. Can the technology be designed to differentiate between pictures of children in a normal/ not abusive setting (e.g. at the beach) and CSAM?
29. Can text analysis software differentiate a legitimate conversation between adults (parents, relatives, teachers, sport coaches, friends etc) and children from a grooming situation?
30. How do you want to ensure that providers solely use the technology – especially the one offered by the EU Centre - for executing the detection order?
31. How would we handle an error? How should eventual cases of misuse be detected?
32. Could you please elaborate on the human oversight and how it can prevent errors by the technologies used?
33. How do you expect providers to inform users on "the impact on the confidentiality of users' communication"? Is it a duty due to the issuance of a detection order? Or may it be a part of the terms and conditions?
34. Do provider of file/image-hosting, which do not have access to the content they store fall under the scope of the Regulation?

Further provider obligations

35. How do reporting obligations under this proposal relate to current NCMEC reporting? How can the two processes best be streamlined? How can be assured that neither a duplication of reports nor a loss of reports is taking place?
36. Which role should the Coordinating Authority play regarding reporting obligation?
37. Regarding a EU-wide removal of CSAM how does COM deal with national differences regarding criminal law?
38. What number of cases does COM expect for the reports to EU CSA? How many cases will be forwarded to the competent national law enforcement authorities and/or Europol?
39. Will the right to an effective redress be affected by the obligation under art. 14 to execute a removal order within 24 hours?
40. At what point can knowledge of the content be assumed to have been obtained by the provider, is human knowledge required?
41. What standard of review does COM assume with regard to the various "actors" in the information chain in the process of issuing an order? Does this include the requirement for a human assessment/audit in each case?
42. Why should Europol be involved in all cases, i.e. not only in cases of unclear MS responsibility?
43. How can blocking orders be limited in practice to specific content or areas of a service, or can only access to the service as a whole be blocked?
44. Do cloud services have to block access to encrypted content if they receive a suspicious activity report about specific users?

Penalties

45. Why did you choose a latitude of judgement regarding penalties?
46. Does Art. 35 apply to cases of misuse of technology or the omission to establish effective measures to prevent such misuse (Art. 10 para 4)?
47. Why doesn't the proposal follow the sanctions set out in TCO Regulation?

48. Could Article 35(2) be limited to breaches of a central obligation or a small number of central obligations?

Information-sharing systems

49. Article 39 (2) does not provide for the national law enforcement authorities to be directly connected to the information exchange systems. In which way will reports be passed on to national LEAs?

50. What shall the information-sharing system embrace? How can effectiveness and data protection best be balanced?

51. Only EU CSA and Europol will have direct access to the database of indicators (Art 46(5)), how can national LEAs/national coordinating authorities best participate of the information? Does COM consider a new interface necessary in order to let national authorities know that further information might be available?

EU CSA & Europol

52. With regards to the proposed EU Centre's cooperation with Europol, how does the Commission envision the distribution of tasks between the two entities in concrete terms in order to assure that any duplication of effort is avoided?

53. We took notice that the Commission's impact assessment does not examine further the possibility of integrating the tasks of prevention and victim support into FRA and the tasks with relevance for law enforcement into Europol instead of creating a new entity. Rather, it seems that this possibility is discarded after preliminary examination. We would therefore like to know why this option was not examined further in the first place? Moreover, we kindly ask COM to explain the advantages its expects from creating a new entity instead of allocating the tasks to FRA and Europol in combination?

54. The legislative proposal foresees that Europol should provide certain "support services" to EU CSA. What are the concrete means and services EU CSA should draw on at Europol? How can those support tasks be demarcated from the tasks of EU CSA? In that context we would like to ask if and if yes, how many additional resources COM estimates for Europol?

55. How should Europol handle this support in terms of resources and how does COM ensure that such support would not come at the expense of Europol's other tasks?

56. How can the proposed governance structure of EU CSA best be streamlined with Europol's governance structure making sure that no misbalance between the Commission and Member states is created?

57. Article 53(2) of the draft deals with mutual access to relevant information and information systems in relation to Europol. Are we right in assuming that the provision does not regulate access to information as such, because reference is made to the relevant provisions ("in accordance with the acts of Union law regulating such access")? What then is the specific regulatory content of the provision? Please explain.

58. For which period does COM estimate that EU CSA can start its work (while maybe not yet being fully operational)?

59. At what stage of the process are images deleted according to the proposal?

60. According to Article 64(4)(h), the Executive Director of EU CSA to be established may impose financial penalties if there are criminal acts detrimental to the financial resources of the Union. How does this relate to EPPO proceedings?

61. How can the proposal ensure that the competences of EU CSA do not collide with the competences of Eurojust?

IRELAND

Ireland welcomes the new proposal on preventing and combatting child sexual abuse.

It is clear that the voluntary approach has not worked and we welcome therefore the proposed obligation placed on providers to detect, report and remove CSAM on all their services.

Ireland agrees that a fair balance must be struck between measures to protect child victims of sexual abuse and their fundamental rights, and the fundamental rights of other users and of the providers. In light of the privacy concerns around detecting CSAM on online platforms, particularly on interpersonal messaging services, we appreciate the proposal's emphasis of the importance of the fundamental rights of users and the care with which the European Commission has sought to set out a graduated risk assessment and mitigation process in advance of any detection order. It will be important to actively engage with all stakeholders, openly listen to concerns and work together to find an optimum and balanced approach to mitigating these risks.

Ireland looks forward to working with partners to ensure that the Regulation supports fully the prevention of child sexual abuse. It is of utmost importance that child victims be identified, rescued, and safeguarded; perpetrators identified and prosecuted; evidence collected and the chain of evidence to support court proceedings and prosecutions preserved. In the context of online solicitation of children ('grooming'), given the sheer volume of potential perpetrators, further provisions might be considered to facilitate early intervention, prevention and deterrence.

National Authorities

Member States will need to designate national authorities, which will be required to undertake an intensive role in relation to the risk assessment and mitigation process, and in relation to the issuance of detection, removal and blocking orders.

The obligations surrounding these national authorities will need to be reviewed in the context of existing and planned structures within Ireland and taking Ireland's Digital Strategy into account, to determine the most efficient and effective approach to meet the requirements of the Regulation.

Ireland is in the process of setting up a Media Commission, which will have extensive digital regulation and online safety responsibilities. It is also planned that the Media Commission will act as Ireland's Digital Services Coordinator (DSC) under the Digital Services Act.

Ireland recognises that significant responsibility will be placed on our authorities because of the number of large technology companies that have their European headquarters here and we intend that our national competent authorities under the new Regulation will be well resourced and high functioning. During the negotiations, we will be keen to ensure that the roles and responsibilities of national authorities, and the ways in which they interact with other stakeholders, are well defined and effective.

EU Centre

Ireland welcomes the establishment of a new EU Centre, which we think has an important role to play in supporting the operation of the Regulation and supporting other stakeholders.

Ireland was surprised and disappointed to see that the Regulation states the location of the EU Centre (The Hague), particularly as this would seem contrary to the Common Approach on the location of the seats of decentralised agencies, which anticipates that decisions on an agency's seat are taken by agreement between the Member States/Council. As the Commission is aware, Ireland was one of a number of countries that had expressed an interest in bidding to host the new Centre. We expect that this matter will be raised during the negotiations.

Questions

1. We would welcome further details on the role and responsibilities of the national Coordinating Authority, including the interaction of national Coordinating Authorities with LEA's, EU Centre, Europol and service providers. Flow charts would be beneficial in this regard.
2. What resources will be required in Member States to implement the proposed Regulation?
3. What kind of resources would the Commission expect a Competent Authority in a Member State to have, to perform these functions?
4. The Regulation envisages the possibility of designating more than one national Competent Authority.
    a. What tasks does the Commission envisage the second National Competent Authority carrying out? Flow charts would be helpful.
    b. What type of body does the Commission envisage this Competent Authority to be?
5. With regard to the legal and functional independence of a national Coordination Authority as stated in Article 26.2 (a), does the Commission envisage the establishment of a completely new authority? Alternatively, could a Coordinating Authority be part of another established independent body, for example Digital Services Coordinator?
6. With regard to Article 26(2)(e), why are Coordinating Authorities not permitted to have any tasks relating to the prevention or combating of child sexual abuse other than those set out under this Regulation?
7. What role does the Commission envisage will be played by members of the INHOPE Network under the Regulation?
8. How does the Commission envisage the responsibilities of the Executive Director of the EU Centre interacting with the responsibilities of Coordinating Authorities in Member States, for example in relation to following up of findings of audits?
9. Can the Commission elaborate on the expected interaction between the EU Centre, the EU Data Protection Board, the national Competent Authorities and the national Data Protection Authorities?
10. Can the Commission clarify why the seat of the EU Centre is designated in the proposal, as this appears contrary to the Common Approach on the location of the seats of decentralised agencies?
11. What role does the Commission anticipate the EU Centre will play in the prevention and combating of CSA in the "offline" sphere?
12. We would welcome more detail on the expected positive impact of the Regulation in relation to prevention, prosecution of crime and victims' rights.
13. We would welcome the opportunity to gain further insights in respect of measures aimed at supporting Member State law enforcement agencies, particularly in coordinating victim identification efforts undertaken in collaboration with existing victim identification programs e.g. INTERPOL, EUROPOL, etc.

14. The Proposal includes a requirement for internet service providers to block access to specific pieces of content on websites under orders from Coordinating Authorities. However, we have received indications that this type of blocking may be technically impossible with HTTPS, which is now used on almost every website. Can the Commission clarify?
15. At a briefing to INHOPE members, it was indicated that companies will only be able to use the CSAM indicator list made available by the EU Centre; how will the EU Centre compile and distribute this list?
16. Currently companies can voluntarily detect CSAM, in line with the provisions of the ePrivacy derogation, which is due to expire in August 2024. Under the Proposal, it would appear companies would no longer be allowed adopt this voluntary approach to detect CSAM; that detection could only take place when they receive a detection order.
    a. Is this correct?
    b. If this is correct, how does the Commission plan to address the potential "gap" in detection, once the ePrivacy derogation ceases and prior to the issuance of a detection order?
17. How long does the Commission envisage it take companies to be served with a detection order?
18. How does the Commission envisage supporting start-ups, small, medium companies, with completion of risk assessments, introduction of mitigating measures and the effective handling of detection orders?
19. Does the Commission anticipate tension between mandatory reporting requirements under US law for US companies based in the EU and the mandatory reporting requirement under this regulation?
20. How will detection orders cohere in practice with the approaches to dealing with illegal content under the Digital Services Act, including in terms of limitations on liability, the prohibition on general monitoring obligations and the practical results, i.e. detection vs removal or disabling of access, required from service providers?
21. Can the Commission clarify the timeframe from receipt of a suspected CSAM report by the EU Centre to issuing a decision on the report?
22. How does the Commission envisage NCMEC reports and EU Centre reports interfacing, in order to avoid duplication?
23. What safeguards will be in place to ensure data held by the proposed EU Centre is secure?
24. Is it proportionate that sensitive data are to be held by multiple authorities and bodies as foreseen by the Regulation?

ITALY

2022/0155 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down rules to prevent and combat child sexual abuse

(Text with EEA relevance)

Whereas:

(1) Information society services have become very important for communication, expression, gathering of information and many other aspects of present-day life, including for children but also for perpetrators of child sexual abuse offences. Such offences, which are subject to minimum rules set at Union level, are very serious criminal offences that need to be prevented and combated effectively in order to protect children's rights and well-being, as is required under the Charter of Fundamental Rights of the European Union ('Charter'), and to protect society at large. Users of such services offered in the Union should be able to trust that the services concerned can be used safely, especially by children.

(7) This Regulation should be without prejudice to the rules resulting from other Union acts, in particular Directive 2011/93 of the European Parliament and of the Council[1], Directive 2000/31/EC of the European Parliament and of the Council[2] and Regulation (EU) …/… of the European Parliament and of the Council[3] [*on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*], Directive 2010/13/EU of the European Parliament and of the Council[4], Regulation (EU) 2016/679

Commented [Autore sc1]: What does it mean? We believe that this extremely wide purpose to protect the whole society in the text of a proposal on CSA which has its legal basis in the Art. 114 TFUE is not clear.

Commented [Autore sc2]: We believe that the negotiation should take into consideration the implementation's assessment of the Directive 93/2011 currently ongoing

1 Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (*OJ L* 335, 17.12.2011, p. 1).

2 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ L 178, 17.7.2000, p. 1).

3 Regulation (EU) …/… of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (OJ L ….).

4 Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media service (OJ L 95, 15.4.2010, p. 1).

of the European Parliament and of the Council[5], and Directive 2002/58/EC of the European Parliament and of the Council[6].

(9) Article 15(1) of Directive 2002/58/EC allows Member States to adopt legislative measures to restrict the scope of the rights and obligations provided for in certain specific provisions of that Directive relating to the confidentiality of communications when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society, inter alia, to prevent, investigate, detect and prosecute criminal offences, provided certain conditions are met, including compliance with the Charter. Applying the requirements of that provision by analogy, this Regulation should limit the exercise of the rights and obligations provided for in Articles 5(1), (3) and 6(1) of Directive 2002/58/EC, insofar as strictly necessary to execute detection orders issued in accordance with this Regulation with a view to prevent and combat online child sexual abuse.

(11) A substantial connection to the Union should be considered to exist where the relevant information society services has an establishment in the Union or, in its absence, on the basis of the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States. The targeting of activities towards one or more Member States should be determined on the basis of all relevant circumstances, including factors such as the use of a language or a currency generally used in that Member State, or the possibility of ordering products or services, or using a national top level domain. The targeting of activities towards a Member State could also be derived from the availability of a software application in the relevant national software application store, from the provision of local advertising or advertising in the language used in that Member State, or from the handling of customer relations such as by providing customer service in the language generally used in that Member State. A substantial connection should also be assumed where a service provider directs its activities to one or more Member State as set out in Article 17(1), point (c), of Regulation (EU) 1215/2012 of the European Parliament and of the Council[7]. Mere technical accessibility of a website from the Union should not, alone, be considered as establishing a substantial connection to the Union.

Commented [Autore sc3]: In many MSs, including Italy, is not possible to use "analogy" within criminal law proceedings and trials, so we wonder whether this provision is in accordance with Constitutional Member States legal framework.

Commented [Autore sc4]: This whole section of the provision is not clear to us, can the Commission further explain from the technical point of view what does this practically and operationally means?

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ L 119, 4.5.2016, p. 1).

6 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ('Directive on privacy and electronic communications') (OJ L 201, 31.7.2002, p. 37).

7 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 351, 20.12.2012, p. 1).

(12) For reasons of consistency and technological neutrality, the term 'child sexual abuse material' should for the purpose of this Regulation be defined as referring to any type of material constituting child pornography or pornographic performance within the meaning of Directive 2011/93/EU, ~~which is capable of being disseminated through the~~ use of hosting or interpersonal communication services. At present, such material typically consists of images or videos, without it however being excluded that it takes other forms, especially in view of future technological developments.

(18) In order to ensure that the objectives of this Regulation are achieved, that flexibility should be subject to the need to comply with Union law and, in particular, the requirements of this Regulation on mitigation measures. Therefore, providers of hosting services and providers of publicly available interpersonal communications services should, when designing and implementing the mitigation measures, give importance not only to ensuring their effectiveness, but also to avoiding any undue negative consequences for other affected parties, notably for the exercise of users' fundamental rights. In order to ensure proportionality, when determining which mitigation measures should reasonably be taken in a given situation, account should also be taken of the financial and technological capabilities and the size of the provider concerned. When selecting appropriate mitigation measures, providers should at least duly consider the possible measures listed in this Regulation, as well as, where appropriate, other measures such as those based on industry best practices, including as established through self-regulatory cooperation, and those contained in guidelines from the Commission. When no risk has been detected after a diligently conducted or updated risk assessment, providers should not be required to take any mitigation measures.

(20) With a view to ensuring effective prevention and fight against online child sexual abuse, when mitigating measures are deemed insufficient to limit the risk of misuse of a certain service for the purpose of online child sexual abuse, the Coordinating Authorities designated by Member States under this Regulation should be empowered to request the issuance of detection orders. In order to avoid any undue interference with fundamental rights and to ensure proportionality, that power should be subject to a carefully balanced set of limits and safeguards. For instance, considering that child sexual abuse material tends to be disseminated through hosting services and publicly available interpersonal communications services, and that solicitation of children mostly takes place in publicly available interpersonal communications services, it should only be possible to address detection orders to providers of such services.

(22) However, the finding of such a significant risk should in itself be insufficient to justify the issuance of a detection order, given that in such a case the order might lead to disproportionate negative consequences for the rights and legitimate interests of other affected parties, in particular for the exercise of users' fundamental rights. Therefore, it should be ensured that detection orders can be issued only after the Coordinating Authorities and the competent judicial authority or independent administrative authority having objectively and diligently assessed, identified and weighted, on a case-by-case basis, not only the likelihood and seriousness of the potential consequences of the service being misused for the type of online child sexual abuse at issue, but also the likelihood and seriousness of any potential negative consequences for other parties affected. With a view to avoiding the imposition of excessive burdens, the assessment should also take account of the financial and technological capabilities and size of the provider concerned.

Commented [AM5]: The Directive 2011/93/EU is under revision. Will this revision have impact on the definition used by the Regulation, there will be an authomatic reference to the new version?

Commented [Autore sc6]: This sentence is difficult to understand, whom can identify these best practices the digital market itself? We believe that the reason of this regulation is that the self-regulatory measures have proved to be not sufficient and appropriate to prevent and combat the CSA crimes.

Commented [Autore sc7]: As the expression "insufficient" could be interpreted differently by Nation Competent Authorities (and possibly crate a not harmonized legal framework within the EU)we believe that will be important to define specific criteria and requirements for the National Authorities of Member States.

Commented [Autore sc8]: Can the Commission further explain the reason for such limitation?

Commented [Autore sc9]: As far as we understand the detection order can be issued only by these 3 actors? Is this correct?

(25) Where new services are concerned, that is, services not previously offered in the Union, the evidence available on the potential misuse of the service in the last 12 months is normally non-existent. Taking this into account, and to ensure the effectiveness of this Regulation, the Coordinating Authority should be able to draw on evidence stemming from comparable services when assessing whether to request the issuance of a detection order in respect of such a new service. A service should be considered comparable where it provides a functional equivalent to the service in question, having regard to all relevant facts and circumstances, in particular its main characteristics and functionalities, the manner in which it is offered and used, the user base, the applicable terms and conditions and risk mitigation measures, as well as the overall remaining risk profile.

(33) In the interest of consistency, efficiency and effectiveness and to minimise the risk of circumvention, such blocking orders should be based on the list of uniform resource locators, leading to specific items of verified child sexual abuse, compiled and provided centrally by the EU Centre on the basis of diligently verified submissions by the relevant authorities of the Member States. In order to avoid the taking of unjustified or disproportionate measures, especially those that would unduly affect the fundamental rights at stake, notably, in addition to the rights of the children, the users' freedom of expression and information and the providers' freedom to conduct a business, appropriate limits and safeguards should be provided for. In particular, it should be ensured that the burdens imposed on the providers of internet access services concerned are not unreasonable, that the need for and proportionality of the blocking orders is diligently assessed also after their issuance and that both the providers and the users affected have effective means of judicial as well as non-judicial redress.

(34) Considering that acquiring, possessing, knowingly obtaining access and transmitting child sexual abuse material constitute criminal offences under Directive 2011/93/EU, it is necessary to exempt providers of relevant information society services from criminal liability when they are involved in such activities, insofar as their activities remain strictly limited to what is needed for the purpose of complying with their obligations under this Regulation and they act in good faith.

(43) In the interest of the effective application and, where necessary, enforcement of this Regulation, each Member State should designate at least one existing or newly established authority competent to ensure such application and enforcement in respect of providers of relevant information society services under the jurisdiction of the designating Member State.

(49) In order to verify that the rules of this Regulation, in particular those on mitigation measures and on the execution of detection orders, removal orders or blocking orders that it issued, are effectively complied in practice, each Coordinating Authority should be able to carry out searches, using the relevant indicators provided by the EU Centre, to detect the dissemination of known or new child sexual abuse material through publicly available material in the hosting services of the providers concerned.

(53) Member States should ensure that for infringements of the obligations laid down in this Regulation there are penalties that are effective, proportionate and dissuasive, taking into account elements such as the nature, gravity, recurrence and duration of the infringement, in view of the public interest pursued, the scope and kind of activities carried out, as well as the economic capacity of the provider of relevant information society services concerned.

Commented [Autore sc10]: We would like to have further information on the practical application of such provision since it is not clear to us

Commented [AM11]: It is not clear to us if these relevant Authorities are the Coordinator Authorities or already existing national Authorities.
We would like to ask an explanation on the meaning of the whole sentence.

Commented [AM12]: What does this mean? What kind of activities are we referring to? The activities carried out according to this Regulations provisions?

Commented [AM13]: We believe that this should be further elaborate in the provisions considering that in case of "good faith " the service providers can be exempt for liability. We would also stress the fact that a too generic definition could lead to different interpretetions by judicial national authorities.

Commented [AM14]: What kind of Authority are we referring to? The Coordinating Authority or a different Authority to be created or designated for the administrative task related to the effective application of this Regulation?

Commented [AM15]: What does it mean? There will be an obligation of each Member State to provide certain number of searches or is it only a general requirement?

Commented [Autore sc16]: What kind of penalties? Administrative or criminal penalties/sanctions?

(56) With a view to ensuring that the indicators generated by the EU Centre for the purpose of detection are as complete as possible, the submission of relevant material and transcripts should be done proactively by the Coordinating Authorities. However, the EU Centre should also be allowed to bring certain material or conversations to the attention of the Coordinating Authorities for those purposes.

(57) Certain providers of relevant information society services offer their services in several or even all Member States, whilst under this Regulation only a single Member State has jurisdiction in respect of a given provider. It is therefore imperative that the Coordinating Authority designated by the Member State having jurisdiction takes account of the interests of all users in the Union when performing its tasks and using its powers, without making any distinction depending on elements such as the users' location or nationality, and that Coordinating Authorities cooperate with each other in an effective and efficient manner. To facilitate such cooperation, the necessary mechanisms and information-sharing systems should be provided for. That cooperation shall be without prejudice to the possibility for Member States to provide for regular exchanges of views with other public authorities where relevant for the performance of the tasks of those other authorities and of the Coordinating Authority.

(64) Given the sensitivity of the data concerned and with a view to avoiding any errors and possible misuse, it is necessary to lay down strict rules on the access to those databases of indicators and databases of reports, on the data contained therein and on their security. In particular, the data concerned should not be stored for longer than is strictly necessary. For the above reasons, access to the database of indicators should be given only to the parties and for the purposes specified in this Regulation, subject to the controls by the EU Centre, and be limited in time and in scope to what is strictly necessary for those purposes.

(65) In order to avoid erroneous reporting of online child sexual abuse under this Regulation and to allow law enforcement authorities to focus on their core investigatory tasks, reports should pass through the EU Centre. The EU Centre should assess those reports in order to identify those that are manifestly unfounded, that is, where it is immediately evident, without any substantive legal or factual analysis, that the reported activities do not constitute online child sexual abuse. Where the report is manifestly unfounded, the EU Centre should provide feedback to the reporting provider of hosting services or provider of publicly available interpersonal communications services in order to allow for improvements in the technologies and processes used and for other appropriate steps, such as reinstating material wrongly removed. As every report could be an important means to investigate and prosecute the child sexual abuse offences concerned and to rescue the victim of the abuse, reports should be processed as quickly as possible.

(71) Considering Europol's mandate and its experience in identifying competent national authorities in unclear situation and its database of criminal intelligence which can contribute to identifying links to investigations in other Member States, the EU Centre should cooperate closely with it, especially in order to ensure the swift identification of competent national law enforcement authorities in cases where that is not clear or where more than one Member State may be affected.

Commented [AM17]: What is the exact meaning of proactively? There will be a control over the activities of the Coordinating Authorities?what kind of guidelines and safegards will be provided?

Commented [Autore sc18]: According to these provisions every Coordinating Authority could have on a bilateral basis different agreements with other Coordinating Authorities. We wonder whether the final information sharing framework at UE level would be efficient and effective.

Commented [AM19]: Will these databases be opened for consultation to non institutional subjects or private parties? Could you give us more detailed information on that particular aspect?

Commented [Autore sc20]: We would like to have further clarification on this sentence.
According to National Criminal Law, Law Enforcement authorities and judicial authorities in many cases should be informed immediately of any possible crime, the assessment of the EU Centre could jeopardise investigations of National investigative authorities

Commented [Autore sc21]: Will the ENU be involved?

(75) In the interest of transparency and accountability and to enable evaluation and, where necessary, adjustments, providers of hosting services, providers of publicly available interpersonal communications services and providers of internet access services, Coordinating Authorities and the EU Centre should be required to collect, record and analyse information, based on anonymised gathering of non-personal data and to publish annual reports on their activities under this Regulation. ~~The Coordinating Authorities~~ should cooperate with Europol and with law enforcement authorities and other relevant national authorities of the Member State that designated the Coordinating Authority in question in gathering that information.

(79) In order to achieve the objectives of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty should be delegated to the Commission to amend the Annexes to this Regulation and to supplement it by laying down detailed rules concerning the setting up, content and access to the databases operated by the EU Centre, concerning the form, precise content and other details of the reports and the reporting process, concerning the determination and charging of the costs incurred by the EU Centre to support providers in the risk assessment, as well as concerning technical requirements for the information sharing systems supporting communications between Coordinating Authorities, the Commission, the EU Centre, other relevant Union agencies and providers of relevant information society services.

HAVE ADOPTED THIS REGULATION:

Article 2

Definitions

(l) 'child sexual abuse material' means material constituting child pornography or pornographic performance as defined in Article 2, points (c) and (e), respectively, of Directive 2011/93/EU;

(o) 'solicitation of children' means the solicitation of children for sexual purposes as referred to in Article 6 of Directive 2011/93/EU;

(q) 'child sexual abuse offences' means offences as defined in Articles 3 to 7 of Directive 2011/93/EU;

(u) 'Coordinating Authority of establishment' means the Coordinating Authority for child sexual abuse issues designated in accordance with Article 25 by the Member State where the provider of information society services has its main establishment or, where applicable, where its legal representative resides or is established;

(w) 'main establishment' means the head office or registered office of the provider of relevant information society services within which the principal financial functions and operational control are exercised.

Commented [Autore sc22]: According to what kind of criteria, safeguards and guidelines? These activities will be carried out on all data and users?

Commented [Autore sc23]: We believe that the Council should be involved, especially in the definition of the rules concerning the access of databases

Commented [AM24]: Considering that the new Directive proposal to implement Directive 93/2011 is expected to be published in the first quarter of 2023 we wonder if the definitions of this section will be modified accordingly in case of new definitions within the text of the new Directive on CSA.

Commented [AM25]: See comment above

Commented [AM26]: See comment on letter l)

Commented [AM27]: We would like to have more clarification on this definition since the "main established principle" and "residence" of legal representative of the information society services could be differently interpreted by Member States authorities according with national jurisdiction law. Moreover we would like to have clarification if these 2 principles are alternatives or the first should be considered prevalent and the letter could only be applicable if the "main establishment" is not applicable?

Commented [AM28]: See comment below, we are not fully convinced that these criteria could be enough clear to avoid overlapping, shortcomings and legal disputes. The risk to be avaided is the time waste before reporting to the LEA the CSA crime information to carry out the investigation.

Article 7

Issuance of detection orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a detection order requiring a provider of hosting services or a provider of interpersonal communications services under the jurisdiction of that Member State to take the measures specified in Article 10 to detect online child sexual abuse on a specific service.

2.

Article 11

Guidelines regarding detection obligations

The Commission, in cooperation with the Coordinating Authorities and the EU Centre and after having conducted a public consultation, may issue guidelines on the application of Articles 7 to 10, having due regard in particular to relevant technological developments and the manners in which the services covered by those provisions are offered and used.

Article 14

Removal orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a removal order requiring a provider of hosting services under the jurisdiction of the Member State that designated that Coordinating Authority to remove or disable access in all Member States of one or more specific items of material that, after a diligent assessment, the Coordinating Authority or the courts or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material.

Article 16

Blocking orders

1. The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or an independent administrative authority of that Member State to issue a blocking order requiring a provider of internet access services under the jurisdiction of that Member State to take reasonable measures to prevent users from accessing known child sexual abuse material indicated by all uniform resource locators on the list of uniform resource locators included in the database of indicators, in accordance with Article 44(2), point (b) and provided by the EU Centre.

Commented [AM29]: The role and prerogatives of the Coordinating Authorities are extremely important, we would like to have further clarification on the expected framework of the whole functioning system of the detection order from first evidence of a possible CSA to the the issue of the order of the judicial or independent administrative authority. Please also consider that together with the administrative procedures also criminal judicial orders can be issued on the CSA so we would like to know how exactly the two dimension can be harmonized.

Commented [AM30]: We believe that the investigative activities ongoing or upcoming on the CSA should be considered in the guidlines

Commented [AM31]: See comments submitted with reference to art. 7

Commented [AM32]: Recalling what said with reference to art. 7 we think that is pivotal to deeply evaluate the impact of the Blocking order on possible criminal investigation ongoing or upcoming on the CSA crime .

Article 20

Victims' right to information

1. Persons residing in the Union shall have the right to receive, upon their request, from the Coordinating Authority designated by the Member State where they reside, information regarding any instances where the dissemination of known child sexual abuse material depicting them is reported to the EU Centre pursuant to Article 12. Persons with disabilities shall have the right to ask and receive such an information in a manner accessible to them.

That Coordinating Authority shall transmit the request to the EU Centre through the system established in accordance with Article 39(2) and shall communicate the results received from the EU Centre to the person making the request.

Commented [AM33]: In order to include also those who work or study abroad and are not currently residing in the EU we would like to add the words "EU Citizens".

Article 22

Preservation of information

2. Providers shall preserve the information referred to in paragraph 1 for no longer than necessary for the applicable purpose and, in any event, no longer than 12 months from the date of the reporting or of the removal or disabling of access, whichever occurs first.

They shall, upon request from the competent national authority or court, preserve the information for a further specified period, set by that authority or court where and to the extent necessary for ongoing administrative or judicial redress proceedings, as referred to in paragraph 1, point (d).

Providers shall ensure that the information referred to in paragraph 1 is preserved in a secure manner and that the preservation is subject to appropriate technical and organisational safeguards. Those safeguards shall ensure, in particular, that the information can be accessed and processed only for the purpose for which it is preserved, that a high level of security is achieved and that the information is deleted upon the expiry of the applicable time periods for preservation. Providers shall regularly review those safeguards and adjust them where necessary.

Commented [AM34]: Even if a criminal investigation is ongoing?

Article 24

Legal representative

1. Providers of relevant information society services which do not have their main establishment in the Union shall designate, in writing, a natural or legal person as its legal representative in the Union.

Commented [AM35]: What will be the consequences if the Information society does not do it?

Article 38

Joint investigations

1. Coordinating Authorities may participate in joint investigations, which may be coordinated with the support of the EU Centre, of matters covered by this Regulation, concerning providers of relevant information society services that offer their services in several Member States.

   Such joint investigations are without prejudice to the tasks and powers of the participating Coordinating Authorities and the requirements applicable to the performance of those tasks and exercise of those powers provided for in this Regulation.

2. The participating Coordinating Authorities shall make the results of the joint investigations available to other Coordinating Authorities, the Commission and the EU Centre, through the system established in accordance with Article 39(2), for the fulfilment of their respective tasks under this Regulation.

Commented [AM36]: Is this provision referred to only joint administrative investigations? What will be the relations with possible joint investigation teams carried out by Eurojust in case of criminal offnces?

HUNGARY

HU fully supports the objectives of the draft regulation; however, we have some general comments regarding its approach on certain important elements.

The proposed legislation appears to have a complex enforcement structure, with no clear or well-defined competences, even though it builds on the solutions used in the draft Digital Services Regulation (hereinafter "DSA") and in Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on combating the dissemination of terrorist content online (hereinafter "TCO"). According to the TCO Regulation, the coordinating authority and the judicial or independent administrative authority are one and the same, but they are separate authorities in the draft Regulation laying down rules for preventing and combating sexual abuse of minors (hereinafter 'CSA'). A simpler solution is for the competent authority to be able to issue blocking or removal orders itself, rather than having to go to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplications should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

The limitations of URL-based screening in the draft proposal could undermine the effectiveness of the CSA Regulation and it would therefore be appropriate to include digital fingerprint-based screening among the technical options.

In Hungary, the problem of end-to-end encryption, which makes it difficult to detect certain crimes and to access and use electronic evidence in criminal proceedings, poses a significant challenge, and it is therefore essential to create the technical conditions for law enforcement agencies to have access to e-evidence, while ensuring appropriate safeguards. In order to act more effectively, possible solutions in this area need to be explored and the Europol Innovation Lab will increasingly provide priority support in this exploration.

We agree with the delegations that called for Europol to be involved in the negotiations on the draft as soon as possible.

It is not clear from the proposal how the new institutional system will draw on the experience of INHOPE and the Member States' Internet hotlines and incorporate them into the institutional system.

In Article 83(2)(a), the proposal provides for data collection based on "gender"; however, for Hungary only the data collection on the basis of biological sex would be acceptable.

The role, competences, and location of the EU centre to be established should be deeply discussed.

Chapter I

We agree with the subject matter and scope set out in Article 1 of the draft, with the reference in Article 1(4) to Chapter 2, Section 2 of the Regulation.

The definitions need to be reviewed. In Article 2 of the draft, we propose to include in point (j) of the definitions an age limit of 18 years or a reference to the age of consent of the Member States, 17 years being unacceptable in this form. We suggest to change it in coherence with the previous definition, or refer to the different interpretation within the MSs.

Chapter II

The title of the chapter does not reflect its content. Sections 2 and 4 already deal with the issuance of a detection and removal decision, which concerns the role of the coordinating authority rather than that of the service provider. The wording of the regulation is very far from meeting the requirement of clear, unambiguous and transparent regulation. It would be good if these powers could be merged or restructured.

In Article 3 par 4 (Subsequently, the provider shall update the risk assessment where necessary and at least once every three years from the date at which it last carried out or updated the risk assessment) the timeframe looks a bit too long, this assessment should be a living exercise

The question of whether the condition in Article 7(4)(a) is fulfilled is partly a police matter, while all other tasks could be carried out by a designated authority, as in the TCO Regulation. The wording of Article 7(4) is incorrect, as it seems to completely exclude the discretion of a judicial authority or an independent administrative body, whose decision is formal if the conditions are met. If this is the aim, it also seems more realistic to concentrate powers in the hands of the judicial authority or the independent administrative body.

The language of the orders as defined in sections 2 and 4 should be the official language of the issuer and English, not the language requested by the service provider. Significant additional administrative burden and costs may be induced by translations. We require here a ruling on the official language of the Coordinating Authorithy+English.

Immediate fulfilment of the information obligation in Section 3 Article 12 (undue delay) may cause problems for law enforcement action and should be suspended, if possible, pending the reaction of EU headquarters. Immediate compliance with the obligation to provide information may cause problems for law enforcement action, which should preferably be suspended pending the reaction of EU Centre.

The provisions on victim protection and support services and their information, as set out in Articles 20, 21, do not reflect the fact that victims are necessarily children. There are no rules on representation, the situation and consequences of the sexual exploitation of children within the family are not addressed, and no reference is made to the relevant EU rules in force. We are talking about children victims here, thus we need a very detailed explanation here on requirements and obstacles. The proposed legislation does not cover rules on representation and protection against criminal parents as legal representatives. In accordance with the first two paragraph of Article 21 we should refer on the applicable EU legislation concerning victim protection and support, and we should channel these activities into the existing mechanisms in this field.

Article 22 requires service providers to keep relevant data. The proposal sets a general retention period of 12 months. However, the draft sets long procedural deadlines in a number of places and, although it is stated that derogations from this general deadline may be made to meet specific needs, it would be preferable to increase this general deadline significantly. We should keep the data until these procedures ends. Deadline mentioned above in this text are much longer in anyway. We suggest to open the possibility for 5 years in this proposal.

Chapter III

Our view is that the coordinating authority's remit should be reviewed. Hungary can cover these competences, but not in one organisation. It would also be unwise to codify such a complex organisation at the level of EU regulation, as this approach would generate conflicts of competence and duplication. The tasks of the authorities and the police are mixed up and do not build on each other in a logical way. We want to build on our existing capacities, with appropriate coordination.

Article 26-30 of the draft expects an independent authority as coordinating authority, on the initiative of which another independent authority will have to take a decision, which seems to be an unnecessary duplication. The competences of the coordinating authority include investigative, analytical and evaluative elements. This cannot be done by an independent administrative authority, and the police service should not be burdened with unnecessary coordination and administrative tasks. The possibility of designating other supporting competent authorities is only mentioned in the draft, and then there are no further references to them, so it is not possible to define their role. The system of complex cooperation at national level should not be interfered with in such a deep way, it is proposed to follow the methodology of the TCO.

In Article 35, the level of fines imposed does not converge with existing EU legislation, we see no clear justification for this. We don't understand why this number was chosen; for the TCO it is 4%, the GDPR also. Is this an area that requires more severe sanctions?

The title of Articles 31 and 38 should be modified, their substantive consequences should be clarified, and the draft should not touch on criminal procedure issues. These monitoring activities in Article 31 are normally channelled also to the law enforcement task. Article 38 cannot be defined as investigation from criminal procedure point of view.

Article 36 par 1 rules that where the Commission has reasons to suspect that a provider of relevant information society services infringed this Regulation in a manner involving at least three Member States, it may recommend that the Coordinating Authority of establishment assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation. We would like to know what is the legal basis and information that allows the COM to come to such a conclusion, and where is the background to this in this draft.

Chapter IV

Article 42 designates The Hague in the Netherlands as the seat of the EU Centre. This was objected by several member states. This solution seems logical in terms of efficient use of capacity and the need for close cooperation with Europol, but it should still be a decision for Member States. We support liaison via liaison officers. We believe that more detailed rules are needed for the relationship with Europol.

Chapter V

Regarding the data collection and transparency reporting more detailed analysis is needed, as it seems to be a bit too detailed. Not just statistics, but detailed activity reports from Member States is required. For coordinating authorities, this detailed data provision will be a significant burden.

As mentioned already at the general remarks, Article 83(2)(a), second indent foresees the collection of data on the basis of "gender", which we do not accept. According to the horizontal Hungarian position, we reject the concept of social gender, and for us the collection of data based on biological gender ("sex") is appropriate. Therefore, Article 83(2)(a), the collection of data based on "gender" should be changed to "sex" (i.e. biological sex). For the Hungarian side, we reject the concept of social sex as such, in our view there is only biological sex. Furthermore, in reality, the authorities collect data only on the basis of biological sex, so the mandate cannot be fulfilled in this way.

We try to be as constructive as possible during the negotiations and we will provide our more detailed position within the framework of the discussions within the LEWP.

HAVE ADOPTED THIS REGULATION:

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter and scope

4. This Regulation limits the exercise of the rights and obligations provided for in 5(1) and (3) and Article 6(1) of Directive 2002/58/EC insofar as necessary for the execution of the detection orders issued in accordance with Section 2 of Chapter 2~~+~~ of this Regulation.

Article 2

Definitions

(j) 'child user' means a natural person who uses a relevant information society service and who is a natural person below the age of 18~~7~~ years;

Commented [HU1]: We suggest to change it in coherence with the previous definition, or refer to the different interpretation within the MSs.

Article 3

Risk assessment

4. The provider shall carry out the first risk assessment by *[Date of application of this Regulation + 3 months]* or, where the provider did not offer the service in the Union by *[Date of application of this Regulation]*, by three months from the date at which the provider started offering the service in the Union.

Subsequently, the provider shall update the risk assessment where necessary and at least once every three years from the date at which it last carried out or updated the risk assessment. However:

Commented [HU2]: This timeframe looks a bit too long this assessment should be a living exercise

Article 7

Issuance of detection orders

4. The Coordinating Authority of establishment shall request the issuance of the detection order, and the competent judicial authority or independent administrative authority shall issue the detection order where it considers that the following conditions are met:

Commented [HU3]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

Commented [HU4]: better wording is needed, it is understood that the independent authority does not have any discretionary power in deciding whether or not to issue

Article 8

Additional rules regarding detection orders

2. The competent judicial authority or independent administrative authority issuing the detection order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

The detection order shall be transmitted to the provider's point of contact referred to in Article 23(1), to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).

The detection order shall be drafted in the language declared by the provider pursuant to Article 23(3).

Commented [HU5]: We require here a ruling on the official language of the Coordinating Authorithy+English

Article 12

Reporting obligations

2. Where the provider submits a report pursuant to paragraph 1, it shall inform the user concerned, providing information on the main content of the report, on the manner in which the provider has become aware of the potential child sexual abuse concerned, on the follow-up given to the report insofar as such information is available to the provider and on the user's possibilities of redress, including on the right to submit complaints to the Coordinating Authority in accordance with Article 34.

The provider shall inform the user concerned without undue delay, either after having received a communication from the EU Centre indicating that it considers the report to be manifestly unfounded as referred to in Article 48(2), or after the expiry of a time period of three months from the date of the report without having received a communication from the EU Centre indicating that the information is not to be provided as referred to in Article 48(6), point (a), whichever occurs first.

Commented [HU6]: immediate compliance with the obligation to provide information may cause problems for law enforcement action, which should preferably be suspended pending the reaction of EU Centre

Article 14

Removal orders

Commented [HU7]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

4. The judicial authority or the independent administrative issuing the removal order shall address it to the main establishment of the provider or, where applicable, to its legal representative designated in accordance with Article 24.

It shall transmit the removal order to the point of contact referred to in Article 23(1) by electronic means capable of producing a written record under conditions that allow to establish the authentication of the sender, including the accuracy of the date and the time of sending and receipt of the order, to the Coordinating Authority of establishment and to the EU Centre, through the system established in accordance with Article 39(2).

It shall draft the removal order in the language declared by the provider pursuant to Article 23(3).

Commented [HU8]: It should be the language of the coordinating authority+English

Article 16

Blocking orders

Article 20

Victims' right to information

1. Persons residing in the Union shall have the right to receive, upon their request, from the Coordinating Authority designated by the Member State where they reside, information regarding any instances where the dissemination of known child sexual abuse material depicting them is reported to the EU Centre pursuant to Article 12. Persons with disabilities shall have the right to ask and receive such an information in a manner accessible to them.

That Coordinating Authority shall transmit the request to the EU Centre through the system established in accordance with Article 39(2) and shall communicate the results received from the EU Centre to the person making the request.

Article 21

Victims' right of assistance and support for removal

1. Providers of hosting services shall provide reasonable assistance, on request, to persons residing in the Union that seek to have one or more specific items of known child sexual abuse material depicting them removed or to have access thereto disabled by the provider.

2. Persons residing in the Union shall have the right to receive, upon their request, from the Coordinating Authority designated by the Member State where the person resides, support from the EU Centre when they seek to have a provider of hosting services remove or disable access to one or more specific items of known child sexual abuse material depicting them. Persons with disabilities shall have the right to ask and receive any information relating to such support in a manner accessible to them.

That Coordinating Authority shall transmit the request to the EU Centre through the system established in accordance with Article 39(2) and shall communicate the results received from the EU Centre to the person making the request.

Article 22

Preservation of information

2. Providers shall preserve the information referred to in paragraph 1 for no longer than necessary for the applicable purpose and, in any event, no longer than 12 months from the date of the reporting or of the removal or disabling of access, whichever occurs first.

Commented [HU9]: The proposed regulation seems to have a complex implementation structure, with no clear or well-defined competences, despite the fact that the proposal builds on the solutions used in the DSA and TCO Regulations. In the TCO Regulation the coordinating authority and the judicial or independent administrative authority are one and the same, but in the CSA Regulation they are separate authorities. A simpler solution would be for the competent authority to be able to issue blocking or removal orders itself, rather than having to apply to a separate judicial or administrative authority. The burden on the coordinating authorities is heavy and duplication should be avoided, it would be difficult and costly to set up a national enforcement structure in line with this proposal.

Commented [HU10]: We are talking about children victims here, thus we need a very detailed explantion here on requierments and obstacles. The proposed legislation does not cover rules on representation and protection against criminal parents as legal representatives.

Commented [HU11]: In accordance with this we should refer on the applicable EU legislation corncerning victim protection and support, and we should chanel these activities into the existing mechanisms in this field.

Commented [HU12]: We should keep the data until these procedures ends. deadline mentioned above in this text are much longer in anyway.we suggest to open the possibility for 5 years in this proposal.

Section 1
Coordinating Authorities for child sexual abuse issues

Article 26

Requirements for Coordinating Authorities

2. When carrying out their tasks and exercising their powers in accordance with this Regulation, the Coordinating Authorities shall act with complete independence. To that aim, Member States shall ensure, in particular, that they:

(a) are legally and functionally independent from any other public authority;

(b) have a status enabling them to act objectively and impartially when carrying out their tasks under this Regulation;

(c) are free from any external influence, whether direct or indirect;

(d) neither seek nor take instructions from any other public authority or any private party;

(e) are not charged with tasks relating to the prevention or combating of child sexual abuse, other than their tasks under this Regulation.

Article 31

Searches to verify compliance

Coordinating Authorities shall have the power to carry out searches on publicly accessible material on hosting services to detect the dissemination of known or new child sexual abuse material, using the indicators contained in the databases referred to in Article 44(1), points (a) and (b), where necessary to verify whether the providers of hosting services under the jurisdiction of the Member State that designated the Coordinating Authorities comply with their obligations under this Regulation.

Article 35

Penalties

2. Member States shall ensure that the maximum amount of penalties imposed for an infringement of this Regulation shall not exceed 6 % of the annual income or global turnover of the preceding business year of the provider.

Commented [HU13]: Our view is that the coordinating authority's remit should be reviewed. Hungary can cover these competences, but it would not be advisable to codify such a complex organisation into one organisation, nor at the level of EU regulation, as this approach would create conflicts of competence and duplication.
The tasks of the judicial, administrative authorities and the police are mixed up and do not build on each other in a logical way, and we would like to build on our existing capacities, with proper coordination.

Commented [HU14]: Article 26-30of the draft expects an independent authority as coordinating authority, on the initiative of which another independent authority will have to take a decision, which seems to be an unnecessary duplication. The competences of the coordinating authority include investigative, analytical and evaluative elements, which an independent administrative authority cannot perform, and the police service should not be burdened with unnecessary coordination and administrative tasks. The possibility of designating other supporting competent authorities is only mentioned in the draft, and then there are no further references to them, so it is not possible to define their role. The system of complex cooperation at national level should not be interfered with in such a deep way, it is proposed to follow the methodology of the TCO.

Commented [HU15]: This monitoring activities are normally chanlled also to the LAE task.

Commented [HU16]: we can live with this regulation, we just don't understand why this number was chosen; for the TCO 4%, the GDPR also, this is an area that requires more severe sanctions?

Article 37

Cross-border cooperation among Coordinating Authorities

1. Where a Coordinating Authority that is not the Coordinating Authority of establishment has reasons to suspect that a provider of relevant information society services infringed this Regulation, it shall request the Coordinating Authority of establishment to assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

Where the Commission has reasons to suspect that a provider of relevant information society services infringed this Regulation in a manner involving at least three Member States, it may recommend that the Coordinating Authority of establishment assess the matter and take the necessary investigatory and enforcement measures to ensure compliance with this Regulation.

Commented [HU17]: What is the legal basis and information that allows the COM to come to such a conclusion, and where is the background to this in this draft?

Article 38

Joint investigations

1. Coordinating Authorities may participate in joint investigations, which may be coordinated with the support of the EU Centre, of matters covered by this Regulation, concerning providers of relevant information society services that offer their services in several Member States.

Such joint investigations are without prejudice to the tasks and powers of the participating Coordinating Authorities and the requirements applicable to the performance of those tasks and exercise of those powers provided for in this Regulation.

2. The participating Coordinating Authorities shall make the results of the joint investigations available to other Coordinating Authorities, the Commission and the EU Centre, through the system established in accordance with Article 39(2), for the fulfilment of their respective tasks under this Regulation.

Commented [HU18]: this cannot be definied as investigation from CP point of view.

Article 42

Seat

The seat of the EU Centre shall be The Hague, The Netherlands.

Commented [HU19]: This solution seems logical in terms of efficient use of capacity and the need for close cooperation with Europol, but it should still be a decision for Member States.

Article 53

Cooperation with Europol

Commented [HU20]: More detailed rules are needed on the relationship with Europol.

LATVIA

1. **Removal orders**

In accordance with Article 14(1) of the CSA draft regulation* "*The Coordinating Authority of establishment shall have the power to request the competent judicial authority of the Member State that designated it or another independent administrative authority of that Member State to issue a removal order requiring a provider of hosting services under the jurisdiction of the Member State that designated that Coordinating Authority to remove or disable access in all Member States of one or more specific items of material that, after a diligent assessment, the Coordinating Authority or the courts or other independent administrative authorities referred to in Article 36(1) identified as constituting child sexual abuse material*".

Question: Could the COM provide more detailed explanation why it has been decided to apply a different approach regarding the issuance of removal orders within the CSA draft regulation as compared to the one envisaged in the TCO Regulation** (Article 3(1) of the TCO Regulation states that "*The competent authority of each Member State shall have the power to issue a removal order requiring hosting service providers to remove terrorist content or to disable access to terrorist content in all Member States*")?

2. **Division of competences between Europol and future EU Centre to prevent and combat child sexual abuse (EU Centre)**

Comment: LV finds it important to receive more detailed information from Europol on its ongoing and planned activities with regard to the CSAM; this would help to better understand the potential interaction between Europol and EU Centre from a very practical point of view. LV would also appreciate if Europol could share its views on the proposed cooperation model between Europol and the EU Centre in the CSA draft regulation.

3. **EU Centre's administrative and management structure**

In accordance with Article 55 of the CSA draft regulation "*The administrative and management structure of the EU Centre shall comprise: (a) a Management board, (b) an Executive Board, (c) an Executive Director and (d) a Technology Committee*". LV also notes that in accordance with Article 61(1) of the CSA draft regulation "*The Executive Board shall be composed of the Chairperson and the Deputy Chairperson of the Management Board, two other members appointed by the Management Board from among its members with the right to vote and two representatives of the Commission to the Management Board*"; in accordance with Article 62 of the CSA draft regulation, the Executive Board has a number of significant tasks as compared to the Management Board (for instance, even to appoint the Executive Director and remove him/her from office).

Questions:

- Bearing in mind that the Executive Board is not a common format for EU Agencies, why it has been decided that there is a need to establish the Executive Board within the administrative and management structure of the EU Centre and – in particular – to give to it a number of significant tasks?
- Is the role and – in particular – are the tasks of the Executive Board consistent with the Common Approach of the European Parliament, the Council and the Commission on decentralised agencies?
- Will the Technology Committee interact/cooperate with Europol's Innovation Lab and the EU Innovation Hub for Internal Security? if yes, what is the foreseen interaction/cooperation model?

4. Application deadline

In accordance with Article 89 of the CSA draft regulation, the CSA draft regulation shall apply from six months after its entry into force. LV notes that TCO Regulation began to apply twelve months after its entry into force and DSA*** (in line with the agreement that has been reached between the co-legislators) will apply eighteen months after its entry into force.

Question: Why it has been decided to foresee a considerably shorter deadline (is this linked to the fact that the current (temporary) regulation will apply only until 03/08/2024)?

** Proposal for a Regulation of the European Parliament and of the Council laying down the rules to prevent and combat child sexual abuse (COM (2022) 209 final).*
*** Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79).*
**** Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM (2020) 825 final).*

PORTUGAL

Portugal wishes to underline the importance of this initiative and would like to congratulate the Commission for its thorough preparation .

The proposals constitute an important effort and step forward in combating the CSA phenomenon, its prevention and mitigation. This development is the result of the commitment already made at European level, assessment of needs and resilient effort to improve and operationalize measures

1. We recall that PT has a scrutiny reservation. So this comments are a very preliminary form of contributing to this effort;
2. PT does not agree with article 42, that reverses a path already initiated in other agency's creation without too much explanations;
3. PT also agrees with the 2nd Opinion of the Regulatory Scrutiny Board Opinion conclusions, stating that the *implementation options should be presented in a more open, balanced and complete manner (3)*;
4. PT notes that the proposals lacks sufficient conditions to be observed in relation to the monitoring tools for illegal content, contrary to what is in the temporary Regulation 2021;
5. We would also like to see a more detailed approach on the role that the Centre could play in terms of political and legislative strategy;
6. PT finds that this is especially noticeable regarding Prevention and Victim Assistance: prevention is only focused on digital aspects, assistance references are almost inexistent. We recall the reservations set out in the 2nd Opinion of the Regulatory Scrutiny Board Opinion, related with the Center specially because the proposal is still not sufficiently clear on how the options that include the detection of new child sexual abuse material or grooming would respect the prohibition of general monitoring obligations. In particular the role of the Center is not sufficiently explained, specifically "in the area of prevention and whether the Center will coordinate member States' victims support efforts, including health, legal, child protection , education and employment";

   We would like more detailed information on how "the center will perform proactive search, how the coordination of this task with the detection done by the service provider themselves will be assured and how it will support SME by verifying the illegality of the material" (2) . An assessment of the coordination with existing European funding projects regarding prevention actions and assistance to victims would also be very much welcome;
7. PT wishes to draw the attention to the fact that the relationship with Europol seems to forget that, currently and according to its Regulation, Europol cannot process data in collaboration with industry and private partners, so that the administrative and logistical gains of such an association seem vague and not fundamental. We would also like to stress that the foreseen strong attachment of the Centre to Europol also risks mitigating Europol's operational role and diverting it towards administrative and logistical supervision obligations.

ROMANIA

RO welcomes the Proposal for a Regulation on preventing and combating sexual abuse against children and **considers it beneficial to develop a clear and legally binding framework** for service providers and hosting providers. We consider that **the proposal responds to the need to impose specific detection obligations on service providers**, based on a detection order, as well as clear reporting obligations in order to effectively remove and reduce the exposure of the materials containing sexually abused children. By imposing such effective measures, the sexual exploitation of children in the online environment will be prevented.

RO regulates the obligation for service providers to: **delete, delete / block materials** containing sexual abuse of minors transmitted online, but **there is no obligation to monitor and detect** such materials.

Therefore, we appreciate that **industry involvement is essential** to identify possible technical solutions for detecting and reporting child sexual abuse in encrypted electronic communications, as well as to addressing the challenges and operational opportunities against these crimes.

Regarding the creation of the EU Center for the Prevention and Combating of Child Sexual Abuse, we believe that, in principle, it can provide substantial assistance by receiving various information reports from companies and by sorting and analyzing them, reaching only law enforcement agencies verified information.

We would appreciate **more specific details on the type of the activities that the Center should carry out**, clarifications on the type of analysis that the Center will perform in support of investigations (filters by country, by law, etc.), and the reason for independent operation of Europol.

Thus, we ask COM to **detail the added value that the new Center would bring, respectively the overlaps with other existing tools**.

For example, Europol currently supports MS work with reports of sexual exploitation of minors by unknown individuals who have used IPs from that MS, prepared by the US NGO NCMEC. National Center for Missing and Exploited Children) and transmitted by ICE (U.S. Immigration and Customs Enforcement).

We also mention the GRACE Project, funded by Horizon 2020, which will apply proven machine learning techniques to the development of benchmarks and analysis to combat the sexual exploitation of children.

SLOVENIA

Slovenia expresses thanks for the document «*Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse*» and emphasizes that we support all efforts to combat the sexual exploitation and sexual abuse of children, both in the physical and virtual world.

We see the need to replace the current interim Regulation (EU) 2021/1232 and we support the initiative to set up common EU rules for preventing and combating child sexual abuse online.

Slovenia would like to express our scrutiny reservation regarding the mentioned Proposal. We believe that it is of utmost importance to have a thorough discussion on the details of the Proposal.

Following the presentation of the proposal at the LEWP meeting of 18 May 2022, the document is still under examination; however, we can provide some preliminary comments:

1. Definitions (Art. 2)

   We believe the Regulation would benefit from a more detailed definition of the enumerated information society services (point f).

   We ask for a clarification of the reasons behind the different age limits set in points (i) and (j).

   We ask for a clarification of the reasons behind using the term “potential” in the definition of known child sexual abuse material (point m)

2. Issuance of detection orders (Art. 7)

   We would ask for a detailed explanation of the envisaged system of issuing a detection order under the condition that the reasons for issuing this order outweigh negative consequences for the rights and legitimate interests of all parties affected (Art. 7(4)(b)). It is unclear which negative consequences would be considered and how.

3. Clarification of establishing Coordinating Authorities (Chapter III, Section 1)

   We would like to point out that it is not entirely clear who the "Coordinating Authorities of establishment" would be. It is clear from Article 26, paragraph 2, that it must be legally independent and functionally independent of any other public authority.

4. Technologies for detection for providers (Art. 10)

   Do we already know which technologies will be use or they already existed?

SLOVAKIA

Slovak Republic generally welcomes and positively perceives the goal that is being pursued by issuing the draft regulation in question. We consider that the issue of child sexual abuse is insufficiently coordinated within the European Union, so we welcome the introduction of a new entity that will perform this task. We also consider it more than necessary for every electronic service providers have an obligation to participate in the fight against child sexual abuse online.

We consider the material has clear interinstitutional character and needs to be carefully studied by respective institutions within SK as to clarify their opinion and to reach one common position that will be communicated to Brussels. To be able to carry out this process, according to national procedures, we need the proposed material available in Slovak language. Certain limitations also arise regarding our national legislation.

Based on the above, until all relevant state administration entities have agreed and the clear position of the Slovak Republic is clarified we raise a scrutiny reservation on the whole text of the proposal.

Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 12 July 2022

WK 10235/2022 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)
N° prev. doc.:	9068/22
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - comments from delegations

Delegations will find attached the compilation of comments received from Members States on the above-mentioned proposal following the meeting of the LEWP (Police) on 18 May 2022.