



Council of the
European Union

120179/EU XXVII.GP
Eingelangt am 15/11/22

Brussels, 15 November 2022
(OR. en, nl)

14823/22

Interinstitutional File:
2022/0155(COD)

JAI 1474	TELECOM 462
ENFOPOL 563	COMPET 903
CRIMORG 160	MI 827
IXIM 261	CONSOM 294
DATAPROTECT 316	DIGIT 207
CYBER 366	CODEC 1756
COPEN 391	INST 414
FREMP 239	PARLNAT 172

COVER NOTE

From: Senate of the Kingdom of the Netherlands
date of receipt: 15 November 2022
To: The President of the Council of the European Union

Subject: Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse [9068/22 - COM(2022) 209 final]

- Opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion¹ of the Senate of the Kingdom of the Netherlands on the above-mentioned Regulation.

¹ The translation(s) of the opinion may be available on the Interparliamentary EU Information Exchange website (IPEX) at the following address: <https://secure.ipex.eu/IPEXL-WEB/document/COM-2022-209>



Eerste Kamer der Staten-Generaal

Europese Commissie
T.a.v. de heer M. Šeřčovič
Wetstraat 200
1049 Brussel
België

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum 15 november 2022

betreft Voorstel voor een Verordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen (COM(2022)209)

ons kenmerk 172205.01U

Geachte heer Šeřčovič,

De leden van de vaste commissie voor Justitie en Veiligheid hebben in hun commissievergadering van 18 oktober 2022 beraadslaagd over het door de Europese Commissie voorgestelde Voorstel voor een Verordening tot vaststelling van regels ter voorkoming en bestrijding van seksueel misbruik van kinderen.¹ De leden van de fracties **GroenLinks** en de **Partij van de Arbeid** (PvdA) gezamenlijk hebben naar aanleiding van het voorstel enkele vragen. De leden van de fractie van de **Socialistische Partij** (SP) sluiten zich aan bij de gestelde vragen.

De leden van de fracties van GroenLinks en de PvdA hebben fundamentele bezwaren tegen het voorstel omdat het uitgaat van het scannen van alle communicatie van iedereen en het daarmee een ernstige inbreuk maakt op de persoonlijke levenssfeer van mensen. Een dergelijke inbreuk op fundamentele mensenrechten is alleen gerechtvaardigd wanneer een maatregel noodzakelijk, proportioneel en effectief is en hetzelfde doel niet met minder ingrijpende maatregelen kan worden bereikt. Kunt u nader ingaan op de noodzakelijkheid, proportionaliteit en subsidiariteit van het voorstel, mede in het licht van de verwachte effectiviteit?

Bent u van mening dat met deze verordening voor de meest effectieve methode is gekozen voor wat betreft de bestrijding van kindermisbruik online en het voorkomen dat beelden het hele internet overgaan? Zo ja, waarom acht u deze methode de meest effectieve? Hebt u andere methoden overwogen, maar deze niet gekozen? De leden zouden graag meer inzicht willen krijgen in de verschillende opties van de Commissie om dit belangrijke probleem te tackelen. De leden stellen deze vraag omdat zij zich afvragen of de gekozen weg de juiste is en of de Commissie middels deze verordening geen veel te grote berg data over zich afroept die amper nog controleerbaar is, maar anderzijds wel fundamenteel de privacy schendt van te veel gebruikers die toch niet op de radar hadden moeten komen. We vragen de commissie met klem een uitgebreide uiteenzetting te geven over de ontwerpvaarders die op tafel hebben gelegen.

Had het niet meer voor de hand gelegen de bestaande Europese samenwerking op het gebied van de aanpak van online seksueel kindermisbruik, waarbij nationale meldpunten beveiligd meldingen uitwisselen en verzoeken doen aan providers om materiaal te verwijderen, als uitgangspunt te nemen en op onderdelen waar dat nodig is te versterken? Is de huidige werkwijze geëvalueerd? Zo ja, kunt u

¹ COM(2022)209.



datum 15 november 2022
ons kenmerk 172205.01U
blad 2

deze evaluatie aan de Eerste Kamer doen toekomen? Zo nee, bent u bereid een dergelijke evaluatie alsnog te laten uitvoeren?

De leden bekruipen het gevoel dat Europese Commissie in deze te veel voor de troepen uit loopt. In 2019, 8 jaar na inwerkingtreding van de Kindermisbruikrichtlijn, zijn maar liefst 23 inbreukprocedures tegen lidstaten gestart omdat de richtlijn nog niet was geïmplementeerd. Hoe ziet u dit? Preventie (richting pedofielen), harmonisatie (wat is strafbaar, leeftijden en strafmaten) van het strafrecht en directe hulp aan de geschade kinderen is nog altijd te veel een ondergeschoven kind. Bent u dat eens met de leden? Zo nee, waarom niet? Zo ja, dan zien de leden graag een reactie hoe de u hieraan gehoor geeft. Hoe gaat u zorgen dat er meer harmonisatie op bovengenoemde onderdelen is bij de lidstaten onderling zodat samenwerking ook eenvoudiger wordt? Wilt u toezeggen dat u naar een uniforme richtlijn streeft qua leeftijden, straffen en strafmaten?

Kunt u een overzicht geven van partijen (waaronder techbedrijven, nationale meldpunten online seksueel kindermisbruik, opsporingsorganisaties) die in de consultatie input hebben gegeven? Kunt u daarbij aangeven welke bezwaren in de consultatie naar voren zijn gekomen, en of er voorstellen zijn gedaan voor alternatieven

Hoe beoordeelt u in het onderhavige voorstel en in de huidige praktijk de hulp aan slachtoffers en daders of potentiële daders? Hoe kijkt u aan tegen registratie- en identificatieplichten voor het huren van servers?

De leden achten het ondermijnen van encryptie en scannen van al onze privécommunicatie en alle berichten en foto's die je naar vrienden stuurt, veel te ver gaan en daarbij zijn de leden niet overtuigd van de effectiviteit en vrezen zij de implicaties van deze maatregel op meerdere terreinen (function creep). Kunt u ingaan op de zorgen van de leden inzake en achtereenvolgens van de effectiviteit van de voorgestelde maatregelen en dit onderbouwen met onderzoeken en argumentatie? En kunt u tenslotte ingaan op de *function creep* die op de loer ligt?

De verordening verschafft het EU Centrum 'indicatoren van online seksueel misbruik van kinderen'. Op basis waarvan bent u gekomen tot deze indicatoren en heeft u ook overwogen om andere indicatoren te gebruiken? Zo ja welke?

Het EU Centrum dient alle meldingen van aanbieders in ontvangst nemen en controleren op online seksueel kindermisbruik. Kunt u toelichten waarom de bevoegdheid tot beoordeling om vast te stellen of er wel of geen strafbaar feit is gepleegd is toegerekend aan het EU Centrum in plaats van opsporingsdiensten? Hoe is een juridische juiste borging van deze beoordeling gegarandeerd? Acht u de beoordeling hiervan voldoende geborgd in deze? In de lidstaten zelf wordt al diverse wijzen gevolg geven aan de opsporing van materiaal van kindermisbruik. Hoe hebt u geborgd dat de *lessons learnt* worden meegenomen in de verschillende lidstaten? Hebt u overwogen om de beoordeling van strafbare feiten en de handhaving daarop bij de nationale lidstaten te beleggen? Kunt u vanuit het oogpunt van subsidiariteit beargumenteren waarom u hebt gekozen voor het huidige ontwerp?

Daarnaast hebben de leden bezwaar bij de rol die private partijen worden toegedicht. Dit zijn geen politie instanties maar commerciële partijen. Hoe ziet u dit? Bent u bereid de keuze inzake de rol van commerciële partijen te heroverwogen en zo ja, welke opties liggen in uw optiek op tafel?

Vreest u niet dat de communicatie van onschuldige burgers in verkeerde handen valt door deze gekozen vorm? Zo nee, waarom niet? Kunt u hierin een gemotiveerd antwoord geven, waar ze specifiek ingaat op de waarborgen om misbruik van het nieuwe systeem door bedrijven en overheden te voorkomen? Zonder encryptie valt communicatie immers maar al te makkelijk in handen waar deze niet voor is bedoeld. Hoe ziet u dit risico? Kunt u de intenties van fraudeurs, afpersers en dergelijke hierin meenemen in het licht van het onterecht worden aangemerkt als kindermisbruiker? Hoe acht u daarbij dat het scannen op *grooming* handhaafbaar is?

Hoe kijkt u naar de capaciteit in de lidstaten om dit probleem adequaat aan te pakken? Bent u het eens dat de capaciteit gericht moet zijn op bronmaatregelen? Welke ziet u? Hoe kijkt u aan tegen infiltratie van het darkweb? Vindt u dat het voldoende inzet op het identificeren van slachtoffers in plaats van het identificeren van daders? Uiteraard dient het beide te gebeuren maar gelet op beperkte capaciteit, hoe adviseert u om prioriteit te stellen?



datum 15 november 2022
ons kenmerk 172205.01U
blad 3

De Nederlandse regering geeft aan dat een systematiek van verwijderings- detectie- en opsporingsbevel niet goed aansluit op het bestuursrecht, maar beter past bij het strafrecht. Hoe ziet u dit?

Tijdens een technische briefing over de verordening in het Nederlandse Parlement werd toegelicht dat een aanbieder niet verplicht is om specifieke technologieën van het EU Centrum te gebruiken voor de opsporing van seksueel kindermisbruik.² Aanbieders mogen zelf kiezen welke technologieën ze gebruiken zolang de gebruikte technologieën voldoen aan de vereisten van de verordening. Kunt u deze vereisten toelichten? Komen deze vereisten overeen met de Europese Regels van het e-commerce?

De leden hebben ook een vraag over de reikwijdte van het begrip seksueel kindermisbruik in het kader van de verordening. In de kern ziet het begrip seksueel misbruik op het (gedwongen of binnen ene afhankelijkheidsrelatie) ondergaan of verrichten van seksuele handelingen. Begrijpen de leden het goed dat in de verordening ook het ongevraagd doorsturen van seksueel getint beeldmateriaal als seksueel misbruik wordt gezien; ook wanneer er vrijwillig is meegewerkt aan de totstandkoming van het beeldmateriaal? Hoe maakt de verordening onderscheid tussen deze verschillende vormen van seksueel misbruik? Daarbij zijn er ook andere vormen van online uitbuiting die misschien niet direct seksueel getint zijn, maar wel met uiterlijke kenmerken te maken hebben en daadwerkelijk (en soms ergere) effecten in de offline wereld hebben. Zoals een meisje uit een streng islamitische familie die zonder hoofddoek wordt gespot of hand in hand loop met iemand van hetzelfde geslacht of andere cultuur. Ziet de verordening ook op dergelijk misbruik? Hoe houdt de Commissie in haar voorstel rekening met voorbeelden zoals hierboven? De leden vragen u de vorige vraag breed te interpreteren en niet alleen uit te gaan van het voorbeeld van het meisje uit een streng islamitische familie, maar dit slechts als voorbeeld van niet-seksueel misbruik te nemen.

Voor slachtoffers van online seksueel misbruik is het van belang dat het seksueel getinte materiaal zo snel mogelijk verwijderd wordt. Hoe meer tijd er verstreken gaat, hoe wijder het verspreid zal zijn, en hoe lastiger het wordt om het materiaal te verwijderen. Deze leden vragen zich af of met dit voorstel niet onnodig veel tijd verloren gaat bij het verifiëren van de meldingen door het EU Centrum, gezien de hoeveelheid aan meldingen het EU Centrum naar verwachting zal ontvangen. Hoe ziet u dit, ook in relatie tot de huidige praktijk?

Om alle data van verschillende mediaplatformen te controleren moeten aanbieders alle privé communicatie ontsleutelen/decrypten op een bepaalde server. Los van de inbreuk die hiermee gedaan wordt op vele grondrechten, zoals het recht op bescherming van privéleven of vrijheid van meningsuiting, kunnen gebruikers als deze informatie wordt gedeeld of gelekt in gevaar komen. Denk bijvoorbeeld aan jongeren die hun seksuele geaardheid online ontdekken, ook in landen waar sommige geaardheden verboden zijn. Hoe kunt u verzekeren dat de privé communicatie niet in de verkeerde handen terecht kan komen?

In de verordening staat dat persoonlijke communicatie enkel wordt gedeeld indien er sprake is van seksueel misbruik. Volgens de Nederlandse Autoriteit Persoonsgegevens hebben de indicatoren die worden toegereikt door het EU Centrum een foutmarge van 12%. Voor deze mensen wordt persoonlijke informatie onrechtmatig gedeeld met zowel de aanbieder, het EU Centrum als mogelijk de Nationale Coördinerende Autoriteit. Hoe kan het recht op privé-communicatie gewaarborgd worden als 12 van de 100 gevallen een foute melding wordt gemaakt?

De leden van de vaste commissie voor Justitie en Veiligheid zien uw reactie met belangstelling tegemoet.

Hoogachtend,

² Technische briefing in de Tweede Kamer der Staten-Generaal op 4 oktober 2022: [Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik | Debat: Gemist \(tweedekamer.nl\)](#)



datum 15 november 2022
ons kenmerk 172205.01U
blad 4

mr. drs. M.M. de Boer
Voorzitter van de vaste commissie voor Justitie en Veiligheid

European Commission
attn. Mr M. Šefčovič
Wetstraat 200
1049 Brussels
Belgium

date 15 November 2022
subject Proposal for a Regulation laying down rules to prevent and combat child sexual abuse COM(2022) 209
our reference 172205.01U

COURTESY TRANSLATION

Dear Mr Šefčovič,

In their committee meeting on 18 October 2022, the members of the standing committee for Justice and Security of the Senate of the States General discussed the European Commission's proposal for a Regulation laying down rules to prevent and combat child sexual abuse.¹ The members of the parliamentary parties of the GreenLeft Alliance (**GroenLinks**) and the Labour Party (**Partij van de Arbeid/PvdA**) have a number of questions they would like to raise about this proposal. The members of the Socialist Party (**Socialistische Partij/SP**) wish to endorse these questions.

The members of the Parliamentary GreenLeft Party and the Parliamentary Labour Party have fundamental objections to the proposal because it involves the scanning of all communications of every internet user and is thus seriously privacy-intrusive. Such a violation of fundamental human rights is justified only if the measure is necessary, proportionate and effective and the same objective cannot be achieved by less intrusive measures. Would you please comment on the necessity, proportionality and subsidiarity of the proposal, also taking into account its expected effectiveness?

Do you consider that the most effective method of combating online child abuse and preventing images from circulating throughout the internet has been chosen for this Regulation? If so, why do you believe this method to be the most effective? Did you consider but reject other methods? The members would like to gain a better understanding of the various options available to the Commission for tackling this important issue. They are raising this question because they wonder whether the chosen path is the correct one and whether this Regulation will not result in the Commission collecting such a vast amount of data as to make checking it virtually impossible, while at

¹ COM(2022) 209.

date: 15 November 2022
our reference: 172205.01U
blad: 2

the same time fundamentally infringing the privacy of too many users who should not have been on the radar in the first place. We urge the Commission to provide a detailed account of the draft frameworks that were considered.

Would not the more obvious course of action have been to take as the starting point the existing European efforts to cooperate in tackling online child sexual abuse, in which national hotlines securely exchange reports and request providers to remove material, and to strengthen this wherever necessary? Has the current procedure been evaluated? If so, can you forward this evaluation to the Senate? If not, are you prepared to have such an evaluation carried out after all?

The members cannot help but feel that the European Commission is going too far too fast in this regard. In 2019, eight years after the entry into force of the Child Abuse Directive, no fewer than 23 infringement procedures had been launched against Member States for failing to start implementation of the directive. How do you view this? Measures to prevent child abuse (paedophiles), harmonise the criminal law (offences, ages and sentences) and provide direct help to children that have suffered harm are subjects that still receive insufficient attention. Do you agree with the members about this? If not, why not? And if you do agree, the members would like to hear how you are responding to this. How will you ensure that there is greater harmonisation in these fields among the Member States in order to simplify cooperation as well? Will you undertake to strive for a uniform directive in terms of ages, penalties and sentences?

Can you provide an overview of parties (including tech companies, national hotlines for reporting online sexual child abuse and law enforcement agencies) that provided input during the consultations? Can you also indicate what objections were voiced during the consultations and whether proposals were made for alternatives?

How do you assess the assistance provided to victims and to perpetrators or potential perpetrators in the present proposal and in current practice? How do you view the registration and identification requirements for server hire?

The members regard the measures to end encrypted communications and allow the scanning of all private communications and all messages and photos sent to friends as going much too far. They are not convinced of the effectiveness of these measures and fear their implications in several areas (function creep). Can you address the concerns of the members on this subject and then explain the effectiveness of the proposed measures, backing this up with research and reasoned arguments? And, finally, can you address the lurking danger of function creep?

The Regulation provides the EU Centre with 'indicators of online child sexual abuse'. On what basis did you decide on these indicators and did you also consider using other indicators? If so, which ones?

date: 15 November 2022
our reference: 172205.01U
blad 3

The EU Centre is required to ensure that all reports received from providers are checked for evidence of online child sexual abuse. Can you explain why the power to determine whether or not a criminal offence has been committed has been conferred on the EU Centre rather than on law enforcement agencies? How is the legal correctness of this assessment guaranteed? Various ways of detecting child abuse material are already in use in the Member States themselves. How have you ensured that use is made of the lessons learned in the various Member States? Did you consider giving the power to assess offences and enforce the law to the Member States? Can you justify your current choice from the perspective of subsidiarity?

Moreover, the members object to the role given to private parties. These are not police authorities but commercial bodies. How do you view this? Would you be prepared to reconsider your decision on the role of commercial bodies and if so, what options do you think are on the table?

Are you not afraid that the communications of innocent members of the public will fall into the wrong hands because of the system you have chosen? If not, why not? Can you provide a reasoned answer that deals specifically with the safeguards to prevent abuse of the new system by companies and government bodies? After all, without encryption, communications can all too easily fall into the hands of those for whom they are not intended. How do you assess this risk? Can you also address the issue of how fraudsters, extortionists and so forth might seek to exploit the position of people wrongly accused of being a child abuser? In this connection, how do you consider that scanning to detect online grooming is enforceable?

Do you consider that the Member States have the capacity to tackle this problem adequately? Do you agree that capacity should focus on measures at source? What measures do you envisage? How do you view dark Web infiltration? Do you think that it focuses sufficiently on identifying victims rather than perpetrators? Both should naturally be identified, but, given limited capacity, what do you consider should be the priorities?

The Dutch government has indicated that a system of removal and detection orders is not really consistent with Dutch administrative law, but is better suited for use under the criminal law. What is your view on this?

During a technical briefing on the Regulation in the Dutch Parliament, it was explained that a provider is not obliged to use specific EU Centre technologies for the detection of child sexual abuse.² Providers are free to choose which technologies to use as long as they comply with the requirements

² Technical briefing in the House of Representatives of the States General on 4 October 2022: Europese Verordening ter voorkoming en bestrijding van seksueel kindermisbruik | Debat Gemist (tweedekamer.nl)

date: 15 November 2022
our reference: 172205.01U
blad: 4

of the Regulation. Can you explain these requirements? Are these requirements in accordance with the EU's e-Commerce rules?

The members also have a question about the scope of the term child sexual abuse under the Regulation. Essentially, the term sexual abuse means undergoing or performing sexual acts (forced acts or within a relationship of dependence). Are the members correct in thinking that the Regulation also treats the unsolicited forwarding of sexually suggestive images as sexual abuse, even in cases where there has been voluntary participation in the creation of the material concerned? How does the Regulation distinguish between these different forms of sexual abuse? Moreover, there are also other forms of online exploitation that may not be directly sexually suggestive, but involve external characteristics and have actual (and sometimes worse) effects in the offline world. For example, a girl from a strict Muslim family who is spotted without a headscarf or walking hand in hand with someone of the same sex or different culture. Does the Regulation also cover abuse of this kind? How does the Commission take into account examples of this kind in its proposal? The members would request you to interpret the previous question broadly and not to confine your answer to the example of the girl from a strict Muslim family, and instead merely to take this as an example of non-sexual abuse.

It is important for victims of online sexual abuse that the sexually suggestive material is removed as quickly as possible. The longer this takes, the more widely the material will be circulated and the more difficult it will be to remove. The members wonder whether this proposal will not result in much time being lost unnecessarily through the need to have the reports verified by the EU Centre, given the quantity of reports the Centre is expected to receive. What is your view on this, taking into account current practice?

In order to check all data from different media platforms, providers must decrypt all private communications on a particular server. Quite apart from the fact that this will entail the violation of many fundamental rights such as the right to privacy and the right to freedom of expression, users could be put at risk if this information is shared or leaked. Think, for example, of young people who discover their sexual orientation online, possibly in countries where some sexual orientations are prohibited. How can you ensure that private communications do not fall into the wrong hands?

The Regulation states that private communications are shared only in the event of sexual abuse. According to the Dutch Data Protection Authority, the indicators provided by the EU Centre have a 12% margin of error. This means that the private information of the people whose data are wrongly reported will be unlawfully shared with the provider, the EU Centre and possibly the National Coordinating Authority as well. How can the right to privacy in relation to private communications be guaranteed if 12 out of 100 cases are incorrectly reported?

The members of the standing committee for Justice and Security await your reply with interest.

date 15 November 2022
our reference 172205.01U
blad 5

Yours sincerely,

M.M. de Boer
Chair of the standing committee for Justice and Security