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 (**Socialistiche 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.

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?

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)

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.

Yours sincerely,

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