Statement 1/2024 on legislative developments regarding the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse

Adopted on 13 February 2024

The European Data Protection Board has adopted the following statement:

The European Data Protection Board ('EDPB') acknowledges the importance of the fight against child sexual abuse online[1]. While it welcomes the recent improvements proposed by the European Parliament[2] that remedy some of the main issues of the original Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse[3] (the 'Proposal'), the EDPB calls upon the co-legislators to make sure that any new legal instrument is not ambiguous and fully respects the fundamental rights to privacy and data protection.

Introduction and summary

In short, the EDPB welcomes the many improvements proposed by the Parliament, such as exempting end-to-end encrypted communications from detection orders. However, the text proposed by the Parliament does not seem to fully resolve the main issues flagged by the EDPB and the European Data Protection Supervisor ('EDPS') related to general and indiscriminate monitoring of private communications.

Furthermore, the EDPB regrets that detection orders are not limited to known child sexual abuse material; the use of technologies to detect new child sexual abuse material may also be ordered, despite the fact that the error rates of these technologies are still concerning.

[1] See EDPB-EDPS Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, adopted on 28 July 2022 ('Joint Opinion 4/2022'), para. 10.
[2] https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html.
[3] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM/2022/209 final, 11 November 2022.

Background

On 11 May 2022, the European Commission published the Proposal that would impose qualified obligations on providers of hosting or interpersonal communication services (and other services) concerning the detection, reporting, removing and blocking of known and new online child sexual abuse material ('CSAM'), as well as solicitation of children ('grooming').

The Proposal would also provide for the establishment of a new, decentralised EU agency and a network of national Coordinating Authorities for child sexual abuse issues, to enable the implementation of the Proposal.

In their Joint Opinion 4/2022, the EDPB and the EDPS stressed that the Proposal raises serious concerns regarding the proportionality of the envisaged interference and limitations to the protection of the fundamental rights to privacy and the protection of personal data. In particular, the EDPB and the EDPS underlined that:

- measures permitting access to the content of a communication on a general and indiscriminate basis are likely to affect the essence of the rights guaranteed in Articles 7 and 8 of the Charter of Fundamental Rights of the EU;
- the Proposal lacks clarity on key elements and leaves very broad margins of appreciation, which would lead to legal uncertainty and leaves too much room for misuse or misinterpretation of the rules on CSAM and grooming detection;
- measures envisaged for the detection of unknown CSAM and grooming in interpersonal communication services would in any event go beyond what is necessary and proportionate due to their intrusiveness, their probabilistic nature and the error rates associated with such technologies;
- the Proposal risks to adversely affect the use of encryption technologies and to undermine the security or confidentiality of electronic communications.

On 23 October 2023, the EDPS organised a seminar dedicated to the ongoing legislative works on the Proposal[4], where similar concerns as well as concerns regarding the effectiveness and risks of the Proposal were raised by a broad range of stakeholders.

On 22 November 2023, the Parliament adopted its negotiating mandate[5] ('EP position').

Analysis of the EP position

The EDPB welcomes the many improvements made in the EP position compared to the original Proposal, such as exempting end-to-end encrypted communications from detection orders. Additionally, the EDPB welcomes that the EP position removes orders to use technologies to analyse audio or written communications[6] from the envisaged detection obligations, and that it stresses the

[4] The event agenda, briefing note, video recording and summary report can be accessed here: https://edps.europa.eu/data-protection/our-work/publications/events/2023-10-23-edps-seminar-csam-point-no-return_en.

[5] https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html.

[6] However, the EDPB noted some inconsistencies in the text regarding the detection of solicitation of children (see e.g. amendment 194, which still mentions detection orders regarding solicitation of children). Moreover, the EDPB is concerned that the exclusion might prove to only be temporary in light of Article 88a of the EP position.

importance of respecting data protection criteria if age verification systems were to be implemented by service providers[7]. However, the text proposed by the Parliament does not seem to fully resolve the main issues flagged by the EDPB and the EDPS related to general and indiscriminate monitoring of private communications.

The EDPB's main concerns relate to the criteria set out in the EP position for issuing detection orders. If read in isolation, Article 7(1) of the EP position would require detection orders to be targeted, specified and limited to individual users, a specific group of users, either as such or as subscribers to a specific channel of communication. Concretely, it would require that there are reasonable grounds of suspicion on individual users, or on a specific group of users, in respect of whom there is a link, even an indirect one, with child sexual abuse material. As a result, it would appear that detection orders should not affect an undefined number of people or extend to all communications exchanged through a specific service.

However, the EP position appears ambiguous as to how detection orders should be 'targeted' and when 'reasonable grounds of suspicion' should be deemed to exist.

'Reasonable grounds of suspicion' are defined in Article 7, paragraph 2, subparagraph 1, letter a) of the EP position as 'those resulting from any information reliable and legally acquired that suggest that individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication might have a link, even an indirect or remote one, with online child sexual abuse material'. However, this definition is complemented by Article 7(5) and (6), which provides for the following non-rebuttable presumptions where such definition is deemed to be met:

- The mitigation measures that the provider has taken, must have insufficient material impact on limiting the systemic risk and the service is being used by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication, to an appreciable extent, for the dissemination of known or new CSAM (Article 7(5) point (a); Article 7(6) point (a) of the EP position); and
- In addition, there must be evidence of the service, having been used in the past 12 months by individual users, or a specific group of users, either as such or as subscribers to a specific channel of communication to an appreciable extent for the dissemination of known or new CSAM (Article 7(5) point (b); Article 7(6) point (b) of the EP position).

The EDPB is of the opinion that this wording does not guarantee that detection orders would actually be targeted and addressed only to individuals who are likely to be involved in the dissemination of CSAM. Rather, in view of the EDPB, the presumptions set out in Article 7(5) and (6) of the EP position are likely to entail that the individuals targeted by the detection orders would not be those who were engaged in the activities described in Article 7(5) and (6) that triggered the reasonable grounds of suspicion. Criteria on how to decide which persons or groups should be targeted by a detection order are missing. In light of this, the EDPB is concerned that the EP position would still allow for the issuance of detection orders that are general and indiscriminate in nature.

[7] For further information, see e.g. guidance issued by the French supervisory authority, available at: https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors, or the Spanish supervisory authority, available at: https://www.aepd.es/guides/decalogue-principles-age-verification-minors-protection.pdf.

Furthermore, the EDPB regrets that the EP position would still provide for the issuance of detection orders for new CSAM, despite the fact that the error rates of the technologies that may be used for this purpose are significant[8].

It is particularly important to address the ambiguities surrounding the issuing of detection orders and to further limit the risk that those orders affect persons who are unlikely to be involved in CSAM-related crimes, given that the detection of suspected CSAM will result in reports being forwarded to a dedicated EU agency and all 'founded' reports further shared by that agency with both national law enforcement authorities and Europol. In this vein, and in view of the concerns already underlined in the Joint Opinion 4/2022 regarding this further processing, the EDPB welcomes the new language on system access and information exchanges between the EU agency and Europol as provided by Article 53(2) of the EP position. The new requirement placed on the dedicated EU agency to conduct a thorough legal and factual analysis prior to the forwarding of reports is, furthermore, an essential minimum safeguard to further mitigate the risk of inaccurate data being shared with law enforcement authorities.

Irrespective of the approach chosen by the Parliament, the EDPB recalls[9] that in the context of interpersonal communications, end-to-end encryption is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider. Preventing or discouraging in any way the use of end-to-end encryption, imposing on service providers an obligation to process electronic communication data for purposes other than providing their services, or imposing on them an obligation to proactively forward electronic communications to third parties would entail the risk that providers offer fewer encrypted services in order to better comply with the obligations, thus weakening the role of encryption in general and undermining the respect for fundamental rights and the trust in digital services.

Conclusion

In conclusion, the EDPB welcomes the direction in which the EP position develops the Commission's Proposal to bring it more in line with fundamental rights standards.

Nevertheless, the EP position falls short of addressing all of the issues raised by the EDPB and the EDPS in their Joint Opinion 4/2022. We therefore urge the co-legislators to make sure that any future text is not ambiguous and fully respects all fundamental rights, including the rights of children and vulnerable people.

For the European Data Protection Board

The Chair

(Anu Talus)

[8] See Joint Opinion 4/2022, paras. 60 et seq.
[9] See Joint Opinion 4/2022, para. 97.