New Controversies around Proposal to Combat Child Sexual Abuse Online

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

Anna Pingen

The proposal to prevent and combat child sexual abuse online, proposed by the Commission on 11 May 2022, remains controversial (→ eucrim 2/2022, 91-92). While more than 70 child rights organisations signed an open letter supporting the EU's proposed law to protect children from sexual abuse, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) pointed out the serious risk the proposal presents for fundamental rights in their Joint Opinion on the proposal adopted on 28 July 2022.

AUTHOR

Anna Pingen
Researcher
Max Planck Institute for the Study of Crime, Security and Law

Published in
2022, Vol. 17(3) eucrim p 173
ISSN: 1862-6947
https://eucrim.eu

While pointing out the particular seriousness and heinousness of sexual abuse of children, the EDPB and the EDPS stressed that the Proposal raises concerns regarding the proportionality of the envisaged interference and the limitations to the protection of the fundamental right to privacy and the protection of personal data. Both pointed out that out that procedural safeguards can never fully replace substantive safeguards.

They criticized that the draft legislation left too much room for potential abuse due to the absence of clear substantive norms. Some key elements, such as the notion of "significant risk" also lack clarity. The broad margin of appreciation afforded to the entities in charge of applying these safeguards (private operators and administrative and/or judicial authorities) leads to legal uncertainty on how to balance the rights at stake in each individual case.

Both the EDPB and EDPS also raised concerns about the measures envisaged for the detection of unknown child sexual abuse material (CSAM) and the solicitation of children (grooming) in interpersonal communication services. Artificial intelligence and other technologies that are used to scan user communications are likely to make mistakes and constitute a significant invasion of people's privacy. The use of technologies to scan audio communication (voice messages and live communications) presents a particular risk of intrusion and should therefore remain outside the scope of detection.

Technologies that use encryption fundamentally support freedom of expression, respect for private life, and communication privacy as well as innovation and expansion of the digital economy. The envisaged blocking measures and requiring providers of Internet services to decrypt online communications in order to block communications involving CSAM are seen as disproportionate. The Proposal must clearly state that nothing in the proposed Regulation should be interpreted as prohibiting or weakening encryption.

The EDPB and EDPS welcomed that the future EU Centre on child sexual abuse and a network of national coordinating authorities for child sexual abuse will not affect the powers and competences of the data protection authorities. The Proposal should, however, clarify the purpose the opinion of the EDPB will have,

once it is issued, on the technologies the EU Centre would make available in order to execute detection orders and how the EU Centre could act after having received an opinion from the EDPB.

Lastly, the EDPB and EDPS supported the envisaged close cooperation between the EU Centre and Europol but made several recommendations for improvement of the relevant provisions, including that the transmission of personal data between the EU Centre and Europol only take place on a case-by-case basis, following a duly assessed request, and via a secure exchange communication tool, such as the SIENA network.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union