Press release – Detecting online child sexual abuse requires strong safeguards

The proposed regulation will provide for limited and temporary changes to the rules governing the privacy of electronic communications so that over the top ("OTT") communication interpersonal services, such as web messaging, voice over Internet Protocol (VoIP), chat and web-based email services, can continue to detect, report and remove child sexual abuse online on a voluntary basis.

The committee adopted its position with 53 votes in favour and 9 against, 2 abstentions. MEPs also backed, with 54 to 10, the decision to enter into interinstitutional talks and the composition of the negotiating team.

MEPs' conditions on the use of technologies to detect child sexual abuse online

Online material linked to child sexual abuse is detected through specific technologies that scan the content, such as images and text, or traffic data. Hashing technology could be used for images and videos to detect child sex abuse material, and classifiers and artificial intelligence could be used to analyse text or traffic data and detect grooming ("solicitation"). MEPs, while allowing this practice to continue, agreed that this material has to be processed using technologies that are the least intrusive to privacy.

MEPs demand that the technology used should not be able to understand the substance of the content but only detect patterns. The processed data should be analysed by a person before being reported to authorities. Interactions that are covered by professional secrecy, such as between doctors and their patients, journalists and their sources or lawyers and their clients should not be interfered with.

This legislation should not be interpreted as prohibiting or weakening end-to-end encryption, MEPs underline, and this derogation should not be extended to include audio communications.

Data retention

When no online child sexual abuse has been detected, all data have to be erased immediately, say MEPs. Only in confirmed cases can the strictly relevant data be stored for use by law enforcement for a maximum of three months.

Quote

After the vote, rapporteur Birgit Sippel (S&D, DE) said : "Child sexual abuse is a horrible crime and we have to get better at preventing it, prosecuting offenders and assisting survivors, both online and offline. Parliament therefore wants existing legal scanning practices to continue being used for online child sexual abuse material. However, the Commission has failed to provide basic information about additional technologies they wish to legalise, without knowing if they even exist in the EU: technologies that analyse the content of every message of every user in order to detect patterns that might point to cyber grooming. I am ready to start negotiations as soon as possible in order to find a legally sound solution that respects the EU Charter of Fundamental rights, the GDPR and the rule of law."

Next steps

Negotiations between the co-legislators can start if plenary endorses the EP's mandate, during next week's session.

Background

The European Electronic Communications Code will soon enter into force (deadline for transposition into national law is 21 December 2020) and will extend the scope of the e-privacy directive to 'over the top' inter-personal communication services. The Commission proposed to temporarily amend the e-privacy directive to allow voluntary detection of child sex abuse online to continue, which would otherwise no longer be possible. The period of application of this derogation, originally proposed by the Commission until end of 2025, should not go beyond 2022, according to MEPs.