

(English version)

Question for written answer E-003250/25
to the Commission
Emmanouil Fragkos (ECR)
(18 August 2025)

Subject: Proposed Chat Control law presents new blow for privacy

A review conducted under the Danish Presidency examining the proposal for a regulation on combatting online child sexual abuse material — dubbed the ‘Chat Control’ or CSAM regulation — has raised new, grave concerns about the respect of fundamental rights in the EU.

As it stands, the proposal envisages mass scanning of private communications, including encrypted conversations, raising serious issues of compliance with Article 7 of the Charter of Fundamental Rights by threatening to undermine the data security of citizens, businesses and institutions. A mandatory weakening of end-to-end encryption would create security gaps open to exploitation by cybercriminals, rival states and terrorist organisations, and would also harm the competitiveness of our digital economy.

At the same time, the proposed technical approach is based on automated content analysis tools which produce high rates of false positives, creating the risk that innocent users could be wrongly incriminated, while the effectiveness of this approach in protecting children has not been proven. Parliament and the Council have repeatedly rejected mass surveillance.

1. Considering the mandatory scanning of all private communications, is the proposed regulation compatible with Article 7 of the Charter of Fundamental Rights?
2. How will it ensure that child protection is achieved through targeted measures that are proven to be effective, without violating the fundamental rights of all citizens?
3. How does it intend to prevent the negative impact on cybersecurity and economic competitiveness caused by weakening encryption?

Submitted: 18.8.2025

Answer given by Mr Brunner on behalf of the European Commission
(10 November 2025)

The Commission proposal for a regulation to prevent and combat child sexual abuse ⁽¹⁾ (the proposal) relies on a thorough and publicly available impact assessment ⁽²⁾, including on fundamental rights.

The proposal strives to achieve a fair balance in the protection of all fundamental rights impacted, including the right to privacy and the rights of the child enshrined in Article 24 of the Charter.

Communications companies are the main actors that are capable of detecting explicit videos or videos that are child sexual abuse material. Currently companies are encouraged to do this voluntarily — a practice that has existed for over a decade and proved essential for child protection. Many major investigations in recent have succeeded thanks to this approach.

Data shows that detection by companies has led to the rescue of a significant number of victims and to the arrest of perpetrators ⁽³⁾. The Commission proposal for a regulation to prevent and combat child sexual abuse ⁽⁴⁾ seeks to make this approach mandatory.

The proposal is clearly defined, the terms are closely monitored by data protection authorities and provide guarantees. A similar approach is already being widely used to detect malware and spam.

The proposal includes provisions on detection orders, which are measures of last resort when prevention measures are insufficient. They target only high-risk services, or where applicable, specific users or groups.

Such orders are issued by a judicial or independent administrative authority balancing all the rights at stake and after a thorough assessment of their necessity and proportionality.

The proposal is technology neutral, while acknowledging encryption as an important tool to guarantee the security and confidentiality of the communications of users.

⁽¹⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>.

⁽²⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209>.

⁽³⁾ For sample cases, see the impact assessment accompanying the proposal, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0209>, Annex 7, p. 267.

⁽⁴⁾ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0209>.

When executing a detection order, providers are required to put in place the requisite safeguards to ensure the security and confidentiality of the communications of users.
