

Follow up to the European Parliament non-legislative resolution on the need for targeted criminal provisions and platforms' responsibility to effectively address cyberbullying and online harassment

- 1. Resolution tabled pursuant to Rule 136(2) and (4) of the European Parliament's Rules of procedure**
- 2. References:** 2026/2693(RSP) / B10-0206/2026 / P10_TA(2026)0163
- 3. Date of adoption of the resolution:** 30 April 2026
- 4. Competent Parliamentary Committee:** n/a
- 5. Brief analysis/ assessment of the resolution and requests made in it:**

This resolution reflects the growing concern across the European Union regarding the impact of cyberbullying and online harassment on minors, women and groups in situations of vulnerability, and highlights the need for coordinated action at EU level. The resolution acknowledges the action plan against cyberbullying and supports its focus on prevention, digital literacy, victim protection and improved enforcement of existing EU legislation, notably the Digital Services Act (DSA).

At the same time, the European Parliament:

- calls for further reflection on whether the current legal framework is sufficient to address the increasing scale, severity and cross-border dimension of cyberbullying and image- or video-based abuse.
- invites the Commission to assess the need for a more harmonised approach at EU level to define cyberbullying and to examine whether certain severe forms of cyberbullying, including the non-consensual dissemination of intimate material, could require action under Union criminal law.
- calls for strengthened enforcement of the DSA, in particular Art.28, concerning the protection of minors online, and for online platforms to be held accountable for systemic risks linked to cyberbullying, harmful recommender systems and illegal content.
- highlights emerging challenges linked to artificial intelligence (AI), including deepfakes and AI-generated abusive content, and calls for banning “nudifier applications” under the AI Act.
- urges providers to apply transparency and watermarking rules so AI-generated content is clearly labelled, particularly to protect minors from deepfakes.

- calls on the Member States to establish comprehensive national anti-cyberbullying plans, to provide for effective, proportionate and dissuasive penalties for cyberbullying offences, to share best practices on their legal approaches; and to prioritise prevention, education, digital literacy, and awareness-raising measures targeting children, parents and educators, as well as restorative approaches.

6. Response to the requests in the resolution and overview of the action taken, or intended to be taken, by the Commission:

Commission action plan against cyberbullying (paragraphs 3, 4)

The Commission shares the European Parliament's objective of ensuring a high level of protection against cyberbullying across the Union. The Commission will continue to support initiatives and exchanges of best practices among Member States on cyberbullying, online harassment and protection of minors online, including national legislative and policy approaches. These efforts aim to strengthen cooperation between national authorities, Safer Internet Centres, civil society organisations and online platforms to facilitate reporting, strengthen victim assistance and improve coordination in cross-border cases.

As regards reporting mechanisms and support to children and young persons experiencing cyberbullying, the Commission will support the rollout of a European online safety app, based on successful national models. This app is intended to provide a secure, user-friendly and confidential tool enabling children and young persons to report cyberbullying, and access support services. Its effectiveness, however, depends on its integration into a broader ecosystem, with reporting linked to coordinated follow-up, including legal, psychological, social and educational assistance, and where appropriate, law enforcement to ensure timely and comprehensive support.

In this context, Member States play a key role in developing comprehensive national approaches to preventing and addressing cyberbullying, combining prevention, awareness-raising, victim support, digital literacy and effective enforcement measures. In doing so, Member States can benefit from the support of the EU network on children's rights in line with the [Commission communication and recommendation on integrated child protection systems](#).

Criminal law (paragraph 5, 6, 7, 8, 9, 10)

The Commission shares the European Parliament's concern regarding the increase in cyberbullying, online harassment and image- or video-based abuse.

As regards criminal law measures at Union level, the Commission notes that Article 83(1) TFEU allows for the establishment of minimum rules in certain areas of particularly serious crimes with a cross-border dimension. In this context, the notion of “cyberbullying” covers a broad spectrum of behaviours of varying gravity and nature, including conduct that may already fall within existing criminal offences under Union or national law.

To ensure a coherent criminal law response to hate offences, and strengthen victim protection across the EU, the Commission proposed to the Council in December 2021 to extend the list of EU crimes under Article 83(1) TFEU to include hate offences. This would enable the adoption of harmonised EU criminal law measures, including on grounds that are not covered by the 2008 Framework Decision. However, the required unanimity in the Council has not yet been reached.

For such reasons, the Commission welcomes the reiteration of the support of the European Parliament for adding hate offences, which could cover the most severe forms of cyberbullying, to the list of EU crimes under Article 83(1) TFEU. While continuing to observe developments in the Council, the Commission is considering an alternative legal basis to tackle online hate offences, within the limits of EU competences under existing Treaty provisions.

At the same time, the existing Union acquis already provides for important safeguards and criminal law measures relevant to harmful online conduct. The Directive on combating violence against women and domestic violence defines, at EU level, the crime of cyber harassment, cyber stalking, non-consensual sharing of intimate or manipulated material (deepfake), online incitement to violence and hatred on grounds of gender and establishes the minimum of the maximum penalty for each of these crimes. It also requires Member States to ensure that illegal online content is promptly removed or that access to it is disabled.

The Framework Decision on combating racism and xenophobia by means of criminal law requires Member States to criminalise the public incitement to violence or hatred based on race, colour, religion, descent or national or ethnic origin. It requires to take into account the racist and xenophobic motivation for all criminal offences. It applies offline and online and while its scope is limited to racism and xenophobia, many Member States in principle have extended protection to other characteristics in their national provisions such as political opinions, sexual orientation or disability.

Where cyberbullying constitutes a criminal offence under national law, the provisions in Directive 2012/29/EU establishing minimum standards for the rights, support and protection of victims of crime apply to victims of such offences. Following the recent adoption on 8 June 2026 of the revised Victims’ Rights Directive, the Commission will assist Member States in ensuring its correct and complete

transposition, so that victims of online and offline offences receive appropriate protection, support and access to justice across the Union.

Finally, the Directive 2016/800 on procedural safeguards for children who are suspects or accused persons in criminal proceedings provides a comprehensive framework for a child-friendly justice response, considering the individual circumstances of the child and emphasises reintegration and rehabilitation. This is particularly relevant given that some children who engage in cyberbullying may themselves be or have previously been victims.

Other relevant instruments include the 2011/93/EU Directive on combating the sexual abuse and sexual exploitation of children and child sexual abuse material, the Audiovisual Media Services Directive, the Digital Services Act and the Artificial Intelligence Act. These instruments are complemented by broader policy initiatives, including the European strategy for a better internet for kids (BIK+), the action plan against cyberbullying, and the Commission guidelines on measures to ensure a high level of privacy, safety and security for minors under Article 28(4) of the Digital Services Act.

Online platforms and the DSA (paragraphs 11, 14, 15, 16)

The Commission agrees that online platforms must comply with their obligations under Union law, in particular the DSA, to ensure a safe, predictable and trustworthy online environment for all users, including minors, in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected. In this regard, the Digital Services Act requires providers of online platforms accessible to minors to put in place appropriate and proportionate measures to ensure a high level of privacy, safety and security for minors on their services. The Guidelines adopted under Article 28(4) DSA provide a non-exhaustive list of measures that the Commission considers providers of online platforms should put in place to comply with that obligation. The DSA also establishes a comprehensive framework of obligations applicable to providers of very large online platforms (VLOPs) and of very large online search engines (VLOSEs), including the obligations to diligently identify, assess and analyse the systemic risks stemming from their services and to put in place reasonable, effective and proportionate measures to mitigate the identified risks. Those systemic risks include any actual or foreseeable negative effects on the exercise of fundamental rights, such as to respect for the rights of the child and to a high-level of consumer protection, and serious negative consequences for a person's physical and mental well-being. The DSA also lays down additional online advertising transparency and data access obligations applicable to providers of VLOPs and VLOSEs.

The Commission is enforcing these rules with speed and rigour. Recent actions include the adoption of preliminary findings against

the provider of Facebook and Instagram for failing to effectively prevent children under 13 from accessing their services, and against providers of VLOPs disseminating pornographic content (namely, Pornhub, XNXX, Stripchat, and XVideos) for failing to implement robust age verification measures, despite their minimum age rules. The Commission has also initiated proceedings against the providers of X, Shein, and Snapchat over risks including AI-generated child sexual abuse material, child-like sex dolls, grooming, and drug sales to minors. In addition, in the preliminary findings against the provider of TikTok, the Commission took the preliminary view that that provider had not adequately assessed how addictive features could affect the physical and mental well-being of its recipients, including minors and not effectively mitigated against this systemic risk.

As regards trusted flaggers, the Commission will continue to support the practical implementation of the DSA, including by issuing guidelines on the trusted flagger mechanism. These will facilitate cooperation among relevant stakeholders, including online platforms and trusted flaggers, concerning the identification and reporting of illegal content, such as cyberbullying and online harassment when illegal. The Commission will also strengthen the capacity of trusted flaggers on gender-based cyber violence to ensure that more such content is flagged to online platform providers.

The Commission will also continue to combat discrimination and foster safer and more inclusive digital spaces through its Union of Equality strategies, including the recently adopted LGBTIQ+, anti-racism and gender equality strategies 2026-2030, as well as the communication on reinforcing the strategy for the rights of persons with disabilities up to 2030. In particular, the Gender Equality Strategy 2026-2030 puts a clear focus on combating gender-based cyber violence and presents several actions in this regard. In this context, the Commission will pursue a structured regulatory dialogue with providers of VLOPs and VLOSEs to strengthen compliance with the Digital Services Act and, in cooperation with national authorities, will use all available tools to ensure effective mitigation of systemic risks in relation to gender-based violence, including where necessary, through targeted guidance.

As regards child sexual abuse material online, the Commission remains committed to strengthening the protection of children online in full respect of all fundamental rights, including children's rights, the rights to privacy and the protection of personal data. The Commission shares the European Parliament's concerns regarding the current lack of a legal framework for the detection of child sexual abuse material online. The Commission had proposed in December 2025 a limited extension of Regulation 2021/1232/EU on a temporary derogation from certain provisions of Directive 2002/58/EC ("the Interim Regulation"); the Interim Regulation lapsed on 3 April 2026. The Council adopted its position in first reading on 2 July 2026. The Commission accepted the position taken by the Council (see Communication pursuant to Article 294(6) of the Treaty on the Function of the European Union on 3 July 2026 ([COM\(2026\)357](#)). The

Parliament voted its amendments to the Council position on 9 July 2026. On 15 July, the Commission, following Article 294(7), point (c), of the Treaty on the Functioning of the European Union, delivered an opinion on the amendments proposed by the European Parliament in second reading ([COM\(2026\)393](#)).

After receiving the Parliament's amendments, the Council has three months to approve or reject the amendments. If the Council does not accept all of the amendments, the co-legislators would move to conciliation to agree on the law.

The process further prolongs the legal uncertainty for the detection of online child sexual abuse pending agreement on the long-term framework.

The Commission recalls that the extension proposal aimed to preserve the existing level of protection and encourages the co-legislators to reach an agreement as soon as possible on the Interim Regulation

In parallel, the Commission continues to support ongoing negotiations by the co-legislators on the proposed [Combating child sexual abuse Regulation](#), which seeks to establish a robust and legally sound long-term regulatory framework to effectively prevent and combat child sexual abuse online, in full respect of all fundamental rights.

The proposal includes measures on prevention, detection, reporting, removal and blocking of child sexual abuse online, as well as the creation of an EU Centre to prevent and combat child sexual abuse, to support implementation and cooperation between all relevant actors and to provide assistance to victims.

Other measures

The Commission shares the European Parliament's concerns regarding the misuse of artificial intelligence (AI) technologies for abusive purposes, including the creation of deepfakes, voice cloning and non-consensual intimate content or child sexual abuse material.

The Artificial Intelligence Act establishes a harmonised framework for trustworthy AI in the Union. It prohibits certain particularly harmful practices including AI systems that exploit children's vulnerabilities or deploy subliminal, manipulative or deceptive techniques that manipulate children or other users and lead to significant harms (e.g. AI systems inciting violence, self-harm, stalking etc.). As regards particularly harmful deepfakes, following the Omnibus on AI, the co-legislators agreed to introduce a new prohibition of AI systems that generate or manipulate non-consensual intimate content. the new prohibition will prohibit "the placing on the market, the putting into service or the use of an AI system that generates or manipulates realistic images, videos, audio or similar material of an identifiable natural person's intimate parts, or of an identifiable natural person engaged in sexually explicit activities, without that person's freely-given, specific, informed, unambiguous and explicit consent for that

generation or manipulation". This prohibition will apply as of December 2026.

In addition, Article 50 establishes transparency obligations for certain AI-generated or manipulated content, requiring that individuals are informed when they are interacting with AI systems, that AI generated or manipulated content is marked to enable its detection in a reliable and effective manner and that deep fakes and certain AI generated text publications are clearly labelled. The Commission is facilitating compliance with above noted transparency obligations through, among others, the development of the Code of Practice on marking and labelling of AI-generated content and Guidelines on Article 50 of the AI Act.

As regards online gaming environments, the Commission acknowledges that online gaming services falling within the scope of the DSA may expose users, including minors, to risks linked to cyberbullying, harassment and harmful conduct. In this context, the Commission recalls that it has adopted Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of the DSA.

The President of the Commission has also set up a Special Panel on Child Safety Online of experts to assess the impact of social media and other digital tools on children. The panel brings together young people and experts from across the EU, including in health, neuroscience, psychology, computer science, child rights, and digital literacy. Based on inputs from the meetings of the panel, the co-chairs delivered a report on the outcomes of the panel, including advice on the best approach for Europe and recommendations for future actions.

Harmful content under the AVMSD (paragraph 19)

As regards the Audiovisual Media Services Directive ('AVMSD'), the Commission recalls that the Directive requires Member States to ensure that appropriate measures are put in place to protect minors from harmful content and all users from content inciting violence or hatred. Concretely, video-sharing platforms, irrespective of their size, are required to take appropriate measures such as reflecting EU media content standards in their terms and conditions, applying mechanisms to report and flag harmful content, age verification systems, parental controls and content rating systems. While continuing to monitor the implementation and application of the Directive at national level, the Commission will further consider cyberbullying during the ongoing evaluation of the Directive and its upcoming review in Q3-Q4 2026 in relation to its rules on the protection of minors online from harmful content.

The Commission will continue to assess the application of existing Union rules to such services and to examine whether existing

measures and safety obligations adequately address the specific risks affecting minors in online gaming environments.

To conclude, in line with the action plan against cyberbullying and the BIK+ Strategy, the Commission will continue to promote awareness-raising activities, digital literacy initiatives and child-centred approaches involving educators, parents, civil society organisations and Safer Internet Centres, while supporting Member States' mutual learning activities and comprehensive anti-bullying plans, including on cyberbullying, centred on children's rights and informed by their views, as reflected in the contributions of 6,343 children through the EU Children's Participation Platform, a key deliverable of the EU Strategy on the rights of the child.