ASSEDEL

Association Européenne
pour la Défense des Droits et des Libertés

ASSEDEL, 11 Rue de Bruxelles
67000 Strasbourg, France, www.assedel.org
info@assedel.org

Regulation to Prevent and Combat Child Sexual Abuse (CSAR)

POLICY ANALYSIS

ASSEDEL (European Association for the Defense of Rights and Freedoms) is a non-profit association, governed by its statutes, in accordance with articles 21 to 79-III of the local civil code of Alsace Moselle relating to associations. Its purpose is to disseminate, promote and defend human rights and fundamental freedoms in the spirit of the European Convention on Human Rights, both within the Council of Europe and the European Parliament and at local level, national and international. In addition, the organization guides and supports victims of human rights violations.

JANVIER 2026

Balancing Child Protection and Privacy: A Critical Evaluation of the EU's Regulation to Prevent and Combat Child Sexual Abuse

The proposed EU Regulation to Prevent and Combat Child Sexual Abuse (CSAR), introduced in May 2022 in response to online child sexual exploitation, aims to harmonize measures against the dissemination of child sexual abuse material (CSAM) and online grooming by imposing risk assessments, mitigation duties, and reporting obligations on online service providers, including encrypted messaging services. While the original proposal included mandatory scanning of private communications, this approach met strong resistance over privacy and fundamental rights concerns, leading to its eventual removal in the Council's November 2025 draft. The current draft maintains provisions on risk mitigation, potential scanning of communications, and identity and age verification, alongside permanent derogations from ePrivacy rules. Critics argue that this framework may still result in de facto compulsory scanning, weaken encryption, enable large-scale monitoring, and that false positives may disproportionately affect vulnerable groups; the scale and severity of these risks, however, depend largely on the detection mechanism employed. As trilogue negotiations continue into 2026, the proposal remains controversial, reflecting ongoing tensions between the EU's objective of protecting children and the need to safeguard privacy, data protection, and fundamental rights.

I. Introduction

The European Union's proposed Regulation laying down rules to prevent and combat child sexual abuse, commonly known as the Child Sexual Abuse Regulation (CSAR)[1] or "Chat Control" represents a legislative attempt to address the escalating crisis of online child exploitation.[2] Formally introduced by the European Commission on 11 May 2022, the proposal builds on the 2020 EU Strategy for a More Effective Fight Against Child Sexual Abuse, which identified the urgent need for harmonized measures to counter the proliferation of child sexual abuse material (CSAM) and grooming via digital platforms.[3] As outlined in the Commission's explanatory memorandum, the Regulation's primary objective is to impose risk assessments, detection obligations and reporting requirements on online service providers, including hosting platforms and end-to-end encrypted messaging apps like WhatsApp and Signal.[4]

End-to-end encryption is a privacy measure that ensures images, videos, messages, and live communications can be seen only by the people sending and receiving them.[5] However, because end-to-end encryption blocks service providers from accessing this content, it also prevents them from identifying child sexual abuse material or responding to lawful requests from law enforcement aimed at investigating crimes, apprehending offenders, and protecting children.[6] Hence, this technology creates a paradox: while it ensures and strengthens personal privacy and increases trust in digital services, it simultaneously complicates the work of law enforcement by providing potential safe spaces for illegal online activities.[7] These platforms will be obliged to detect, report and remove CSAM. At the same time the intention is to establish an EU Centre to coordinate cross-border efforts and support victims. This framework extends the interim measures of Regulation (EU) 2021/1232, which temporarily derogates from ePrivacy rules to enable voluntary scanning until 2026. The aim is a permanent, market-wide harmonization that complements the Digital Services Act and Directive 2011/93/EU on combating child sexual abuse.

---

[1] Regulation (EU) 2024/1692 of the European Parliament and of the Council of 11 June 2024 laying down rules to prevent and combat child sexual abuse (Child Sexual Abuse Regulation) [2024] OJ L 1692.

[2] Council of Europe, Outcome Report of the Expert Workshop on the EU Proposed Regulation on Preventing and Combating Child Sexual Abuse (2023) accessed 11 December 2025.

[3] European Commission, Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast) COM(2024) 60 final (6 February 2024) accessed 11 December 2025.

[4] Deepak Gupta, *EU's Chat Control Proposal: Balancing Child Protection and Digital Rights* (guptadeepak.com, 28 April 2025) https://guptadeepak.com/eus-chat-control-proposal-balancing-child-protection-and-digital-rights/ accessed 1 December 2025.

[5] Home Office, End-to-End Encryption and Child Safety (20 September 2023) accessed 11 December 2025.

[6] Laura Draper, Protecting Children in the Age of End-to-End Encryption (Joint PIJIP/TLS Research Paper Series, 2022) accessed 11 December 2025.

[7] INTERPOL, 'Interpol General Assembly Resolution Calls for Increased Safeguards Against Online Child Sexual Exploitation' (24 November 2021) https://www.interpol.int/News-and-Events/News/2021/INTERPOL-General-Assembly-resolution-calls-for-increased-safeguards-against-online-child-sexual-exploitation accessed 3 December 2025.

Additionally, the proposal seeks to disrupt the usage of networks for malicious purposes at their digital source without further burdening low-risk services by limiting mandatory detection orders to high-risk providers (especially those offering end-to-end encrypted communications) and establishing a procedure for low-risk services to be formally exempted from such obligations.[8]

II. Background of the Proposal

The proposal for a Regulation laying down rules to prevent and combat child sexual abuse was presented by the European Commission on 11 May 2022 as a direct response to the dramatic increase in online child sexual exploitation.[9] Child sexual abuse online has exploded. Europol received 725 000 reports of child sexual abuse material (CSAM) in 2019. One year later, in 2020, the number was already over 1 million. Around 85 % of that material was stored on servers inside the European Union.[10] As a result of this sharp rise, the Union felt the pressure of acting in this regard. In 2021, it passed a temporary law (Regulation 2021/1232)[11] that allowed companies to voluntarily scan for known child abuse images without breaching normal privacy rules. The permission was only valid for a few years.

When the temporary law was about to expire, the European Commission determined that a more permanent solution was necessary.

On 11 May 2022, it published a very strong proposal. The original 2022[12] text had four main elements:

1. Every platform (such as messaging apps and app stores) must check every year how risky its service is.
2. If the risk is high, a court or authority can order the company to scan all messages and this would apply even apps using end-to-end encryption services such as WhatsApp or Signal. The scan would happen on the user's phone (client-side scanning) before the message is encrypted.
3. A new EU Centre in The Hague would keep lists of known abuse images, build new scanning tools, check reports and help victims across borders.
4. Extra child-protection rules: age checks, limits on apps for minors and strict default privacy settings.

---

[8] Teresa Quintel, *The Commission Proposal on Combatting Child Sexual Abuse: Confidentiality of Communications at Risk?* (2022) 8 *European Data Protection Law Review* 262

[9] European Commission, Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast) COM(2024) 60 final (6 February 2024) accessed 11 December 2025.

[10] Council of Europe, Outcome Report of the Expert Workshop on the EU Proposed Regulation on Preventing and Combating Child Sexual Abuse (2023) accessed 11 December 2025.

[11] Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse [2021] OJ L 273/65.

[12] 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, 52022PC0209 (European Commission, 11 May 2022) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209 accessed 1 December 2025.

These orders would need a judge's approval and could last up to two years.[13] However, the basic idea was clear: there would be compulsory scanning of private messages whenever a "significant risk" existed.[14] The proposal met huge resistance. People feared it would breach encryption and turn every phone into a surveillance device.[15] The text changed a lot over three years. To start with, in November 2023 The European Parliament voted for strong protection for end-to-end encryption and said scanning should only be a last resort. In 2024 and early 2025 In the Council of the European Union, Germany, the Netherlands, Austria, Poland and others blocked every version that included mandatory scanning. During the summer and autumn of 2025, the Danish presidency made one final attempt. Early drafts still contained some mandatory rules, but support collapsed.

On November 26th 2025 The Council finally agreed on a completely new text (document 15318/25).[16] The biggest change: all mandatory scanning orders were deleted.

III. What the law looks like today (December 2025 version)

Companies can keep scanning voluntarily and this permission is now permanent (the old temporary law is made endless).[17] The EU Centre to prevent and counter child sexual abuse will be created and will store lists of abuse images, help companies with tools, give money for scanning technology and coordinate removals.[18] Further, a three-level risk system is introduced: low-risk, medium-risk and high-risk. As for the high-risk services, they must take "mitigation measures".[19] Scanning is not forced however it is listed as one possible measure. Companies that scan "voluntarily" get legal protection, funding and a better risk score. Many experts and privacy groups say this is still "mandatory scanning through the back door". Companies will feel strong pressure to scan because:

- they want to be labelled "low risk",
- they receive money and legal safety if they scan,
- they fear huge fines or bad publicity if abuse happens on their platform.

---

[13] Laura Draper, Protecting Children in the Age of End-to-End Encryption (Joint PIJIP/TLS Research Paper Series, 2022) accessed 11 December 2025.

[14] Laura Draper, Protecting Children in the Age of End-to-End Encryption (Joint PIJIP/TLS Research Paper Series, 2022) accessed 11 December 2025.

[15] Laura Draper, Protecting Children in the Age of End-to-End Encryption (Joint PIJIP/TLS Research Paper Series, 2022) accessed 11 December 2025.

[16] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – Partial mandate for negotiations with the European Parliament* (Doc 15318/25, 13 November 2025) https://data.consilium.europa.eu/doc/document/ST-15318-2025-INIT/en/pdf accessed 1 December 2025.

[17] European Parliament, Legislative Train Schedule, 'EU Strategy for a More Effective Fight against Child Sexual Abuse' accessed 11 December 2025.

[18] Anna Pingen, 'Controversial Proposal on Combating Child Sexual Abuse Online' (eucrim, 12 May 2022) accessed 11 December 2025.

[19] 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, 52022PC0209 (European Commission, 11 May 2022) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0209 accessed 1 December 2025.

This new law works alongside the Digital Services Act[20]. It also introduces a permanent exception to the ePrivacy Directive[21], the rule that normally protects the confidentiality of messages. This is despite the Commission's earlier promise that any such exceptions would be only temporary.

Other countries are watching the EU's approach closely. The United Kingdom abandoned similar scanning proposals after public protests, while the United States operates under comparatively weaker privacy protections. At the same time, governments with fewer democratic safeguards are already pointing to the EU, arguing, "Even Europe is scanning private messages."

Right now (December 2025), the Council, the European Parliament and the Commission are holding closed "trilogue" talks.[22] The goal is to reach a final agreement by spring 2026 to prevent any gap when the current temporary law expires in April 2026.[23]

In short, the original plan for forced scanning of everyone's private messages has been removed. However, a permanent, strongly incentivized "voluntary" system has taken its place and many people still worry that the result will be the same in practice. The final text is not yet decided and the fight over privacy and child protection continues.

IV. What Remains to correct in the Draft law

Even after the changes, some parts of the new Council draft from November 2025 are still controversial. They could clash with EU privacy laws and may violate fundamental rights as well.[24] Among others, the relevant issues that might arise are the following: (i) the risk mitigation under article 4, (ii) the potential scanning of the encrypted communication, (iii) identity and age verification, (iv) voluntary detection.

To start with, (i) under article 4 of the Council draft we find the concept of "Risk-Mitigation".[25] Providers of email, messaging and cloud services must do regular risk assessments. They need to check whether their service could be used for child sexual abuse material (CSAM) or grooming. Then, they must take "all appropriate risk mitigation measures." The current text no longer provides for immediate mandatory scanning. However, it continues to authorize providers to engage in voluntary detection, including the scanning of communications.

---

[20] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022] OJ L 277/1.

[21] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive) [2002] OJ L 201/37.

[22] European Parliament, Legislative Train Schedule, 'Prevention and Fight against Child Sexual Abuse' (Carriages preview) accessed 11 December 2025.

[23] European Day for the Protection of Children against Sexual Exploitation and Sexual Abuse | Epthinktank | European Parliament

[24] Deepak Gupta, 'EU's Chat Control Proposal: Balancing Child Protection and Digital Rights' (Security Boulevard, 28 April 2025) <https://securityboulevard.com/2025/04/eus-chat-control-proposal-balancing-child-protection-and-digital-rights/> accessed 11 December 2025.

[25] Ibid.

Critics argue that this system creates indirect pressure on providers to engage in scanning.[26] If a platform chooses not to scan, it risks being classified as a 'high-risk' service under the Regulation. That classification may lead to increased regulatory oversight, financial penalties, and reputational consequences.[27] As a result, although scanning is formally described as 'voluntary', it becomes, in practice, very difficult for platforms to refuse. Therefore, there are different legal issues arising from this wide "risk mitigation" as its lack of clear limits makes compliance with the principles of necessity and proportionality difficult to assess. In addition, it may conflict with Articles 7 and 8 of the EU Charter on privacy and data protection. Moreover, the growing normalization of 'voluntary' scanning under regulatory pressure risks undermining trust in the confidentiality of communications. The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) have warned that this framework could lead to large-scale monitoring without sufficient legal justification.

As for the (ii) potential scanning of encrypted communications, although mandatory scanning orders have been removed, the law still permits the scanning of private messages, including those protected by end-to-end encryption.[28] The risk-based system strongly incentivizes companies to carry out such scanning. The measures proposed to tackle the issue of child sexual abuse, create complex grey areas between public safety and fundamental rights. While the EU justifies increasingly powerful content monitoring capabilities in the name of protecting children, at the same time, these measures risk enabling mass surveillance by weakening encryption and place ordinary users under heightened scrutiny.

Moreover, large-scale scanning systems must search immense data sets for rare harms, meaning that even with relatively accurate detection methods, innocent people are far more likely to be flagged than actual offenders. This introduces the issue of false positives, which may disproportionately impact already vulnerable groups, who often share risk markers, such as living in disadvantaged neighborhoods, that automated systems may mistakenly interpret as indicators of criminal behavior.[29] Likewise, predictive policing systems often single out minority communities at higher rates, prompting worries about technological tools reinforcing systemic racism.[30] Misclassifications deepen feelings of exclusion and reinforce existing social inequalities. Furthermore, being subjected to digital suspicion may lead to greater social marginalization, in particular for communities that already face systemic disadvantages and discrimination. In the long term, this can undermine public trust in both technology providers and state institutions as well as confidence in democratic values.

However, the likelihood of false positives also varies significantly depending on the detection mechanisms employed. Automated scanning tools, while efficient at scale, are more prone to errors and may reflect underlying biases within their design.

---

[26] Deepak Gupta, 'EU's Chat Control Proposal: Balancing Child Protection and Digital Rights' (Security Boulevard, 28 April 2025) <https://securityboulevard.com/2025/04/eus-chat-control-proposal-balancing-child-protection-and-digital-rights/> accessed 11 December 2025.

[27] Ibid.

[28] European Digital Rights (EDRi), *EU Chat Control Regulation* (EDRi) https://eu.ci/eu-chat-control-regulation/ accessed 1 December 2025.

[29] Diderichsen A (ed), Policing False Positives: Lessons from Epidemiology < https://nsfk.org/wp-content/uploads/2025/04/e2725-nsfk-research-seminar-report-2018.pdf#page=123 >

[30] Hakeemat I, 'Balancing Data Privacy and Technology Advancements: Navigating Ethical Challenges and Shaping Policy Solutions' (2024) 5(12) *International Journal of Research Publication and Reviews* 8118 https://doi.org/10.55248/gengpi.5.1224.3549 accessed 3 December 2025.

By contrast, systems that incorporate human review tend to offer greater accuracy and reduce the risk of misclassifications.[31] Therefore, the mechanisms employed are crucial in determining both the accuracy of detection and the potential for harm caused by false positives. Yet, critics state that the approaches proposed to combat online child sexual abuse all risk vulnerability that can be exploited by hackers and hostile nation states, which further undermines the security of digital communications and exposes both individuals and critical systems to potential harm.[32]

Building on these broader concerns about security and human-rights risks, the draft's proposed measures on identity and age verification further concentrate sensitive personal data. To prevent minors from accessing or misusing online platforms, the draft reintroduces mandatory age verification. While intended to protect children, this could effectively end anonymous or pseudonymous use online. This not only allows unauthorized access by third parties and foreign hostile governments to access personal data, but this power can also be misused by the government itself. Moreover, even governments operating under strong rule-of-law frameworks create risks of data leaks to other parties simply by accessing personal information.[33] Critics warn that such measures may harm vulnerable users, including journalists or abuse survivors, who rely on safe, confidential spaces.[35] Freedom House notes that government monitoring of social media worldwide has already produced a chilling effect on human rights. Without end-to-end encryption, minorities and other vulnerable groups living under authoritarian regimes could face severe threats, including human rights abuses and persecution.[34]

The legal implications are significant. Combined with content scanning, age checks (iii) pose serious threats to anonymity and privacy, both essential for freedom of expression and the protection of personal safety. Biometric or ID-based verification may also conflict with the GDPR's data minimization principle, which prohibits collecting, using, or retaining more personal data than necessary to achieve a lawful purpose. Because the draft law would apply to all users, rather than only suspected offenders, it risks creating a system of indiscriminate data collection.

Finally, the draft wants to make the current (iv) voluntary CSAM scanning rules permanent, even though they were originally intended to be temporary. This could lead to an

---

[31] Schwemer, S.F. Decision Quality and Errors in Content Moderation. IIC 55, 139–156 (2024). https://doi.org/10.1007/s40319-023-01418-4

[32] Bagwe M, 'EU Chat Control Proposal to Prevent Child Sexual Abuse Slammed by Critics' (18 June 2024) *The Cyber Express* https://thecyberexpress.com/eu-chat-control-proposal-slammed/ accessed 3 December 2025.

[33] UNICEF, *Encryption, Privacy and the Right to Protection from Harm* (2020) https://www.unicef.org/innocenti/media/3446/file/UNICEF-Encryption-Privacy-Right-Protection-From-Harm-2020.pdf accessed 3 December 2025.

[34] Freedom House, *Freedom on the Net 2019: The Crisis of Social Media* (2019) https://freedomonthenet.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf accessed 3 December 2025.

[35] Patrick Breyer, *EU Chat Control Proposal Still Poses High Risks Despite Removal of Mandatory Scanning, Experts Warn* (patrick-breyer.de) https://www.patrick-breyer.de/en/eu-chat-control-proposal-still-poses-high-risks-despite-removal-of-mandatory-scanning-experts-warn/ accessed 1 December 2025.

expansion of scanning over time. However, the notion of "voluntary" is ambiguous. It overlaps with the law's risk-mitigation requirements, meaning that in practice it could function similarly to mandatory scanning.

V. Conclusion and Recommendations

The 2025 Council position on the Regulation to Prevent and Combat Child Sexual Abuse (CSAR) reveals a European Union that is united in its desire to protect children, but still profoundly divided on how to achieve this without eroding fundamental rights. This regulation represents a significant and ambitious attempt to combat the alarming rise of online child sexual abuse. Over time, the proposal has evolved from mandatory scanning of private communications to a risk-based, incentivized "voluntary" system. While this shift addresses some privacy concerns, "voluntary" scanning remains poorly defined, and the current draft continues to raise substantial legal, ethical, and technical challenges.

Relevant concerns include:

1. Indirect pressure on service providers: Although scanning is formally voluntary, the risk-based classification system, legal protections, and reputational incentives may effectively compel platforms to scan communications, potentially undermining the principle of voluntary participation.

2. Privacy and encryption risks: The regulation maintains the possibility of scanning end-to-end encrypted messages, which weakens encryption, and may expose users to surveillance, increasing security vulnerabilities.

3. Human rights and fundamental freedoms: Measures such as identity and age verification, along with potential large-scale scanning, could conflict with EU privacy laws, the GDPR, and Articles 7 and 8 of the EU Charter. These measures may disproportionately affect vulnerable groups, including minors and journalists, eroding trust in digital services and state institutions.

4. Risk of false positives and social bias: Automated detection systems are prone to misclassification, which could unjustly target certain communities, exacerbate inequalities, and undermine public confidence in both technology and democratic governance.

5. Permanent expansion of surveillance measures: Making temporary CSAM scanning rules permanent risks normalizing mass monitoring, with potential misuse of data by states or malicious actors.

In sum, while the regulation's objectives, child protection, cross-border coordination, and stronger risk mitigation, are laudable, the current draft introduces significant ambiguities and unintended consequences that could compromise privacy, security, and fundamental rights.

Recommendations

1. Clarify the limits of "voluntary" scanning: Explicitly define voluntary measures and ensure that risk-based incentives do not effectively mandate scanning. Clear legal safeguards are needed to prevent coercion of service providers.

2. Protect end-to-end encryption: Avoid weakening encryption standards, and consider technical solutions that allow child protection without compromising the confidentiality of all communications.

3. Introduce strong oversight and accountability: Independent monitoring, judicial review, and transparent reporting mechanisms should accompany any scanning or risk mitigation activities to ensure proportionality and compliance with fundamental rights.

4. Minimize data collection: Age verification, identity checks, and scanning should adhere strictly to the GDPR's data minimization principles. Personal data should only be processed when strictly necessary and with robust safeguards.

5. Mitigate false positives: Develop hybrid detection systems combining automated tools with human review to reduce errors and bias. Regular audits of detection mechanisms should be required.

6. Engage stakeholders and the public: Maintain transparency and actively involve privacy advocates, civil society, technical experts, and survivor organizations in the design and implementation of the regulation. Complement technological measures with effective, rights-preserving solutions, such as improved takedown procedures, increased resources for specialized law enforcement units, stronger cooperation with survivor organizations, and enhanced prevention and education strategies, to ensure public trust and minimize unintended harms.