

Jana Stehlíková\* - 7 May 2026

## The Termination of ‘Chat Control 1.0’:

### Just an Intermezzo or a Real Turning Point in the Big Tech Battle and Online Surveillance in the EU?

#### Digital privacy has scored 1.0 to zero at EU level

On Thursday, 26 March 2026, millions of people were scrolling through social media as usual, commenting on content, sending messages or emails to each other, and engaging with their contacts or followers. They were probably unaware that a voting session was taking place simultaneously in the European Parliament (EP), to decide on a controversial proposal that would have had a crucial impact on the privacy of their conversations from 4 April 2026 onwards. The vote concerned was on the future of the Interim Regulation (EU) 2021/1232 (also known as ‘Chat Control 1.0’), which allows online platform providers to voluntarily scan non-encrypted private communications for child sexual abuse material (CSAM). The questions were: Would it be extended again despite conflicting with the ‘ePrivacy Directive’ (officially Directive 2002/58/EC), or would it expire by midnight on 3 April? And what about the original proposal to make it permanent legislation, referred to as ‘Chat Control 2.0’, which would give big tech companies such as Meta and Microsoft an unprecedented green light to monitor private conversations?

In the final vote, Members of the European Parliament (MEPs) rejected the extension of the provisional act. This therefore expired on 3 April without being replaced. You may now be wondering what this means. Should we celebrate the victory of privacy protection and the end of surveillance? After all, this decision confirms the EU’s commitment to safeguarding private spaces and digital rights. Or have we witnessed the creation of a regulatory gap that could undermine efforts to detect and prevent CSAM on online platforms?

The negotiations and the European Parliament’s final vote invite further analysis, particularly in the con-

text of the Council of the EU’s anticipated position, at a time when several EU member states are introducing stricter social media regulation and age-based access restrictions. These recent developments highlight the continued relevance of the ‘Nothing to Hide’ narrative in shaping attitudes towards digital surveillance. However, they also raise concerns that such measures could have significant implications for privacy and fundamental rights by opening a regulatory ‘Pandora’s box’.

#### The well-known EU dilemma of security versus privacy

To answer the raised questions, we must take a step back and analyse the Interim Regulation, considering the benefits it brought during its five years in force, as well as the price paid for them, particularly within the broader EU privacy regulatory context. The security versus privacy dilemma is nothing new– it has been under discussion many times and, in many contexts,<sup>2</sup> including with regard to digital privacy and cybersecurity.

Let’s focus on our particular case. In December 2025, the EC had to raise the issue of how to further proceed with ‘Chat Control 1.0’ with the Council of the EU and the European Parliament. This regulation allowed providers of certain communication services, such as social media platforms, to scan and analyse content for the purpose of detecting online CSAM, and removing such material immediately. The Regulation’s objective is laudable, and the benefits were clearly outlined by Swedish Home Affairs Commissioner Ylva Johansson when she introduced the proposal in 2021.

\* **Jana Stehlíková** works as a Director of International Study Programmes at the European Academy Otzenhausen, an independent educational institution in Germany. She obtained a PhD in International Political Relations from the University of Economics in Prague, writing her dissertation on ‘The European Union as a Normative Power: The Extraterritorial Reach of the EU’s Personal Data Protection Standards’, examining the ‘Brussels effect’ and formal and behavioural compliance with EU standards in Norway, Serbia, and Ukraine. Her research focuses mainly on questions related to the recent development of European integration and digital affairs.

At the time, the regulation proposal received the necessary backing from both the Council of the EU and the European Parliament as an interim measure in response to the heightened risk of online sexual abuse during the Covid-19 pandemic, when much of the world's activity moved online. The legislation also aimed to encourage providers - primarily overseas tech giants such as Meta and Google - to cooperate with the authorities and play an active role in safeguarding vulnerable members of society. At least, that was what the EC, represented by Ms Johansson, had hoped for.

However, it was intended as an interim measure only, pending the adoption of a long-term legal framework to address child sexual abuse at the EU level. The EC emphasised this to the co-legislative bodies in order to gain their support, given that Chat Control 1.0 clearly conflicted with the EU's established legal framework for privacy policies, as set out in Directive 2002/58/EC ('the ePrivacy Directive') and Regulation (EU) 2016/679 ('the General Data Protection Regulation', or GDPR). The conflict was particularly apparent in relation to the necessity and proportionality of automatically analysing all text-based communications.

Failure to present the anticipated long-term legal framework in a timely manner led to an initial extension of the legal force of the interim 'Chat Control 1.0' legislation, which had been set to expire on 3 April 2026. However, even this extended period proved insufficient for the European Commission to develop a comprehensive long-term strategy to combat CSAM. Consequently, in an effort to address the regulatory gap, the Commission proposed a further extension, alongside plans to make the original Interim Regulation permanent (commonly referred to as 'Chat Control 2.0'). This approach, however, was not endorsed by MEPs, who did not accept the premise that an imperfect measure was preferable to no framework at all. The proposal was ultimately rejected by the European Parliament in a closely contested vote on 26 March.<sup>3</sup>

### **Tough Trilogue Disputes: When Surveillance Opponents Clash with Security Advocates**

Those who expected the negotiations to be rather routine and predictable may have been surprised. During the first round of negotiations between the Council of the EU and the Parliament, several MEPs emphasised their readiness to advocate strongly for

privacy and data protection, thereby reinforcing the broader tendency within Parliament to align more closely with a privacy-protection perspective than with a 'Nothing to Hide' approach. For example, Birgit Sippel (S&D/DEU), while recognising the responsibility to address the horrific crime of child sexual abuse, emphasised in her statement the importance of safeguarding fundamental rights for all.<sup>4,5</sup>

The EU governments have indicated their willingness to compromise on digital privacy for the sake of online security, especially when it comes to protecting children. Thus, tough negotiations and carefully balanced compromises were required to give the legislation a realistic prospect of adoption by both legislative bodies during the trilogue process.

Several crucial amendments proposed by the MEP to the original Commission proposal were negotiated during the trilogue sessions. Firstly, the European Parliament rejected the proposed two-year extension (until 3 April 2028) and instead proposed a one-year extension.<sup>6</sup> The next amendment aimed to strengthen the focus on data processing in line with the proportionality principle, by (1) restricting automated analysis to *known* online child sexual abuse material, (2) limiting the *detection of the solicitation of children* and (3) not allowing the *processing of interpersonal communications for which end-to-end encryption has been, is, or will be used*.<sup>7</sup> The third proposed amendment suggested limiting the users whose communications could be scanned to those representing a higher risk, such as *individual users, specific groups of users or subscribers to a specific communication channel, who had been identified by the competent judicial authority*.<sup>8</sup> Ultimately, the scope of regulation should have been limited to instances where the *provider has received a specific report or notification regarding child sexual abuse from a user, a trusted flagger, or an organisation acting in the public interest concerning a particular communication*.<sup>9</sup>

As the Council of the EU rejected the EP-approved amendments to the original EC proposal, the final vote on the proposal was also rejected in a neck-and-neck vote (36 % in favour (228 votes); 49 % against (311 votes); 15 % abstentions (92)).<sup>10</sup> As a direct consequence, the Interim Regulation expired on 3 April 2026 without the promised replacement by the long-term legal framework to address child sexual abuse at the EU level.

## No Fear of Legal Limbo

Following the failure of the legislation, initial critiques highlighted the vulnerability of victims and the unnecessary risk posed to children by limitations on national authorities' ability to protect them, which would be exacerbated by the loss of access to automated analysis of all text-based communications. According to advocates of the implementation of 'Chat Control 2.0' or at least the prolongation of the legal effects of the Interim Regulation, these limitations could indirectly empower perpetrators by hindering disclosure.

Many of these arguments had already been challenged prior to the final vote on the proposal. First, targeted telecommunications surveillance based on concrete suspicion and authorised by a judicial warrant remained fully available after 3 April 2026. Moreover, statistical evidence – for example from Ireland – suggests that the inaccuracy rate of reported cases is relatively high, indicating current limitations in the technical capacity required to render such measures sufficiently reliable and proportionate.<sup>11</sup> This evidence lends support to the opinion of the European Data Protection Supervisor on 'Chat Control 1.0', particularly with regard to the necessity and proportionality of the automated analysis of all text-based communications.<sup>12</sup>

Rather than making 'Chat Control 1.0' a permanent regulation, terminating it primarily prevents social media platform providers — many of which are registered outside the EU — from scanning and analysing users' communications in an unnecessary and disproportionate manner.<sup>13</sup> Even if you have nothing to hide, there is no valid reason why your conversations should be the subject of automated analysis for whatever reason the provider may have.

## Conclusion

The insurmountable obstacles to reaching a compromise between the European Parliament and the Council of the EU on balancing privacy protection

with security on online platforms came as no surprise. The two legal bodies have been in conflict for a long time over 'not if, but how' to secure online platforms.

Given recent developments in France, Denmark, and Ireland – where national governments have proposed bans or age restrictions (typically 15 or 16) – the Council's position was to be expected. The European Parliament, by contrast, has consistently prioritised strengthening the rights of EU citizens and their control over privacy and personal data. This divergence reflects a deeper structural tension between a security-oriented regulatory logic and a rights-based digital governance approach. Unless a shared normative framework emerges, future negotiations are likely to reproduce the same deadlock, potentially shifting meaningful regulatory outcomes to the national level.

What lessons have been learned from presenting the Interim Regulation as a proposal for permanent regulation and from the trilogue process? In this particular case, the outcome can be interpreted as a victory for privacy, though this does not necessarily translate into a broader normative success, as a comprehensive legal framework to address child sexual abuse in the digital sphere remains absent. Nevertheless, it is evident that social media platforms and their lobbyists have actively campaigned to prevent the loss of access to automated analysis of user communications, framed under the ostensibly noble objective of protecting child victims of sexual abuse – albeit ultimately without success.

What can we expect or hope for next? Policymakers must find solutions that will effectively protect children from online predators. 'Chat Control 2.0' was not the right solution. However, this does not diminish the importance of ensuring a safe online environment; on the contrary, it is arguably more important than ever. The focus of future discussions should therefore be on what is truly at stake, and on the societal and legal costs that different approaches entail. The 'nothing to hide' principle has not been adopted as a guiding standard within the EU's legal framework.

## References

1. *Regulation (EU) 2021/1232 of the European Parliament and of the Council*, EUR-Lex (European Union law database). Published on July 30, 2021. Quoted on March 28, 2026.
2. Bellanova, Rocco, 2017: *Digital, politics, and algorithms: Governing digital data through the lens of data protection*. *European Journal of Social Theory*, Vol. 20(3), pp. 329–347; Cavelti, Myriam & Leese, Matthias, 2018: *Politicising Security at the Boundaries: Privacy in*

- Surveillance and Cybersecurity. *European Review of International Studies*, Vol. 5, No. 3, pp. 49-69; Unver, H. Akin, 2017. DIGITAL CHALLENGES TO DEMOCRACY: POLITICS OF AUTOMATION, ATTENTION, AND ENGAGEMENT. *Journal of International Affairs*, Vol. 71, No. 1, pp. 127-146.
3. [Vote Result: Proposal for a regulation of the European Parliament and of the Council amending Regulation \(EU\) 2021/1232 as regards the extension of its period of application](#). Published on March 26, 2026. Quoted on March 28, 2026.
  4. Soares, Joana: [MEPs vote to extend 'Chat Control' rules to 2027, but limit scanning](#). *EU Perspectives*. Online. Published on March 11, 2026. Quoted on March 28, 2026.
  5. EP PRESS. [Child sexual abuse online: statement by the rapporteur on extending temporary rules](#). Online. Published on 17 March 2026. Quoted on March 28, 2026.
  6. [Amendments adopted by the European Parliament on 11 March 2026 on the proposal for a regulation of the European Parliament and of the Council amending Regulation \(EU\) 2021/1232 as regards the extension of its period of application \(COM\(2025\)0797 – C10-0370/2025 – 2025/0429\(COD\)\)](#). Published on March 11, 2026. Quoted on March 28, 2026.
  7. *Ibid.*
  8. *Ibid.*
  9. *Ibid.*
  10. See also Reference 3.
  11. Cronin, Olga, 2012: [An Garda Síochána unlawfully retains files on innocent people who it has already cleared of producing or sharing of child sex abuse material](#). *Irish Council for Civil Liberties*. Published on October 22, 2022. Quoted on March 28, 2026.
  12. EDPS 2026: [European Data Protection Supervisor. Opinion 7/2026 on the Proposal for a Regulation extending the application of Regulation \(EU\) 2021/1232](#). Online. Published on: 16 February 2026
  13. Breyer, Patrick, 2026: [The Battle Over Chat Control: How EU Governments and the Tech Lobby Are Trying to Overturn Parliament's Vote — A Comprehensive Fact Check](#). Online. Published on March 24, 2026. Quoted on March 28, 2026.; Breyer, Patrick, 2026: [Historic Chat Control Vote in the EU Parliament: MEPs Vote to End Untargeted Mass Scanning of Private Chats](#). Online. Published on March 11, 2026. Quoted on March 28, 2026.