— FZI Position on Chat Control

Initiative jeopardizes the fundamental right of security and confidentiality in digital communication

Version: 1.0
Publication: 09/27/2024
Editors: Aline Vugrincic, Maria Rill, Samuel Kalbfleisch

Table of Contents

1 Our request: Protect the security and confidentiality of digital communication

The draft "Regulation laying down rules to prevent and combat child sexual abuse", currently being prepared by the Council of the European Union[1], aims to better protect children and young people from sexual abuse in the digital space. This aim is undisputed. According to our scientific analysis, the envisaged implementation fails to achieve this very aim. It suggests a technical solution that, due to the state of the art, currently does not exist.

Instead, the implementation of what is better known as the CSA Regulation or Chat Control EU initiative will, in the future, allow state security authorities new possibilities unintended by the legislator, such as mass surveillance. On entry into force of the draft regulation, a major infringement of the fundamental right to security and confidentiality of digital communication affecting all residents of the European Union (EU) and shaking a cornerstone of our democratic community of values will occur.

We, therefore, demand the preservation and continued protection of the fundamental right to security and confidentiality of digital communication. The planned technical implementation of chat control massively jeopardizes the confidentiality of even end-to-end encrypted chat messages. The European Union should, therefore, not transform the CSA Regulation in its current form into an EU Directive or Regulation.

[1]https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52022PC0209, last accessed on 25.09.2024

2 Plea and appeal to you

We believe the CSA Regulation must not enter into force in its current form. In the digital space, too, a functioning democracy needs secure, private communication.

Implementing the planned chat control constitutes a considerable intrusion into individual freedom rights. It enables state mass surveillance that makes every EU resident vulnerable.

We currently see no possibility of a technically practical and, at the same time, fundamental rights-compliant implementation of a chat control. Instead, we see the draft CSA regulation being put to the vote as a threat to democracy and personal freedom by weakening fundamental rights. We are convinced that the declared aim of chat control, which is to provide more effective protection for children and young people, will not be achieved.

The Council of the European Union intends to vote on the draft CSA Regulation as early as October 10, 2024. We therefore ask and appeal to you for the following:

- If you are eligible to vote in the Council of the European Union, we urge you to vote for preserving fundamental rights in the EU and against the draft CSA Regulation for the reasons set out below.
- Support the politicians concerned with home and judicial affairs in the executive and legislative with the background information presented below.
- Raise awareness among colleagues in the European Parliament, the German Bundestag, and the state parliaments about the threat to the fundamental right to security and confidentiality of digital communication.
- Draw attention to the fact that a highly relevant social problem cannot be solved by unsuitable technical means and to the danger to democracy and personal freedom that would result from implementing the CSA Regulation.

3 Chat control as a solution?

Based on the reported figures on the production and dissemination of abusive depictions of children and adolescents, the Federal Criminal Police Office (BKA) compiles an annual "Federal Situation Report on Sexual Offenses against Children and Adolescents." The number of these cases[2] has grown continuously in recent years. According to the BKA, around 180,300 reports were received in 2023. This is a growth of 32% compared to the previous year, 2022. Almost half of the reports, around 89,350, were relevant under German penal law. The massive problem of sexual harassment of minors, such as cyber grooming[3] , is thus evident.

The debate on possible solutions against the harassment of children and young people on the internet has been going on for many years. In 2022, the EU Commission published the CSA Regulation as its proposal for tackling the problem. This is commonly known as "chat control".

Scientists at the FZI Research Center for Information Technology have looked at the CSA Regulation in-depth. They investigated the extent to which the solution proposed by the EU Commission in the form of so-called chat control could improve the situation of increasing harassment of children and young people on the Internet, and how the adequate technical implementation of this solution could be realized. As an independent, non-profit foundation for applied ICT research with a social mission, we examined the draft text of the CSA Regulation from both a technical and legal perspective.

3.1.1 Revoking of chat privacy and end-to-end encryption

The Council of the European Union was due to vote on the draft CSA Regulation as early as June 2024. The item was then removed from the agenda[4] . The various EU governments were now expected to take a position on a new draft text of the CSA Regulation by the time of an informal preparatory meeting on September 23, 2024. This was prepared and submitted by the Hungarian Council Presidency[5] . A formal vote in the Council of EU Justice and Home Affairs Ministers[6] is to take place at its next meeting on October 10/11, 2024[7] .

The draft EU regulation promoted by the Hungarian EU Council Presidency

- aims to ensure that messages from diverse messengers such as WhatsApp, Threema or Signal should be scanned for images of child sexual abuse as a general preventative measure and
- social media platforms such as Instagram or TikTok should be obliged to take measures to prevent the uploading and distribution of abusive material on the Internet.

[2]https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/SexualdeliktezNvKindernuJugendlichen/2023/BLBSexualdelikte.html, last accessed on 25.09.2024

[3]https://www.bka.de/cybergrooming.html, last accessed on 25.09.2024

[4]https://data.consilium.europa.eu/doc/document/ST-11222-2024-INIT/en/pdf#page=30, last accessed on 25.09.2024

[5]https://www.parlament.gv.at/dokument/XXVII/EU/195500/imfname_11406149.pdf, last accessed on 25.09.2024

[6]https://www.consilium.europa.eu/en/meetings/jha/2024/10/10-11, last accessed on 25.09.2024

[7]https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/chatkontrolle-neue-abstimmung-fuer-10-oktober-angesetzt, last accessed on 25.09.2024

To this end, the encryption of chat messages is also to be bypassed. Content will be monitored already on the user's end device using client-side scanning technology[8] .

It can be assumed that those who possess and intend to circulate abusive images will evade chat control. They will switch to alternative messenger services, sending methods, or manual data encryption. This means the persons that should be identified via chat control would still be difficult or impossible to trace. Meanwhile, other users would have to accept disproportionate interference with their rights.

Another reason why chat control is not effective is the fact that the majority of "child abuse content is shared via platforms and forums", according to the Vice President of the Child Protection Association[9] , Joachim Türk, in an interview.

3.1.2 Practical significance and implementation

Many modern messenger services use end-to-end encryption to ensure privacy and data protection when dispatching messages.

This procedure protects messages during transmission over the Internet. Only the sender and recipient of the message can read it. Neither the messenger provider, Internet service providers, hackers, or state actors can decipher the content of the message.

The efforts of the EU institutions and, currently, the Hungarian Council Presidency to introduce chat control counteract this protection. In the future, all messages from everyone in the European Union would be automatically checked for criminal content, and in the event of suspicion the message would be forwarded unencrypted.

For the technical implementation of such a chat control, providers would have two options:

- Abandonment of end-to-end encryption. In the future, the messenger operator could read out and scan all messages right on the server. This option would significantly limit the confidentiality of all chat messages and completely abolish it as regards the operator.
- With client-side scanning, the messages are scanned on the end user's device, for example, on the smartphone. In case of suspicion, the confidentiality of the chat messages is then bypassed, and the message is forwarded unencrypted. This means that monitoring software is integrated into all cooperating messenger apps. Technically savvy users can circumvent this second option of client-side scanning. This applies in particular to apps such as Signal or Threema, the source code of which is publicly available.

The envisaged approach to chat control is, therefore, not effective. It falls short of the aim to protect children and young people from abuse.

Instead, the chat control approach curtails the fundamental rights of all EU residents. It lays the foundation for in-depth mass surveillance that erodes privacy and undermines a cornerstone of democracy. End-to-end encryption is also a protection against mass surveillance by the state. The latter has been used time and

[8]ibid.; https://www.bundestag.de/resource/blob/984702/6757ed249bcad12a6e00864d7a410fda/30-Sitzungsprotokoll-mit-Anlagen-OeA.pdf, last accessed on 25.09.2024
[9]https://www.deutschlandfunk.de/chatkontrolle-eu-messenger-kindesmissbrauch-scanning-durchsuchung-kommission-gesetzentwurf-100.html, last accessed on 25.09.2024

again by governments, regimes, and secret services in the past and present to monitor and suppress their people. State-collected data is even repeatedly misused for private interests[10] .[11]

In addition, the draft CSA regulation requires messenger services to monitor all messages sent through them for content of this kind. The authors envision an automated decision as to whether a message contains unwanted material. If a message is found to contain unwanted material, it will be diverted for further review.

For obvious reasons, all messages must be scanned to uncover any illegal content. In the postal service's letter business, this would correspond to opening all letters in all distribution centers every day and checking for unwanted content.

The original draft of the regulation stipulates that both known and new forms of abuse should be recognized. Cyber grooming is also to be covered. The form of the content is not restricted in the regulation, which means that in addition to visual content, text and voice messages are also included. The compromise proposal of the Hungarian Council Presidency envisages that cyber grooming and scanning for previously unknown material should be left out for the time being. However, Hungary proposes to expand chat control accordingly in a later regulation[12] .

At the same time, however, providers of messenger services themselves could use the unencrypted information for their own purposes in the future. This would enable them, for example, to adapt the focus of message content to their own expectations or those of sponsors and advertising partners.

Depending on the quality of the technical implementation in messenger apps, there is also a significant risk that third parties could exploit the planned chat control for espionage, data theft, manipulation, or blackmail, for example. Subsequent extensions to the CSA Regulation are already envisaged in the current draft, as, for example, proposed by the Hungarian Council Presidency. An existing legal and technical basis for message snooping greatly facilitates a politically desired short-term adjustment of the surveillance scope.

Conclusion: Chat control de facto ends the privacy of chat messages. It also questions end-to-end encryption, one of the cornerstones of digital communication security. A number of messenger services, therefore, reject the Chat Control Regulation[13] . Signal and Threema have already announced their withdrawal from the EU market if the worst comes to the worst. According to the company, Threema would take legal action against chat control or even circumvent it[14] .

---

[10]https://www.behoerden-spiegel.de/2024/09/18/berliner-datenschutzbericht-veroeffentlicht, last accessed on 25.09.2024

[11]https://www.bpb.de/shop/zeitschriften/izpb/china-337/275566/situation-von-medien-und-internet; https://freedomhouse.org/country/china/freedom-world/2024, last accessed on 25.09.2024

[12]https://www.patrick-breyer.de/wp-content/uploads/2024/09/st12406.en_clean.pdf, last accessed on 25.09.2024

[13]Meredith Whittaker, Signal President, New Branding, Same Scanning: "Upload Moderation" Undermines End-to-End Encryption; https://signal.org/blog/pdfs/upload-moderation.pdf; EU's Chat Control puts security and privacy at risk; https://element.io/blog/eus-chat-control-puts-security-and-privacy-at-risk; https://threema.ch/de/blog/posts/chatkontrolle-stoppen, last accessed on 25.09.2024

[14]https://threema.ch/de/blog/posts/chatkontrolle-stoppen; https://www.chip.de/news/Zieht-sich-Signal-aus-Europa-zurueck-Das-steckt-dahinter_185303157.html, last accessed on 25.09.2024

3.1.3 The use of Artificial Intelligence is foreseeable

If previously unknown abusive content or grooming is to be recognized in the future, as already envisaged by the Hungarian Council Presidency, it is foreseeable that error-prone AI systems will be employed as the standard means. While known image representations can still be recognized via hashes with a comparatively low false positive rate, significantly more error-prone systems, such as AI classifiers, must be used for the automated assessment of unknown content. These have high false positive rates. Many chat messages with legitimate content would also be erroneously classified as abusive material or cyber grooming.

Even if an object is correctly recognized as a human by an AI classifier, interpreting this representation is a further challenge, such as distinguishing a legitimate vacation photo of a child on the beach from criminally relevant pictures that suggest abuse. Estimating the age of a person depicted can be a challenge, even for humans. Teenagers who voluntarily and consensually send such images or texts could also be increasingly confronted with legal problems if their messages are interpreted as CSA material (so-called "schoolyard cases"[15]).

The requirement to detect cyber-grooming also involves extensive automated scanning and interpreting of text messages. Since even people find it difficult to distinguish unwanted from wanted contact attempts without the appropriate context, a particularly high rate of false positives can be expected when classifying messages using AI systems.

3.1.4 Revoking of encryption could violate several fundamental rights

The CSA regulation could be contrary to EU law because it may violate several articles of the Charter of Fundamental Rights of the European Union (CFR). For example, chat control is contrary to the right to privacy (Art. 7 CFR), which protects the confidentiality and integrity of communication. Users could also be obliged to share data, such as their real name or age, for identification and verification purposes. This would make anonymous communication in private, as well as for whistleblowers or marginalized groups, more difficult – if not impossible.

In addition, there could also be a violation of the right to informational self-determination at the national fundamental rights level, Art. 2 para. 1 in conjunction with Art. 1 para. 1 GG. Users can no longer trust that their communication is protected and invisible to third parties16. " If individuals cannot, with sufficient certainty, determine what kind of personal information is known to certain parts of their social environment, and if it is difficult to ascertain what kind of information potential communication partners are privy to, this could greatly impede their freedom to make self-determined plans or decisions17". As early as 1983, the Federal Constitutional Court argued that unlimited data collection threatened the free basic order[18] . To (almost) override this in such a way through chat control is a substantial departure from the enshrined and guaranteed fundamental rights. Communication via emails, text messages, and chats is also protected by the secrecy of telecommunications under Art. 10 para. 1 GG. A restriction of this right is only possible based on law and must also be proportionate. The interference with the protected sphere of these fundamental rights by the chat control is, in any case, not or only very unlikely to be proportionate.

[15]https://www.heise.de/news/Nacktfotos-So-will-Justizminister-Buschmann-Schulhof-Faelle-entkriminalisieren-9532696.html, last accessed on 25.09.2024
[16]Marquard in ZD-Aktuell 2024, 01628
[17]BVerfG (First Senate), judgment of December 15, 1983, Ref. 1 BvR 209/83, para. 73
[18]ibid. para. 74

As part of the examination, the protection of children and young people in relation to the protection of each individual person with regard to the monitoring of chat messages must be considered. In 2023, 2,580 cases of cyber-grooming were recorded in the police crime statistics, with the dark figure estimated to be much larger[19]. In the same period, an estimated 400 billion messages were sent via various messengers or text messages[20]. Cyber grooming, therefore, only affects a fraction of this massive volume of messages. This raises the question of whether it is proportionate for everyone to have to give up their digital privacy. In addition, it remains possible to circumvent the security precautions of chat control. Furthermore, many perpetrators will be difficult to identify. The actual goal of protecting children and young people from abuse and harassment is, therefore, very likely to be missed.

It is doubtful that the purpose of chat control, which is to prevent and combat the sexual abuse of children and young people, can be achieved through monitoring. Perpetrators could exchange content via other channels, and children and young people could continue to become victims of sexual abuse. Depending on the technical design, children and young people could continue to be confronted with messages or content, meaning that the desired and necessary protective purpose would also fall short here.

The Child Protection Association emphasizes that children's rights to freedom of expression and participation are also being curtailed: The fear of being constantly monitored could impair children's development, as they would no longer be able to inform themselves about specific topics or seek help without fear of consequences[21] .

Turning away from the presumption of innocence

The widespread use of chat control would place all users under general suspicion of disseminating images or video material or grooming via text messages[22]. However, Art. 48 para. 1 CFR guarantees the presumption of innocence, meaning that everyone is presumed innocent until proven guilty in legally binding court proceedings. Arbitrarily suspecting people of possessing CSA material or grooming contradicts this presumption of innocence. However, if everyone's chats were to be monitored without cause, this would seriously jeopardize the principle of the presumption of innocence. To date, the Code of Criminal Procedure only provides for surveillance by law enforcement authorities if this is ordered by the public prosecutor's office or a court. This also constitutes an encroachment on fundamental rights, but the proportionality of the encroachment must be reviewed. The intervention may be disproportionate, for example, if an alternative less intrusive measure than telecommunications surveillance could fulfill the intended purpose. Such an approach is not planned in the CSA Regulation.

Interference with the right to informational self-determination in accordance with data protection

Monitoring and analyzing users' communications through chat control could also violate data protection regulations, as it potentially involves users' personal data without ensuring adequate security and data protection measures. Providers of personal communication services shall take the necessary measures for age verification and assessment in accordance with Art. 4 para. 3 of the CSA Regulation so that underage

[19]https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/cybergrooming, last accessed on 25.09.2024
[20]https://www.bitkom.org/Presse/Presseinformation/Eine-Milliarde-Kurznachrichten-pro-Tag, last accessed on 25.09.2024
[21]https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, last accessed on 25.09.2024
[22]https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, last accessed on 25.09.2024

users can be reliably identified. The same obligation also applies to providers of stores for software applications pursuant to Art. 6 para. 1 lit. b and lit. c of the CSA Regulation. There is a risk that several individuals or groups of individuals could gain access to the required identification data[23]. It could happen that providers of the various services have to check all data processed via or with their services for the content specified in Art. 7 para. 4 of the CSA Regulation[24] .

[23]https://www.dr-datenschutz.de/die-chatkontrolle-eu-kommission-auf-abwegen, last accessed on 25.09.2024

[24]https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf, last accessed on 25.09.2024

4 Chat control misses the real target

The introduction of chat control to prevent and combat child sexual abuse does not address the root causes of the problem and only suggests a technical solution. If the chat control currently proposed in the draft is implemented, the actual goal will be missed, and instead, a far-reaching intrusion into the fundamental right to security and confidentiality of communication will occur.

Analysis proves the following:

- The confidentiality of chat messages and end-to-end encryption safeguard the fundamental rights of 450 million EU citizens.[25]
- The protection of children and young people on the Internet through the planned measures will, at best, be achieved temporarily and only highly fragmented. More likely, though, it will be completely missed.[26]

Protecting children and young people requires appropriate technical[27] , legal, educational, and healthcare measures. Cyber grooming has been prohibited under Section 176 of the German Criminal Code since 2020. Technical measures are being tested, for example, as part of a cooperation between the online platform Knuddelz and the BKA.[28] However, as the BKA's 2024 situation report and the continuing increase of case numbers show, the current measures are insufficient.

Crucial, for example, are the early education and training of children and parents, both inside and outside of schools.[29] Mass surveillance, on the other hand, would also curtail the freedom of children, as the German Child Protection Association emphasized in its statement to the German Bundestag[30] .

About the FZI

The FZI Research Center for Information Technology, with headquarters in Karlsruhe and a branch office in Berlin, is a non-profit institution for information technology application research and technology transfer. It delivers the latest scientific findings in information technology to companies and public institutions and qualifies individuals for academic and business careers or the leap into self-employment. Supervised by professors from various faculties, the research groups at the FZI develop interdisciplinary concepts, software, hardware, and system solutions for their clients and implement the solutions found as prototypes. The FZI House of Living Labs provides a unique research environment for application research. The FZI is an innovation partner of the Karlsruhe Institute of Technology (KIT) and strategic partner of the German Informatics Society (GI).

---

[25]https://www.datenschutzkonferenz-online.de/media/en/20231017DSKEntschliessungChatkontrolle.pdf, last accessed on 25.09.2024
[26]Zurawksi in ZD-Aktuell 2022, 01240
[27]https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Kinderschutz-im-Internet/kinderschutz-im-internet_node.html, last accessed on 25.09.2024
[28]https://hilfe.knuddels.de/de/articles/7983486-knuddels-und-das-bka-starten-kooperation, last accessed on 25.09.2024
[29]https://link.springer.com/article/10.1007/s00787-024-02566-9, last accessed on 25.09.2024
[30]https://www.bundestag.de/resource/blob/935798/3c6f75f6c2056130bca757bf7b4d0445/Stellungnahme-Tuerk-data.pdf, last accessed on 25.09.2024

Further information and contact

Jérôme Nguyen, Communications
FZI Research Center for Information Technology
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
Phone: +49 721 9654-924
E-mail: presse@fzi.de
Internet: www.fzi.de

Maria Rill, Research Division Cybersecurity and Law
Department Law
FZI Research Center for Information Technology
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
E-mail: m.rill@fzi.de

Samuel Kalbfleisch, Research Division Cybersecurity and Law
Department Security Engineering
FZI Research Center for Information Technology
Haid-und-Neu-Str. 10-14, 76131 Karlsruhe
E-Mail: Kalbfleisch@fzi.de