

Dear Council of the European Union,

Dear national governments,

In the last days of the Belgian EU Council Presidency, Belgium has put forward its final initiative to reach a general approach in the Council of the EU regarding the highly contested CSA regulation (*Proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*). In possibly putting the CSA Regulation to a vote on 19 June, the Council is risking far more than just passing a simple regulation.

Sexual abuse and the exploitation of children, including the dissemination of child sexual abuse material, must be addressed with the utmost determination in accordance with the rule of law. While the regulation proposal put forward by the EU Commission includes some good and crucial measures, such as the EU center, it is highly questionable whether core aspects of the regulation are compatible with European fundamental rights.

As parliamentarians, we observe with great concern the proposal of the Council of the EU that would put to an end the confidentiality of private communication. Even if the Belgian Council Presidency has now presented a compromise proposal that would limit the obligation to scanning private unencrypted as well as encrypted video and image content, it remains just as much an encroachment on fundamental digital rights and takes the discussion back to the origin of the debate. In fact, the Belgian proposal represents the Commission's first plans that came to light in December 2021.

Safe and encrypted communication is of utmost importance for every human being. This also accounts for children and victims of sexual abuse to allow for safe emergency and help services - particularly in countries where victim support organisations cannot rely on the support and confidentiality of state law enforcement authorities.

Besides risking to contradict the aim of the CSA proposal by intervening in the digital self-determination of people, there might be several unintentional but dangerous side effects:

- **Client Side Scanning (CSS) and any other mass surveillance, would render confidential information carriers impossible:** Scanning would affect users who rely on confidential communication and whose communication is particularly protected (professionals bound by confidentiality such as journalists, lawyers, the medical sector, but also whistleblowers). Furthermore, built-in backdoors could compromise the confidentiality of digitally transmitted trade secrets and business transactions. Encryption protects the identity and the contents of communication participants, thus preserving the autonomy of victims of sexual violence.
- **Democratic society and democratic debate need trustworthy spaces:** Democratic societies need privacy for the formation of opinions and will. The proposed measures carry the danger of leading to self-censorship, jeopardizing safe spaces for children and victims of sexual violence, but also for everyone else. It will also likely leave to users unwilling to use digital services and lose trust in providers if their data is not secure and protected.
- **Blueprint for authoritarian states and weakening cybersecurity:** By building an architecture capable of undermining all possibility of private digital communication, the regulation might inadvertently serve as a blueprint for surveillance in authoritarian states and can serve as a built-in backdoor that can easily be exploited for all sorts of surveillance practices (e.g. trade secrets) and cybercriminals. Once built, this IT-architecture is an invitation to undermine privacy.
- **Impairment of digital educational, youth, and assistance services:** It will eliminate the common practice to exchange important sexual health information

via encrypted messages, especially when young people do not have easy access to such education as is case in some European countries.

The mandatory investigation of private communication messages without suspicion carries the risk of creating a climate of general suspicion. Such an approach will irreparably damage the image of the European Union as a guarantor of freedom.

We explicitly warn that the obligation to systematically scan encrypted communication, whether called “upload-moderation” or “client-side scanning”, would not only break secure end-to-end encryption, but will to a high probability also not withstand the case law of the European Court of Justice. Rather, such an attack would be in complete contrast to the European commitment to secure communication and digital privacy, as well as human rights in the digital space.

We therefore urgently need an approach that prioritizes the protection and prevention of child sexual abuse, provides more resources and better-targeted coordination of European law enforcement authorities, strengthens victim support in accordance with fundamental rights, and avoids relying on a false sense of security through technosolutionism.

As national and European parliamentarians, we are convinced that the proposed measures are incompatible with European fundamental rights. We are committed to safeguarding the right to anonymous and pseudonymous use of the internet, as well as strengthening end-to-end encryption.

We urgently call on all negotiating governments in the COREPER to reject a general approach based on compromise proposal that Belgium has put forward.

Signatories

Tobias B. Bacherle, MP, Alliance 90/The Greens, Germany

Maximilian Funke-Kaiser, MP, FDP, Germany

Konstantin von Notz, MP & Vice Chair of the group, Alliance 90/The Greens, Germany

Konstantin Kuhle, MP & Vice Chair of the group, FDP, Germany

Süleyman Zorba, MP, The Greens, Austria

Sven Clement, MP, Pirates, Luxembourg

Rasmus Andresen, MEP, The Greens/EFA, Germany

Maik Außendorf, MP, Alliance 90/The Greens, Germany

Michael Bloss, MEP, The Greens/EFA, Germany

Damian Boeselager, MEP, The Greens/EFA, Germany

Patrick Breyer, MEP, The Greens/EFA, Germany

Georg Bürstmayr, MP, The Greens, Austria

Marcel Emmerich, MP, Alliance 90/The Greens, Germany

Emilia Fester, MP, Alliance 90/The Greens, Germany
Alexandra Geese, MEP, The Greens/EFA, Germany
Stefan Gelbhaar, MP, Alliance 90/The Greens, Germany
Andreas Glück, MEP, Renew Europe, Germany
Sabine Grützmacher, MP, Alliance 90/The Greens, Germany
Svenja Hahn, MEP, Renew Europe, Germany
Katrin Helling-Plahr, MP, FDP, Germany
Manuel Höferlin, MP, FDP, Germany
Misbah Khan, MP, Alliance 90/The Greens, Germany
Marcel Kolaja, MEP, The Greens/EFA, Czech Republic
Moritz Körner, MEP, Renew Europe, Germany
Katharina Kucharowits, MP, SPÖ, Austria
Denise Loop, MP, Alliance 90/The Greens, Germany
Boris Mijatovic, MP, Alliance 90/The Greens, Germany
Maximilian Mordhorst, MP, FDP, Germany
Hannah Neumann, MEP, The Greens/EFA, Germany
Dr. Nikolaus Scherak, MP, NEOS, Austria
Jan-Christoph Oetjen, MEP, Renew Europe, Germany
Tabea Rößner, MP, Alliance 90/The Greens, Germany
Michael Sacher, MP, Alliance 90/The Greens, Germany
Kordula Schulz-Asche, MP, Alliance 90/The Greens, Germany
Kim van Sparrentak, MP, The Greens/EFA, Netherlands
Marie-Agnes Strack-Zimmermann, MP, FDP, Germany