Massive gaps and faulty assumptions: A feminist look at the CSA regulation

Elina Eickstädt and Elisa Lindinger

The EU Commission draft "Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse," also known as the CSA regulation or the CSAR file, has been massively criticised by civil society since May 2022. The debate shows that there are massive gaps and faulty assumptions in digital policy legislations.

The limits of technosolutionism

It is clear that the creation and dissemination of child sexual abuse material (CSAM) must be actively fought against. However, the CSA regulation falls short of this as it only proposes a series of technical solutions. This is problematic insofar as it is based on imprecisely defined technologies that are still to be developed instead of looking at existing, successful child protection structures and their further development. And so, technical innovations are prioritised instead of social intervention, support and empowerment.

Such a process can and must be criticised as technosolutionism. Technosolutionism assumes that every problem can be resolved with technical innovations. However, this is not only a short-sighted perspective, it also forgets that new problems can also arise through the introduction of complex new technical systems. This is particularly obvious when looking at algorithmic decision-making systems: The CSA regulation proposes that this method is used to automatically detect illegal content and forward it to law enforcement authorities. But how this detection works technically is not mentioned in the proposal – it remains "technology-neutral". However, the automated flagging of content is a far more complex problem than may be assumed from the outside. Even today, other application cases clearly show that communications in under-represented groups are flagged far more than the average by such algorithms and without any substantive basis. The technical solution therefore promulgates social discrimination,

while at the same time appearing to be objective and thus less subject to attack. Naive technosolutionism blends out the fact that technical solutions can always only be as neutral as the group that creates them and the data they are based upon.

The discussion about simple and clean technical solutions also ignores the fact that a high level of human intervention is still often necessary. Even though the CSA regulation proposes reporting and checking structures in the form of an EU Centre, it is likely that large tech companies will initially use existing content moderation structures and check notifications internally before transmitting suspicious cases to the EU Centre. Content moderators work under high pressure and tight schedules, and are exposed to extremely mentally stressful content every day. The CSA regulation will mean a huge expansion of this highly problematic field of work, but without any definition of the necessary occupational safety measures. Proposals that set out how working conditions must be improved already exist.

Breaking encrypted communication is not an option

The CSA regulation proposes that all interpersonal communication should be scanned. This covers all possible digital communication channels – messenger apps, chats on game platforms, learning apps, etc. Even applications that encrypt communication between conversation participants, and which are supposed to be particularly secure, are not excluded. This means: Real end-to-end encrypted communication would therefore no longer be possible. Because such checks would not be implemented in a specific case of suspicion, but would be constant and everywhere. Because encryption is binary: it is either intact and cannot be attacked easily or it is broken and therefore vulnerable to attacks.

International IT security experts and the United Nations High Commissioner for Human Rights are warning about the proposed technologies for client-side scanning in the impact assessment of the regulation. Because, in this process, files are searched for illegal material on the user device and, if deemed to be suspicious, are diverted before actual encryption takes place. Users therefore lose all control over the confidentiality of their communication. However, privacy is a fundamental right, according to the European Convention on Human Rights (Art. 8). The proposal weakens existing member state legislation, such as the German fundamental right to confidentiality and

probity in information technology systems that protects digitally stored or edited personal data and private communications. Preventive interventions in this protected area face considerable obstacles and are only permissible when warranted, i.e., if there is a specific case of suspicion. The CSA regulation will mean that such protected areas will factually no longer exist and will be subject to continuous machine and human monitoring.

The right to privacy is however essential, particularly for children and young adults. From the age of 10 and onwards, children and young adults demand more privacy, while at the same time are more willing to take risks – both offline and online. Being able to garner experience and become more independent is an important developmental step towards adulthood and one that must not be withheld from children and young adults (cf. Wisniewski et al. 2022). Undermining privacy and making encryption technically impossible sends a fatal signal:
“On one hand, adults tell teens that they need to care about their online privacy to stay safe; on the other hand, as designers and parents, we develop and use surveillance technologies that take teens’ privacy away for the sake of their online safety."
(Wisniewski et al. 2022, 319)

But it is not only children and young people that have a right to privacy, including through encryption, and which must be protected. Members of disadvantaged groups, journalists, whistleblowers and lawyers are among those most affected by monitoring and misuse of power through state and other control authorities, and are therefore particularly dependent on intact encryption of their communication. Once this has been undermined, the way is free for repression.

Even if just one technical option for automatically searching and diverting communication content exists, it can also be utilised and misused for completely different purposes. The CSA regulation prioritises the right for protection against violence (UN Convention on the Rights of the Child, Article 19) above the right to privacy. Weighing these central rights against each other, although they should be actually be considered and implemented as a whole, simply leads to bold demands and deadlocked positions.

New policy proposals, regulations and guidelines, including the CSA regulation, should protect fundamental rights, not undermine them. The European declaration on digital rights and principles states the right to the confidentiality of people's communications and the information on their electronic devices (European Declaration on Digital Rights and Principles for the Digital Decade, Chapter V). Such a right is in direct contradiction to the client-side scanning proposed in the impact assessment of the CSA regulation. To ensure effective protection of encrypted communication, technologies such as client-side scanning must be prohibited. To de facto globally undermine such encrypted communication is a breach in the dam of communication integrity and the consequences will no longer be able to be reversed.

Non-existing technologies are not a solid basis for legislation

The CSA regulation does not set out any clear proposals about which specific technologies will be used to implement the measures. The responsibility for their selection and development is instead palmed off onto the tech companies. However, the technological effort required is both comprehensive and complex. On the one hand, the factual elements are not yet sufficiently defined to be able to actually develop expedient technological detection methods (for example, for so-called “grooming”, i.e., making contact with children and young persons for the purpose of abuse). And, on the other hand, existing algorithmic detection methods demonstrate significant weaknesses, regarding hate speech for instance where the context needs to be recognised and correctly evaluated. The CSA regulation is therefore looking at non-existent technologies to implement its proposals.

Additionally: Even if, theoretically, all communication providers and platform operators could develop their own technical solutions for the implementation of the CSA regulation, such processes are expensive and can essentially only be implemented by the biggest companies such as Microsoft, Alphabet or Apple, or by including specialised external companies. This has two specific consequences that are in stark contrast to all other regulatory approaches of the EU:

1. Even as the EU is struggling to regulate and limit the supremacy of tech giants, these companies have been handed an entirely new playing field, i.e., an official mandate to create and deploy highly invasive technologies that restrict the

fundamental rights of European Union citizens The digital market is therefore becoming increasingly unbalanced as the biggest tech companies continue to expand its dominant position.

2. This means that better solutions have very little opportunity to become successful. Companies that specialise in monitoring communication are amongst the strongest proponents of the CSA regulation. Their claims as to the current effectiveness of their technology can still be found (unverified) in EU political drafts.

Feminist digital policy as a solution

The current draft of the CSA regulation conflicts in many areas with intersectional feminist perspectives. It reinforces power imbalances, institutionalises paternalistic behaviour against adolescents and completely ignores the needs of other threatened groups in its considerations.

Feminist digital policy critically questions whether the use of technologies is actually expedient and searches for sustainable solutions to get to the roots of the problems. The use of technologies as a means of state and private sector surveillance is – even it is for protective purposes – ultimately paternalistic. The CSA regulation aims to protect children and young people by using machines, instead of supporting them through education and empowerment. This is something that would actually be helpful – in contrast to the CSA regulation – particularly with regards to abusive attacks at closer quarters. Social problems cannot be resolved on a purely technical basis. Social initiatives must be at the forefront in order to be really effective.

The non-negotiability of fundamental rights is also a part of a feminist digital policy perspective. The right to privacy and the right to protection against violence should not be pitted against one another. They are all essential for the social and democratic participation of everyone, particularly under-represented groups and not least for children and adolescents.

Policy drafts must be subjected to a contextual, societal impact assessment so that the legally prescribed use of technologies does not obscure existing problems or even create new challenges. The past shows that such impact assessments usually only

cover legal or technical levels. However, to create really sustainable and ethically responsible solutions, civil and economic factors must also be included. The technical implementation must also be critically accompanied and iteratively analysed. Because it is unclear which solutions are being developed regarding technology-open regulations. It is therefore even more important that the legislator is responsible for creating a basis that specifies a clear red line for ethically and legally highly problematic technologies.

The CSA regulation shows the complexity of the relationship between social problems and potential digital solutions, and how rapidly technosolutionism can lead to unintended negative consequences. It is the responsibility of legislators to unravel such complexities and develop customised, expedient solution approaches that minimise negative impacts.

Authors: Elina Eickstädt and Elisa Lindinger

February, 2023

https://feministtechpolicy.org/

A website by SUPERRR Lab

Oranienstr. 58 A

10969 Berlin

https://superrr.net/