EU Commission consultation
Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers

May 5, 2021
Das NETTZ - Vernetzungsstelle gegen Hate Speech (networking initiative against hate speech, betterplace lab): www.das-nettz.de, info@das-nettz.de

We call on the EU Commission to make digital spaces a safe place for all people. Internet service providers need to protect those people most affected of discirimination and digital violence. People most affected by digital violence need to be consistently included in the development, implementation and evaluation of all measures taken. Besides measures at political and legal level, social networks must be compelled to take more responsibility.

- Platforms and social networks must provide adequate resources in terms of personnel and expertise to ensure that negative side effects of their activities are effectively tackled.
- Civil society must be enabled to play its part in developing solutions. This includes backing for initiatives and projects that support civil society and bolster democracy in a sustainable way and a continuous dialogue with civil society activists and organizations.
- Continuous training is needed on issues such as discrimination in general, including sexism, anti-Roma discrimination and racism, among other things. Relevant staff at the internet service providers must be made aware of advisory centers for the victims of digital violence.
- Options to report potentially illegal content must be easy to find and use. Information on support for persons affected and on national contact points should be prominently displayed (example: contact points for persons at risk of suicide or info on Covid-19).
- Online communication requires fast reactions: People being attacked online need rapid access to platform teams (for example, awareness teams for rapid support in the event of hacks) to receive the support needed (e.g. delete toxic content against victims, protect their profiles, provide consultation)
- Companies should link their measures to international human rights and regularly evaluate and update the implementation of their own ethical standards.
- Advertising on platforms must be regulated more strictly, in particular with regard to political advertising: It should not be possible to advertise extremist content or content from extremist actors. Political advertising in general should be more transparent. Users have a right to know who is behind an information and if the sender has paid for its distribution.
- Extremist actors should be deplatformed, in consultation with independent experts, in case of repeated violation. Comprehensive and verifiable standards should be established, however, to protect freedom of expression as long it is legal and respects human rights.
- Furthermore, internet platforms should introduce measures to limit the scope of extremist actors and purposeful disinformation. No one has a basic right to broad coverage of harmful content.
- Internet companies (as well as policymakers and civil society) need to get to grips with extremist eco-systems in order to think and act beyond platforms. Hatred,

exclusion and verbal violence are not (only) organised on mainstream platforms and so it is all the more important and necessary to look beyond existing networks.

- Transparent communication is needed on the part of internet platforms and social networks. This applies to action and measures taken regarding the deletion of content as well as the reduction of its findability. This is necessary to demonstrate whether platform measures to tackle hatred, exclusion and verbal violence are actually working.
- The right of these companies to protect internal information to prevent that “bad actors” might be able to exploit such information must be protected. Nevertheless, it is essential that experts and academics have access to the relevant data, e.g. to enable them to draw comparisons and comprehensively evaluate how measures are working. That is the only way of developing effective regulatory measures.
- Intensified research is needed on online hatred, exclusion and verbal violence, but also on related phenomena, such as digital violence, in order to gain a better understanding of the extent of the problem. This also applies to other forms of discrimination. Data interfaces are needed for academic analysis. There is still too little research on the dissemination, coordination and perpetration of digital hate speech. One reason for this is the restrictive control over data exercised by private actors. Responsible research must be facilitated. The same applies to regulators.
- Cooperation between criminal prosecution authorities, regulators and service providers needs to be improved. To date, law enforcement has often foundered on service providers’ reluctance to comply with requests for information.
- This must apply for all companies acting in the European Union. A corporate seat or the storage of data abroad is no excuse not to comply with EU law. Within the EU, the collaboration between Member States should be faster and more effective. We we hereby plead for a restriction of the country of origin principle if otherwise a fast enforceability of youth protection and prohibition of hate crime is not possible.
- As long as hate speech goes unchallenged in comments sections its perpetrators consider themselves vindicated and continue to spread hatred. Numerous analyses and studies show that comment moderation works. Internet providers have to make moderation as easy as possible, with the help of tools, training etc. for people administrating and moderating online groups.
- It should be technically possible to decide how to use the comment function. If it is not possible to moderate comments an option to deactivate the comment function must be made available on major social media websites.
- European and internationally coordinated measures are needed. The internet is not a national space, and so national solutions can be effective only up to a point. The EU Code of Conduct on Hate Speech can provide inspiration. But points of criticism and lessons learned should also be taken up, among other things in relation to companies’ voluntary commitments because, for example, some companies and platforms do not participate and thus are not evaluated.
- International best practices on tackling hate crime and other illegal content should be exchanged in the context of ongoing collaborations. Shared best practices and recommendations need to be discussed and evaluated on a regular basis to be able to develop binding commitments from them.
- User data protection must be central to all proposed measures and demands. Civil society will remain on board only if sensitivity is exercised in relation to civil liberties and data protection.