ARTICLE 19 recommendations for the Digital Services Act Trilogue

The Digital Services Act (DSA) presents an important opportunity to open up 'Big Tech' to scrutiny and to protect human rights online. As the negotiations of the DSA reach their final stage in the trilogue, we urge the European Parliament and Member States in the EU Council to do their utmost to ensure that the DSA keeps its promise to increase safety online, improve transparency and accountability of online platforms all while fully respecting fundamental rights.

Since the first proposal was published, ARTICLE 19 has argued that the DSA must have the protection of freedom of expression at its core. While the draft DSA does contain a number of safeguards for the protection of freedom of expression and privacy, we have throughout the legislative process repeatedly raised that some of its aspects are disquieting and should be brought in line with international human rights and free speech standards (see for example our recommendations on regulating recommender systems, due diligence obligations for online platforms or the new proposed notice and action mechanism).

ARTICLE 19 recommends in particular:

1. **To protect users' rights to privacy and anonymity online and refrain from imposing general monitoring obligations**

Encryption and anonymity are key to protecting users' right to privacy and to ensuring that they feel confident to express themselves freely in their online communication. If users are unable to communicate privately this will substantially affect their right to freedom of expression. States should therefore refrain from restricting encrypted and anonymous services by intermediary service providers and from requiring such providers to analyse individuals' communication and online activity via a general monitoring obligation. Apart from interfering with users' privacy rights, a general monitoring obligation would likely lead to companies detecting and removing vast amounts of legitimate content, as content-monitoring technologies such as hash-matching algorithms and natural language processing tools are currently not advanced enough to distinguish legal from illegal content in a reliable manner.

For these reasons, we support:

> Article 7 EP
>
> No general monitoring or active fact-finding obligations
>
> 1. No general obligation to monitor, neither de jure, nor de facto, through automated or non-automated means, the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity or for monitoring the behaviour of natural persons shall be imposed on those providers.
> 1a. Providers of intermediary services shall not be obliged to use automated tools for content moderation or for monitoring the behaviour of natural persons.
> 1b. Member States shall not prevent providers of intermediary services from offering end-to-end encrypted services.
> 1c. Member States shall not impose a general obligation on providers of intermediary services to limit the anonymous use of their services. Member States shall not oblige

providers of intermediary services to generally and indiscriminately retain personal data of the recipients of their services. Any targeted retention of a specific recipient's data shall be ordered by a judicial authority in accordance with Union or national law.
1d. Without prejudice to Regulation (EU) 2016/679 and Directive 2002/58/EC, providers shall make reasonable efforts to enable the use of and payment for that service without collecting personal data of the recipient.

2. To avoid over-removal of content

The DSA must not create a mechanism that incentivises companies to over-remove content to shield themselves from liability. Maintaining conditional immunity from liability for hosting content in the draft DSA will go a long way in achieving this goal. At the same time, the principle of conditional liability must be accompanied by a solid provision for the notice and action mechanisms. This is because providers may lose their immunity if they fail to expeditiously remove or disable access to the illegal content following a notice of illegality. It is therefore of critical importance that users' content that has been the subject of a notice of illegality remains accessible pending assessment of its legality (and that immunity of providers remain intact during that time).

Removing content before such an assessment is even carried out would undoubtedly lead to a significant amount of completely legitimate content being taken down, opening up the door for abuse of the notice and action mechanism. This would not only be in contravention of due process principles but it would also risk the curtailment of freedom of expression.

For these reasons, we support:

Article 14(3) EP

3. Notices that include the elements referred to in paragraph 2, on the basis of which a diligent hosting service provider is able to establish the illegality of the content in question without conducting a legal or factual examination, shall be considered to give rise to actual knowledge or awareness for the purposes of Article 5 in respect of the specific item of information concerned.

Article 14(3a) (new) EP

3a. Information that has been the subject of a notice shall remain accessible while the assessment of its legality is still pending, without prejudice to the right of providers of hosting services to apply their terms and conditions. Providers of hosting services shall not be held liable for failure to remove notified information, while the assessment of legality is still pending.

3. To bring due diligence obligations and risk mitigation measures in compliance with human rights standards

The draft DSA requires Very Large Online Platforms (VLOPs) to carry out risk assessments concerning a number of aspects, namely the dissemination of illegal content, any negative effects on fundamental rights and the intentional manipulation of their service by automated means with a foreseeable negative effect on public health, public safety, civic discourse and electoral processes. ARTICLE 19 endorses in principle the adoption of due diligence obligations by VLOPs to ensure that potential risks to users' human rights are properly identified and addressed. At the same time, ARTICLE 19 has highlighted that the identification of systemic risks and the adoption of appropriate measures need to meet the legality test under international human rights law. Users or third parties must be able to foresee how their freedom of speech rights might be restricted to counter systemic risks. This requires clear

rules governing the identification of systemic risks and clear limits as to which measures are acceptable and which are off-limits. As ARTICLE 19 has highlighted before, the vague terminology around what could constitute a systemic risk remains a source of concern. At the very least, the DSA should contain strong transparency requirements regarding the methods applied in carrying out risk assessments and determining the measures to adopt. This should be coupled with the involvement of human rights organisations at all stages of this process.

For these reasons, we support:

Article 26(2a) (new) EP

2a. When conducting risk assessments, very large online platforms shall consult, where appropriate, representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations. Their involvement shall be tailored to the specific systemic risks that the very large online platforms aim to assess.

Article 26(2b) (new) EP

2b. The supporting documents of the risk assessment shall be communicated to the Digital Services Coordinator of establishment and to the Commission.

Article 26(2c) (new) EP

2c. The obligations referred to in paragraphs 1 and 2 shall by no means lead to a general monitoring obligation.

Article 27(1) EP

1. Very large online platforms shall put in place, reasonable, transparent, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26. Such measures may include, where applicable:

Article 27(1a) (new) EP

1a. Very large online platforms shall, where appropriate, design their risk mitigation measures with the involvement of representatives of the recipients of the service, independent experts and civil society organisations. Where no such involvement is foreseen, this shall be made clear in the transparency report referred to in Article 33.

Article 27(1b) (new) EP

1b. Very large online platforms shall provide a detailed list of the risk mitigation measures taken and their justification to the independent auditors in order to prepare the audit report referred to in Article 28.

Article 27(1c) (new) EP

1c. The Commission shall evaluate the implementation and effectiveness of mitigation measures undertaken by very large online platforms referred to in Article 27(1) and where necessary may issue recommendations.

Article 31(2) EP

2. Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers, vetted not-for-profit bodies,

organisations or associations, who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification, mitigation and understanding of systemic risks as set out in Article 26(1) and Article 27(1).

Article 31(2a) EP

2a. Vetted researchers, vetted not-for-profit bodies, organisations and associations shall have access to aggregate numbers for the total views and view rate of content prior to a removal on the basis of orders issued in accordance with Article 8 or content moderation engaged in at the provider's own initiative and under its terms and conditions.

ARTICLE 19 is concerned that the European Parliament proposal is expanding the catalogue of potential systemic risks that can justify risk mitigation measures by the dissemination of "content that is in breach with [VLOPs'] terms and conditions". This would allow companies to take measures based on terms and conditions which can be subjected to change at any point and which may go well beyond the legitimate aims foreseen in international human rights law.

For these reasons, we reject:

Article 26(1)(a) EP

(a) the dissemination of illegal content through their services or content that is in breach with their terms and conditions.

4. To provide users with effective remedy mechanisms

Procedural safeguards are an essential component of protecting users' free speech online. For example, ARTICLE 19 believes that individuals should not only have access to internal complaint-handling and redress mechanisms but also to judicial remedies. Users should be able to challenge any decision by service providers that affects users' rights, for example, the removal of content or suspension of the service, before independent courts or tribunals.

For these reasons, we support:

Article 9a (new) EP

Effective remedies for recipients of the service

1. Recipients of the service whose content was removed according to Article 8 or whose information was sought according to Article 9 shall have the right to effective remedies against such orders, including, where applicable, restauration of content where such content has been in compliance with the terms and conditions, but has been erroneously considered as illegal by the service provider, without prejudice to remedies available under Directive (EU) 2016/680 and Regulation (EU) 2016/679.
2. Such right to an effective remedy shall be exercised before a judicial authority in the issuing Member State in accordance with national law and shall include the possibility to challenge the legality of the measure, including its necessity and proportionality.
3. Digital Services Coordinators shall develop national tools and guidance to recipients of the service as regards complaint and redress mechanisms applicable in their respective territory.

Article 17(5a) (new) EP

5a. Recipients of the service shall have the possibility to seek swift judicial redress in accordance with the laws of the Member States concerned.