

# Due diligence obligations in the EU's Digital Services Act

ARTICLE 19's recommendations to lawmakers  
21 May 2021

**ARTICLE 19** has serious concerns about the proposals contained in Articles 26 and 27 of the proposed EU Digital Services Act (DSA), which set out due diligence obligations for online platforms. Due diligence obligations could be used to ensure that potential risks to users' human rights, including the right to freedom of expression, are identified and addressed. However, the current proposals are vague and fail to set strong enough rights protections. The European Parliament should seek to urgently clarify the provisions, as well as mandating human rights impacts assessments and greater transparency from companies to enable the better protection of human rights online.

## The proposed provisions

Proposed Article 26 of the draft Digital Services Act would require Very Large Online Platforms (VLOPs) to carry out risk assessments at least once a year in relation to the functioning and use of their services. In particular, they would be required to identify systemic risks related to the dissemination of illegal content, any negative effects for the exercise of certain fundamental rights, and the intentional manipulation of their service. Under Article 27, VLOPs are then required to take 'reasonable, proportionate and effective measures' to mitigate the risks identified under the supervision of the European Commission in cooperation with the European Board for Digital Services and the Digital Services Coordinators.

Article 26 and 27 do not prescribe the particular measures that VLOPs ought to take in response to the identification of systemic risks. It is also unclear what constitutes a sufficient systemic risk for the purpose of any risk mitigation. The definition of these terms and their implementation would be left to the discretion of the platforms under the supervision and following the guidelines of prospective regulators, including the European Commission. Platforms would also be expected to comply with Codes of Conduct addressing specific systemic risks or particular types of content. The adoption of the Codes would be facilitated by the Commission and the Digital Services Board.

## What is the problem for freedom of expression?

In our view, these provisions are deeply problematic for several reasons:

### Vagueness and lack of legal certainty

In our view, Articles 26 and 27 are too vague and fail to meet the legality test under international human rights law, i.e. they are insufficiently precise to enable platforms, users and others to foresee how any risks to human rights or otherwise will be addressed.

Article 26 provides that VLOPs should assess, among others, systemic risks related to the dissemination of illegal content and "any negative effects" for the exercise of a number of fundamental

rights. Over the years, however, our experience is that governments and the Commission in particular have had a very different understanding of how to address the dissemination of illegal content whilst protecting fundamental rights. In particular, national governments tend to promote the use of upload filters and general monitoring in order to detect and prevent illegal content from even being uploaded in the first place, despite the fact that it would seriously infringe both the rights to privacy and freedom of expression. Some governments have sought to mandate the removal of manifestly illegal content within 24 hours or in the case of allegedly terrorist content, 1 hour. The weakening of encryption is also a regular demand of law enforcement agencies in order to deal with child sex abuse images despite the fact that it would create unacceptable and disproportionate risks to the information security of all users.

Article 26 and 27 do not make reference to these types of measures but they give incredibly broad discretionary powers to the Commission and regulators to define in guidelines and Codes of Conduct what companies ought to do to address these ill-defined risks. The above measures therefore remain a possibility.

### Insufficient protection of fundamental rights

Our concerns about the lack of clarity of the types of measures that companies ought to adopt to address 'systemic risks' are compounded by weak references to the protection of fundamental rights. Article 26(1)(b) only requires companies to assess "negative effects" on fundamental rights, not whether those rights would be violated. Meanwhile, Article 27 on mitigation measures only makes reference to 'reasonable' rather than 'necessary' measures to address those risks and protect human rights. The DSA is also lacking provisions that would enable human rights groups to actively raise concerns with Digital Service Coordinators, the Board or the Commission about human rights infringements once Codes of Conduct are adopted and mitigation measures implemented.

### Other concerns

Article 26 also makes reference to the 'intentional manipulation' of platforms' services. To its credit, the Commission has been reluctant to regulate disinformation directly due to its inherent political nature and the chilling effect it would inevitably have on freedom of expression. This is laudable but we are concerned that 'manipulation' is a very vague term. Intent is also difficult to establish purely from online activity. Campaign groups may well use bots to promote their causes online, for example. Moreover, companies would be required to take measures in relation to behaviour that would have a mere "foreseeable negative effect" on a broad range of issues or stakeholders that go well beyond the legitimate aims foreseen in international human rights law. For instance, the use of language that is offensive to some would have a 'foreseeable negative effect' on civic discourse. In practice, we are concerned that platforms would be under pressure to demote 'borderline' content, i.e. that is neither illegal nor in breach of their terms of service, with the result that debate on controversial topics would all but disappear (for recent examples, see here and here).

### Recommendations for due diligence obligations that protect human rights

For the reasons outlined above, Articles 26 and 27 should be urgently re-thought and clarified. If these provisions are maintained, they should at least make clear that certain measures to address these risks are never acceptable, such as the weakening of end-to-end encryption or general monitoring obligations.

**Contact:** For more information on the contents of this briefing, please contact: Gabrielle Guillemin, Senior Legal Officer at ARTICLE 19, at [gabrielle@article19.org](mailto:gabrielle@article19.org)

They should also ensure real democratic accountability, for example through the approval of annual reports by the European Parliament. Measures that significantly interfere with fundamental rights should be adopted through democratic procedures, not through Codes of Conduct.

In addition, safeguards for the protection of human rights should be strengthened throughout the DSA. In particular, provision should be made for mandatory human rights impact assessments and procedures that would enable human rights groups to raise concerns or bring complaints against due diligence measures that unduly interfere with freedom of expression and other fundamental rights, such as the use of recommender systems or filters that effectively prevent debate on controversial issues. This should be coupled with strong transparency requirements about the measures adopted by companies in order to address human rights concerns. The Commission, the Board and national Digital Services Coordinators should also have an express duty to protect freedom of expression and other fundamental rights in the implementation of the DSA.