



EU: Will the Digital Services Act succeed in holding Big Tech accountable?

On 5 July 2022, the European Parliament approved the Digital Services Act (DSA) by plenary vote. Together with its sister proposal, the Digital Markets Act (DMA), the DSA is set to have major implications for freedom of expression. Since the DSA proposal was first discussed, ARTICLE 19 has argued that, to be a success, the protection of human rights and in particular free speech online must be at its core. How does the DSA fare against its promise to open up 'Big Tech' to scrutiny and to safeguard users' rights online?

The DSA replaces the current EU framework for digital services, the E-Commerce Directive, and seeks to harmonise the rules applicable to the provision of digital services across the EU. It also consolidates various separate pieces of EU legislation and self-regulatory practices that address online illegal or 'harmful' content. The DSA however goes further than that. It is an attempt to reflect new technological realities and to make 'Big Tech' accountable through new transparency and due diligence obligations.

Where does the DSA adopt the right approach?

One of the main positive aspects of the DSA is that it will not prescribe what type of content needs to be restricted or removed (unlike other legislative proposals currently considered, namely the [UK Online Safety Bill](#)). Instead, it focuses on processes and transparency. ARTICLE 19 believes that thanks to this, many of its provisions will open up online platforms to scrutiny and significantly improve the protection of human rights online:

- Unlike the E-Commerce Directive and other previous EU legislation or initiatives impacting freedom of expression (such as the 2016 [EU Code on Countering Illegal Hate Speech](#), the [2019 Copyright Directive](#) or more recently the [2021 Terrorist Content Online Regulation](#)), the DSA lists **the protection of fundamental rights as one of its main objectives** (Article 1). The relevant fundamental rights are concretised in different obligations for service providers and corresponding rights for users (for instance when granting due process rights to the latter). At times, the DSA also requires service providers to take fundamental rights as such into account (for instance in its due diligence obligations).
- Importantly, the **DSA retains conditional immunity from liability for hosting providers** (Article 5), the cornerstones of freedom of expression enshrined in the E-Commerce Directive - albeit this is somewhat undermined by the DSA's flawed notice-and-action mechanism discussed below. The DSA also maintains the prohibition of general monitoring or active fact-finding obligations (Article 7). Given that in recent years the political discourse has been shifting towards requiring online platforms to take on a more active role in tackling illegal or 'harmful' content they host, this was by no means a foregone conclusion.
- The DSA **puts a very strong emphasis on transparency**. Indeed, the transparency obligations on intermediary services are wide-ranging and include:
 - The terms and conditions will have to transparently set out information with regards to

any restrictions imposed on the use of the service, including any policies, procedures, measures and tools used for the purpose of content moderation, including algorithmic decision-making and human review (Article 12).

- Providers of intermediary services will further have to publish reports at least once a year on any content moderation they engaged in. This includes information about orders received from national authorities; content moderation engaged at their own initiative; the number of complaints received through the internal complaint-handling systems; any use made of automated means for the purpose of content moderation; the number of notices received under the notice-and-action procedure (only for hosting providers); information about disputes filed with the out-of-court dispute settlement bodies; and suspension measures taken in response to the posting of manifestly illegal content, manifestly unfounded notices and the submission of manifestly unfounded complaints (only for online platforms, see Articles 13 and 23).
- Those platforms that display advertising must ensure that the recipient of the service can identify clearly that the information displayed is an advertisement as well as the natural or legal person behind it. Users must also be given meaningful information about the main parameters used to determine the recipient of such advertisements and about how those parameters can be changed (Article 24). Very large online platforms (VLOPs) are also subject to additional transparency online advertising requirements, including the creation of publicly available repositories for the ads they display (Article 30).
- The DSA will further allow users to be better informed about how content is recommended to them. The platforms will have to set out the main parameters used in their recommender systems - fully or partially automated systems used by platforms to determine what content to promote or demote to different users – in their terms and conditions (Article 24a).
- VLOPs are further subject to certain transparency requirements with regards to their due diligence obligations. Specifically, they will have to publish their assessments in relation to systemic risks on their platforms, the related mitigation measures they have adopted in response, the independent audit report on those as well as an audit implementation report (Articles 26 to 28).
- The DSA further provides that VLOPs need to provide access to data to regulators and vetted academic researchers to audit algorithmic operations and effects (Article 31).
- The **DSA significantly improves users' procedural rights**. As we highlighted in our [Missing Voices campaign](#), it is essential that users have their freedom of expression protected through the ability to appeal content decisions, and have their posts and accounts reinstated when the process concludes in their favour. We, therefore, welcome that the DSA requires all hosting providers to provide a statement of reasons for any restriction imposed on a user's content or accounts (Article 15) and to put in place an internal complaint-handling system mechanism (Article 17). In addition, the DSA provides for user redress through an out-of-court dispute settlement (Article 18) and establishes rules on the lodging of complaints to supervisory authorities (Article 43) as well as on representative actions (Article 68).
- Finally, the DSA recognises to a certain extent that it will be key that **civil society and independent experts be in a position to scrutinise service providers' compliance with the DSA**. For example, the DSA recommends that VLOPs consult with civil society and independent experts when conducting their risk assessments and design their risk

mitigation measures (Recital 59; the due diligence obligations required under Article 26 and 27 are discussed further below). It also states that the Commission may involve civil society and independent experts for their involvement in the drawing up of Codes of Conduct as well as the drawing up of crisis protocols for addressing public security or public health crises (Articles 35 to 37). Furthermore, civil society organisations may qualify as vetted researchers given access to data for the purposes of conducting research with respect to the due diligence obligations established in the DSA as long as they are “conducting scientific research with the primary goal of supporting their public interest mission”. Finally, the DSA also permits civil society organisations to defend users’ rights by permitting them to lodge representative actions against providers of intermediary services (Article 68). While ARTICLE 19 would have liked to see more mandatory civil society involvement, the way that civil society actors are taken into account by the DSA undoubtedly constitutes a step in the right direction.

Where does the DSA fall short?

At the same time, ARTICLE 19 is disappointed that the DSA does not bring the systemic change required to ensure the protection of human rights and users’ choice online. There is in fact a real concern that the DSA could help to further consolidate the dominance of the biggest online platforms as it fails to sufficiently curb their market power or set limits on their business model based on the massive exploitation of users’ personal data:

- The DSA **fails to decentralize content curation** and open the market to alternative players. [ARTICLE 19 had advocated](#) that Article 29 of the DSA should require VLOPs to unbundle hosting from content curation, and to allow third parties to provide alternative recommendation systems on their platform. Given that recommendation algorithms often promote extreme and controversial speech at the expense of more moderate voices, this was a missed opportunity to limit such practices and foster real exposure diversity and better choices for users.
- We are further disappointed by the **lack of ambition to limit the business model of platforms based on behavioural advertising**. While we welcome that the DSA takes some first important steps to tackle surveillance-based advertising – it introduces a limited ban on deceptive interface designs, prohibits platforms to serve behaviourally targeted ads for minors (Article 24(b)) and it establishes a limited ban on the use of sensitive personal data for targeted advertising – some important weaknesses remain. Indeed, only some of the platforms’ manipulative practices will be covered by the DSA (for instance, it only applies to online platforms, not all intermediary services) and the ban on the use of sensitive personal data only applies to platforms showing ads to their own users.

In addition, the DSA **falls short of protecting freedom of expression** in the following ways:

- The notice-and-takedown mechanism for allegedly illegal content (Article 14) will likely **lead to over-removal of legal content**. This is because the notice-and-takedown mechanism is linked to the concept of conditional immunity from liability for hosting providers under Article 5. Providers may lose their immunity if they fail to expeditiously remove or disable access to the illegal content following a notice of illegality. This mechanism effectively outsources the decision of whether users’ speech is legal or not to private companies. This is deeply problematic as only independent judicial authorities should be given the power to make such a determination. In addition to the legitimacy concerns of outsourcing decisions on the legality of users’ speech to private actors, we note that in the majority of cases, these assessments are extremely complex and context-dependant and should therefore be made by trained individuals. The DSA could have been

far more protective of freedom of expression if instead it adopted a notice-to-notice mechanism for private disputes and required service providers to notify law enforcement agencies of allegations of serious criminality, [as recommended by ARTICLE 19](#). At the very minimum, the DSA should have required that users' content remain accessible pending assessment of its legality by the platforms.

- We also consider that the **due diligence obligations for VLOPs** (Articles 26 and 27) remain flawed. The due diligence obligations require VLOPs to assess systemic risks stemming from their services in relation to issues such as the dissemination of illegal content; the protection of fundamental rights; and the protection of public health. Based on those risk assessments, VLOPs are required to adopt wide-ranging mitigation measures, which will implicate users' freedom of expression rights. This is not to say that the due diligence obligations do not contain positive aspects, such as the requirement to assess negative effects on human rights and the freedom and pluralism of the media. We are also pleased that the final text offers a significant improvement to the initial Commission proposal and is in line with some of [ARTICLE 19's recommendations](#). However, some of the terminology remains too vague to be human-rights compliant and it is problematic that the DSA leaves a large amount of discretion to companies (and ultimately the Commission) to decide how the systemic risks identified should be mitigated. Furthermore, like the notice-and-action mechanism, the due diligence obligations provide an incentive for companies to over-remove protected content, as they emphasise the need for "expeditious removal of or disabling access to the [illegal] content notified". The DSA further fails to provide any guidance on how to balance any potential conflict between the requirement to swiftly remove allegedly illegal content with the protection of fundamental rights.
- We are further disappointed that the DSA contains **no explicit right for users to encryption and anonymity**. Both are key to protecting users' right to privacy and ensuring that they feel confident to express themselves freely in their online communication. Given that the political discourse is shifting more and more towards curbing encryption and anonymity (and [current legislative proposals](#) could make government scanning of users' content and metadata mandatory throughout the EU), it would have been all the more important that these rights be enshrined in the DSA.
- **The crisis response mechanism** (Article 27a) that was introduced at the last minute and as part of the closed-door Trilogue negotiations is alarming. While the final text contains some additional safeguards after [strong pushback by ARTICLE 19 and other civil society organisations](#) (for example, a sunset clause of three months was added and the Commission will now have to act only upon recommendation of the Board representing national regulators), the DSA still gives the European Commission too much power to control freedom of expression on large online platforms when it decides that a crisis has occurred. Freedom of expression becomes more, not less, important in times of crisis.

Way forward

The DSA presented a unique opportunity to find a regulatory response to some of the most pressing challenges in the digital space including the market dominance of a number of tech companies, the power they wield over individuals and the wider effect this has on freedom of expression and democracy itself. While we believe that EU legislators could have been more ambitious in many ways, the DSA does bring some improvements. Whether those improvements will be meaningful will largely depend on the approach taken by the EU and Member States regulators at the enforcement stage. It is therefore essential that civil society and independent experts are closely involved in this process going forward.

The DSA may well set the global standard for regulating online content. ARTICLE 19 will continue to monitor how it will influence legislators around the world and work to ensure that freedom of expression remains at the centre of any internet regulation.