The New European Digital Services Act: Risky for Consumers and Innovation

Mikołaj Barczentewicz, Senior Lecturer in Law and Research Director of the Law and Technology Hub, University of Surrey

The EU Commission proposed the new Digital Services Act (DSA) and Digital Markets Act (DMA) in December 2020. Collectively, these proposals are an important opportunity to protect the competitiveness and integrity of the European internal market as well as to uphold the EU Charter of Fundamental Rights, which are threatened by the growing complexity of special EU and national laws applicable to digital services.

Like other recent EU and national measures, the DSA aims to promote online 'safety' and 'governance'. However, the proposal does not provide sufficient legal certainty to businesses and consumers and exacerbates existing risks to fundamental rights and innovation. Additional evidence is required to highlight that the risks which the DMA and the DSA currently pose to the rights enshrined in the EU Charter are proportionate.

Overview

The European Commission published its proposal for the new Digital Services Act (DSA) in December 2020. The proposal shares some of the beneficial features associated with the current regulatory framework for digital services and contains some valuable ideas such as upholding the country-of-origin principle in online regulation. However, it also introduces significant new risks to innovation and competitiveness in Europe and to the rights and freedoms enjoyed by Europeans. In response to the Commission's proposal, a draft report written by Christel Schaldemose (S&D), rapporteur of the European Parliament's Internal Market and Consumer Protection Committee (IMCO), has been published. The amendments proposed by Schaldemose would make the DSA even less friendly to innovation and present a greater risk for the fundamental freedoms of Europeans.

The European Commission must provide more evidence, in addition to that which was presented in the DSA impact assessment, in order to assert that the key aspects of the proposed regulation are worthwhile, not to mention ensuring that the risks they pose to the rights enshrined in the EU Charter are proportionate. A seemingly common belief that 'something must be done' about the unsavory practices that can occur online cannot be a license to regulate without a solid evidential basis. The European legislature should remember that just because some problems exist, it does not mean that they can be proportionately addressed through the law (see e.g. Chomanski 2021).

The DSA as an important opportunity

Online services have created unprecedented opportunities for Europeans to communicate, to form communities, and to trade. This would not have been possible without two legal pillars:

- The prohibition on general monitoring obligations (Article 15 of the e-Commerce Directive - ECD), which means that Member States cannot require online service providers to monitor (snoop on) all the content that they have access to;
- The conditional liability shield (Article 14 ECD), which protects service providers from legal liability for user-provided content if they take down illegal content once they learn about the illegality.

Those principles have never been unqualified, but they are now under a particularly strong threat, both from the EU legislature and from Member States. Much of this barrage is constituted by well-intentioned, if not always well-considered, attempts to curb the harmful content that can be found online like terrorist content or copyright infringements.

In this context, the DSA is an important opportunity to protect and improve the regulatory framework which facilitates many of the undeniable benefits that Europeans enjoy online today. The DSA could achieve this in two ways:

- By constituting a uniform code which would replace conflicting EU rules and preclude national laws undermining the integrity of the internal market in digital services or
- By harnessing regulatory competition through strong country-of-origin rules, precluding other Member States from imposing stricter regulations on an online service provider than the rules of the Member State where the provider is established or has a legal representative.

Some of the key provisions of the DSA fall significantly short of achieving either of these goals (see Cauffmann & Goanta 2021). The DSA does not provide a uniform code, e.g. on takedown mechanisms or on liability for content. It retains other EU rules, for example those in the Terrorist Content Regulation and in the Copyright Directive. Despite the general endorsement of the country-of-origin principle in Article 40, the DSA does not give sufficient effect to the principle. For example, it allows for extra-territorial 'orders to act against illegal content,' even those issued by administrative bodies and not by the courts.

Instead of using the opportunity to simplify the rules applicable to digital service providers and promote innovation in Europe, the DSA maintains the increasingly byzantine framework of laws. Start-ups and smaller enterprises risk being regulated 'to death' by the alphabet soup of EU and national regulations. Even without changing the substance of the already existing rules, e.g on takedown mechanisms, the DSA could have provided the benefit of a 'one-stop shop' which would significantly reduce complexity and compliance costs. In addition, an attempt to create uniform rules in the form of one single regulation would have forced the EU legislature to address the difficult tradeoffs and complexities that digital service providers are faced with.

Risks to innovation

The DSA not only fails to alleviate the compliance costs stemming from various laws applicable to digital service providers, but adds new burdens which raise the question of proportionality of restrictions on the freedom to conduct a business under the Article 16 of the EU Charter.[1]

Potentially extremely costly out-of-court dispute settlement

The DSA proposes a new 'out-of-court dispute settlement' mechanism (Article 18) for users of online platforms. The fees for such dispute settlement would be covered by online platforms if they lose and the platforms will not be able to recover their own costs, even if they win. In its DSA Impact Assessment, the European Commission did not even attempt to calculate the burdens this might impose, especially on medium-sized enterprises. Even good faith disputes could escalate to the point of becoming an unsustainable burden for anyone other than the largest players.

The original DSA proposal excluded small and micro enterprises from this mechanism, but it still means that any company with a turnover above €50 million or balance sheet above €43 million would be caught out. Many online platforms, especially startups, operate with very small or negative profit margins. Hence, a startup with a turnover of €50 million, but low or no profits and low reserves, could be bankrupted by having to incur the high costs of dispute settlements. This could occur even if the startup wins disputes.

However, the amendments suggested by IMCO rapporteur MEP Schaldemose, are much worse. She suggests removing the exemption for small and micro enterprises from the provisions of Section 3 DSA, including the article on dispute settlements. Schaldemose's proposals do not provide for an impact assessment of any kind despite the potential for significant consequences for small and medium-sized businesses across Europe.

Disproportionate transparency obligations

The DSA contains a number of information and transparency obligations on digital service providers, some of which would not apply to small and medium-sized enterprises. Given that some of the obligations, like the Article 13 duty to report on content moderation practices, are meant to apply to all 'intermediaries', it is unclear who will benefit from the vast majority of those reports. The obligation to provide reports may be difficult to justify if the obligation is not proportionate and requires the heavy investment of intermediaries in new systems and staff. Similarly, it cannot be assumed that providing consumers with additional information about advertising (Article 24) will bring a proportionate benefit to consumers, especially given that there is evidence to the contrary (Dobber et al, 2021).

Although transparency may be 'nice to have', it does not ensure that reporting will be proportionate in all contexts. Neither the DSA, nor the associated documents published by the European Commission, address this issue. In respect of 'orders to act against illegal content' issued by state authorities, the authorities themselves should provide the relevant reports. As there are more intermediaries than authorities, it is hardly proportionate to impose significant burdens on private enterprises to report on what a Member State is doing.

The second problem with information and transparency obligations is that if providers are required to disclose too much about their moderation and security practices, they will be in effect providing guidelines to bad actors (terrorism promoters, spammers and other criminals) on how to evade the safeguards. It is desirable for providers to provide a certain level of clarity to users on what content may be removed, but this needs to be weighed against the risks.

One way in which this risk may be managed is through non-public privileged access to information for vetted researchers and for authorities (Articles 31 and 57). Access for researchers and for authorities comes with serious risks to privacy, data protection and to commercial secrets (see Amnesty International 2021, p.14; DOT Europe 2021, p.26). It is almost impossible for academic researchers to 'preserve the specific data security and confidentiality requirements' (Article 31(4)) if they are given access to internal databases of large online platforms and it is unlikely that the national authorities would be able to do so (under Article 57).

[1] Algrove, B., 'The EU's Digital Services Act: are we still free to conduct business?', *EU Law Live*, 31 May 2021 (https://eulawlive.com/op-ed-the-eus-digital-services-act-are-we-still-free-to-conduct-business-by-ben-allgrove/).

The preparation and sharing of 'proxy databases' with researchers may provide a partial solution. However, such 'proxy databases' will need to be sanitized, for example in relation to personal and sensitive data, and may prove to be costly and difficult for all platforms. In spite of such measures, given the sensitivity of the data - in part, because it can be used to circumvent the moderation and security safeguards of online platforms - there should be a proportionate vetting process for anyone who may have access to the data, including those individuals with administrative access to systems or networks from which the data may be extracted. The criteria provided in Article 31(4) are far from addressing the seriousness of the issue.

Regulatory oversight which does not guarantee independence

Finally, the governance structure which will be created by the DSA, including the new 'European Board for Digital Services' (Section 2 DSA), does not ensure that the interests of consumers and innovation will be adequately protected. The Board will consist of the European Commission, a political organ, and of nominally independent national Digital Services Coordinators, many of whom will likely be actively 'supervised' (under Article 39(3)) by their national governments. Hence, it is realistic to expect that the Board will be swayed by political considerations or by precautionary concerns stemming from 'moral panics' more than by robust evidence.

Risks to privacy and safety of personal data

Potential threat to encryption

The DSA contains many vague provisions which will be specified at a later date without robust legislative scrutiny through the European Commission's delegated legislation, quasi-voluntary Codes of Conduct, enforcement actions by administrative bodies and case law. There is a real risk that some of these measures will attempt to use the DSA to undermine the most significant practical protection of privacy and safety of personal data of Europeans: end-to-end encryption. This risk could be reduced by a clear rule providing that the DSA cannot be used to undermine encryption (see e.g. Keller 2021, p.14).

Some of the information and transparency measures discussed earlier also pose risks to privacy and safety of personal data.

Risks to freedom of speech and freedom of association

The DSA will promote over-removal of user content by digital services, due to alleged illegality of content and due to alleged violations of a provider's terms of service. This is a grave threat to freedom of expression (Article 11 EU Charter) and freedom of association (Article 12 EU Charter) exercised by users of online services.

Difficulty with attempting to force online platforms to carry speech

Most of the service providers are private businesses and it would be problematic to force them to publish content, in part because it would be a restriction of their constitutionally protected freedom to conduct a business (Article 16 EU Charter). Moreover, the vast majority of unwanted content that providers remove is spam and any protections against content removal will make fighting spam more difficult.

However, the law should also be very careful not to incentivise providers to over-remove content. Unfortunately, the DSA will have that effect.

Extra-territorial takedown orders by administrative authorities

The DSA will require providers to obey 'orders to act against illegal content' (Article 8) issued by national authorities. Instead of accepting the sound principles that determinations of what constitutes illegal content can only be decided by the courts and only have effect within the boundaries of the domestic jurisdiction, the DSA allows Member States to designate 'administrative authorities' with powers to issue such orders. In addition, the DSA allows for orders to have extra-territorial scope. This practically guarantees that national administrative agencies will apply their restrictive national rules on speech and demand removal of content in other EU Member States, even if such demands are unconstitutional in some other countries. Such demands may violate the safeguards provided by the DSA (Article 6(2)(a) and (b) and recital 31), but the very considerable burden of resisting an unlawful, but perhaps not manifestly unlawful, order will be entirely on the providers and they will often simply acquiesce.

Anyone's complaint would constitute 'actual knowledge or awareness' of illegality

The DSA also provides for a 'notice and action' mechanism (Article 14). This mechanism encompasses a fundamental flaw whereby a notice of illegality, issued by anyone, 'shall be considered to give rise to actual knowledge or awareness' (Article 14(3)) with the consequence that the provider will no longer benefit from the liability shield (Article 5). At scale, it will be impossible for providers to assess whether the notices that purport to provide all the information required by the DSA have merit. This will provide very strong incentives for providers to simply remove any notified content and none of the safeguards provided in the DSA will have much effect in preventing this (see e.g. Mchangama, 2021).

Rules too vague given risks to Charter freedoms

It is also very worrying that many of the details of the new regulatory framework are left to be determined at a later date outside of the legislative process, for example through 'Codes of Conduct' (Articles 35-36). Given that those details can lead to very significant restrictions of rights protected by the EU Charter, especially if the 'voluntary' but publicly-facilitated rules become de facto speech codes for all EU citizens due to their relevance to legal sanctions (recital 68), this strategy could fail to meet the standard of clarity and foreseeability under Article 52(1) EU Charter (see Wilman 2021, p.225).

References

Amnesty International (2021) 'Amnesty International Position on the Proposal for a Digital Services Act and a Digital Markets Act' (https://www.amnesty.eu/news/amnesty-international-position-on-the-proposals-for-a-digital-services-act-and-a-digital-markets-act/).

Cauffman, C. & Goanta, C. (2021) 'A New Order: The Digital Services Act and Consumer Protection'. *European Journal of Risk Regulation* (https://doi.org/10.1017/err.2021.8).

Chomanski, B. (2021) 'The Missing Ingredient in the Case for Regulating Big Tech'. *Minds and Machines* (https://doi.org/10.1007/s11023-021-09562-x).

Dobber, T., Kruikemeier, S., Goodman, E., Helberger, N., & Minihold, S. (2021) 'Effectiveness of Online Political Ad Disclosure Labels: Empirical Findings'. University of Amsterdam ICDS. (https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-discloures-experiment_update.pdf).

DOT Europe (2021) 'A Single Market for Digital Services: DOT Europe Questions and Recommendations on the DSA' (https://doteurope.eu/wp-content/uploads/2021/04/DOT-Europe-DSA-Questions-and-Recommendations-Chapters-1-3-.pdf).

Mchangama, J., Alkiviadou N. & Mendiratta R. (2021) 'Rushing to Judgment: Are Short Mandatory Takedown Limits for Online Hate Speech Compatible with The Freedom of Expression?'. Copenhagen: Justitia (https://globalfreedomofexpression.columbia.edu/publications/rushing-to-judgment-are-short-mandatory-takedown-limits-for-online-hate-speech-compatible-with-the-freedom-of-expression/).

Keller, D. (2021) 'Topic 3 of the DSA: The US perspective'. In *The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective: Background Paper*. European Parliament: IMCO (https://www.europarl.europa.eu/cmsdata/234761/21-05-19%20Background%20note%20REV%20final.pdf)

Wilman, F. (2021) *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US*. Cheltenham: Elgar.