Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

DIGITAL SERVICES ACT
PART III: OVERSIGHT AND ENFORCEMENT

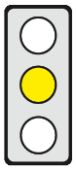
cep**PolicyBrief** No. 24/2021

KEY ISSUES

Background: Digital services acting as intermediaries, i.e. connecting users with suppliers of goods, services and content, are increasingly being misused to spread illegal content online. The providers of such services thus play a central role in combating illegal content but lack transparency on how they moderate – e.g. remove – content.

Objective of the Regulation: The Commission wants to regulate and harmonize the responsibilities and accountability of providers of intermediary services, including online platforms, and the oversight and enforcement procedures, in order to improve the internal market for such services and to create a safe and transparent online environment.

Affected parties: Providers of intermediary services, including online platforms, e.g. social media and marketplaces, business and private users ("recipients") of intermediary services.



Pro: (1) The fact that the Member State of establishment basically has sole responsibility for enforcement of the Digital Services Act facilitates the provision of EU-wide services by intermediary service providers.

(2) It is appropriate for the Digital Services Act to permit subsidiary enforcement by the Commission in the case of breaches of obligation by very large online platforms (VLOPs).

Contra: (1) The interference with the competence of the other Member States, arising from the state of establishment's sole responsibility for enforcement, is unlawful in view of the likely enforcement deficits. Where the state of establishment fails to act, other Member States must also be permitted to take measures for their territory.

(2) The procedure for cross-border cooperation between Digital Services Coordinators must be made more stringent. The enforcement procedure against VLOPs is also too protracted.

The most important passages in the text are indicated by a line in the margin.

CONTENT

Title

Proposal COM(2020) 825 of 15 December 2020 for a **Regulation** of the European Parliament and of the Council **on a Single Market for Digital Services (Digital Services Act)** and amending Directive 2000/31/EC

Brief Summary

- **Objectives and Definitions**
  - Digital services acting as intermediaries, i.e. connecting users with suppliers of goods, services and content, are increasingly being misused to spread illegal content online. The providers of such services thus play a central role in combating illegal content but lack transparency on how they moderate – e.g., remove – content.
  - With the Digital Services Act (DSA), the Commission wants to update and harmonise the responsibilities and accountability of providers of intermediary services (ISPs) in order to
    - improve the internal market for intermediary services (IS) and
    - create a safe and transparent online environment where fundamental rights are protected, e.g. freedom of expression, freedom of information and freedom to conduct a business [Art. 1].
  - IS are access, caching or hosting services [Art. 2 (f), (b), see cep**PolicyBrief** No. 22/2021].
  - Hosting services consist of storing content provided by the users ("recipients") of the service at their request, e.g. video streaming and cloud services and online platforms such as marketplaces and social media.
  - Illegal content is any information which, [Art. 2 (g), Recital 12]
    - under national or EU law, is either illegal per se – e.g. terrorist content –, or
    - relates to illegal activities, products or services, e.g. the sale of counterfeit products.
  - The DSA sets out harmonised
    - liability exemptions for ISPs [see cep**PolicyBrief** No. 22/2021],
    - due-diligence obligations for ISPs, tailored to specific categories of ISPs [see cep**PolicyBrief** No. 23/2021],
    - rules on oversight, cooperation and enforcement [this cep**PolicyBrief**].
- **Oversight and enforcement by the Member States**
  - The DSA will in principle be enforced by the Member States. Each Member State must [Art. 38, 39, 41 (5, 6)]
    - designate one or more competent independent authorities responsible for the enforcement and appoint one of them as its Digital Services Coordinator ("DSC") to coordinate the national enforcement measures and act as a contact point for the Commission and the DSCs of other Member States [Recitals 72, 73];

Authors: Anja Hoffmann, Matthias Kullas and Andrea DePetris | kullas@cep.eu
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Germany | Telephone + 49 761 38693-0 | www.cep.eu

- properly equip and empower its DSC and ensure that its measures are subject to effective judicial remedies and that the right to be heard and the right to privacy are respected [Art. 41 (5, 6)].

– Each DSC has jurisdiction over all ISPs whose main establishment, or – if the ISP has no establishment in the EU – legal representative, is located in the DSC's Member State. If an ISP fails to appoint a representative, all Member States have jurisdiction but must ensure ISPs are not prosecuted or punished twice [Art. 40].
– If an ISP is suspected of having infringed its obligations under the DSA, the DSC of the competent Member State ["DSC of establishment", DSCE] must investigate the matter and take effective, dissuasive and proportionate measures against infringements [Art. 41 (5)]. For this purpose, DSCEs have the following powers:
  - various powers to investigate infringements, e.g. to request information, conduct on-site inspections and interview staff [Art. 41 (1)];
  - specific enforcement powers in respect of ISPs, e.g. to [Art. 41 (2)]
    - order the cessation of infringements;
    - adopt interim measures in order to prevent serious harm;
    - impose fines and periodic penalty payments to be laid down by the Member States as follows:
      - fines for DSA infringements of up to 6% of the ISP's annual income or turnover, and
      - periodic penalty payments of up to 5% of its average daily turnover in order to enforce compliance with a decision of that DSCE, e.g. its order for cessation of an infringement;
    - as an ultima ratio, require an ISP to submit and follow an action plan and, if it does not "sufficiently comply" and the persisting infringement entails a serious criminal offence threatening the life or safety of persons, request a national court to order a temporary access restriction to the ISP's services [Art. 41 (3)].
– In addition, all DSCs must
  - certify national out-of-court settlement bodies [Art. 18] and appoint trusted flaggers [Art. 19];
  - receive and assess or transmit complaints against ISPs lodged by recipients in their Member State [Art. 43].

► **Cross-border cooperation among DSCs**

– An independent European Board for Digital Services ("Board") composed of all DSCs and possibly other national authorities will advise and assist DSCs and the Commission in the supervision of very large online platforms [VLOPs; s. cep**PolicyBrief** No. 23/2021] and ensure effective cooperation and the uniform application of the DSA [Art. 47-49].
– DSCs must justify deviations from the Board's advice [Art. 49 (2)].
– DSCs must cooperate with each other according to a further detailed procedure [Art. 45]:
  - If a DSC suspects an infringement, it must or, if the breach affects more than two Member States, the Board "may" request the competent DSCE to enforce compliance, which must take "utmost account" of the request.
  - If the DSC or the Board does not receive a reply within two months, or disagrees with the DSCE's assessment or measures, it may refer the matter to the Commission which "may" – within three months – request the DSCE to take further action and inform the Commission – within two months – about the measures taken.
– DSCs may participate in joint investigations if the infringing ISP operates in several Member States [Art. 46].

► **Stricter supervision and enforcement for Very Large Online Platforms (VLOPs) at EU-level**

– Very large online platforms [VLOPs] are subject to stricter supervision and enforcement at EU-level (p. 3). The Commission "may" initiate or take over proceedings against VLOPs:
  - If a VLOP is suspected of having infringed any DSA obligation [s. cep**PolicyBrief** No. 23/2021], the DSCE must either
    - investigate the matter on its own initiative or upon a "recommendation" from the Commission or the Board [Art. 50 (1)]; or
    - request the Commission to investigate and enforce the matter [Art. 46 (2)]. The Commission "may" then initiate proceedings against the VLOP [Art. 51 (1) b)]
  - If the DSCE adopts a decision stating that a VLOP has infringed a VLOP-specific obligation, it must [Art. 50 (2-4)]
    - request the VLOP to explain within one month, in an action plan, how it plans to end the infringement;
    - following the Board's opinion on the action plan due within one month, either accept the action plan within another month and review its implementation, or request the VLOP to undergo an independent audit to assess whether the action plan is effective and send the audit report within four months to the Commission;
    - communicate to the Commission, the Board and the VLOP within fixed deadlines – e.g. in case of an audit, one month from the receipt of the audit report – whether or not the VLOP has ended the infringement.
    - If the infringement continues, the Commission "may" take over and initiate proceedings [Art. 51 (1) c)].
  - The Commission "may" also initiate proceedings against a VLOP suspected of breaching an obligation if the DSCE has failed to take action in spite of the Commission's request [Arts. 51 (1) a), 45 (7)].
– The Commission has "strong" investigation and enforcement powers [Recital 98]. It may, inter alia,
  - carry out investigations on the (suspected) infringement, e.g. through requests for information [Art. 52], interviews [Art. 53] and on-site inspections with the assistance of auditors or experts [Art. 54];
  - order interim measures in cases where there is a risk of serious harm for the recipients [Art. 55], make the commitments of VLOPs binding [Art. 56] and take actions to monitor compliance, e.g. order VLOPs to explain and provide access to their databases and algorithms [Art. 57];

- adopt "non-compliance decisions" and order VLOPs, that do not comply with the DSA or, inter alia, with interim measures ordered against them, to take the necessary measures to ensure compliance [Art. 58];
- impose fines on VLOPs of up to 6% of their total turnover in the preceding financial year for such non-compliance, or of up to 1% of that turnover e.g. for non-compliance with simple Commission requests [Art. 59];
- impose periodic penalty payments on VLOPs, or interviewed persons, of up to 5% of the average daily turnover in the preceding financial year, in order to enforce a non-compliance decision or any other formal Commission decision compelling them e.g. to supply information [Art. 60].

– If the infringement persists and causes serious harm, the Commission may – as an ultima ratio – request the DSCE to seek a temporary access restriction to the VLOP's services by a national court [Arts. 65, 41(3)].

Statement on Subsidiarity by the Commission

The conditions for cross-border digital services can only be harmonised at EU level (see cep**PolicyBrief** No. 22/2021).

Policy Context

The European Parliament has released resolutions [2020/18/INL, 2020/19/INL and 2020/2022/INI] with recommendations on a DSA. Together with the Digital Markets Act (see cep**Input** No. 12/2021,cep**PolicyBriefs** No. 14/2021 and No. 15/2021), the DSA is part of the Commission's proposal on new rules for digital platforms.

Legislative Procedure

15 December 2020	Adoption by the Commission
Open	Adoption by the European Parliament and the Council, publication in the Official Journal of the European Union, entry into force

Options for Influencing the Political Process

Directorates General:	DG Communications Networks, Content and Technology
Committees of the European Parliament:	IMCO (leading), Rapporteur: Christel Schaldemose (Denmark, S&D), LIBE, JURI, ITRE, ECON TRAN, CULT, FEMM
Federal Germany Ministries:	Economic Affairs (leading)
Committees of the German Bundestag:	Open
Decision-making Mode in the Council:	Qualified majority (acceptance by 55% of Member States which make up 65% of the EU population)

Formalities

Competence:	Art. 114 TFEU (Internal Market)
Type of Legislative Competence:	Shared competence [Art. 4 (2) TFEU]
Procedure:	Art. 294 TFEU (ordinary legislative procedure)

ASSESSMENT

Economic Impact Assessment

The obligation to appoint a DSC will facilitate cooperation between the Member States and with the Commission. Many Member States will entrust enforcement of the DSA to several authorities and it may not be immediately clear to externals which authority is competent in the specific case. It is therefore appropriate that the Commission, Board and ISPs are able to use a single point of contact and that the DSC will ensure the necessary internal cooperation and coordination with all competent national authorities. In order to guarantee that the DSC provides adequate external representation of the interests of the internally competent national independent authorities, Member States should be allowed to make their instructions binding upon their DSC.

Since the obligations under the DSA are public law and not private law obligations, effective public enforcement is required to ensure compliance. The DSA rightly upholds the country of origin rule of the E-Commerce Directive: **The fact that the Member State of establishment basically has sole responsibility facilitates the provision of cross-border services by ISPs** because, to a large extent, ISPs only have to comply with the instructions of that Member State when providing services in the EU. **There is** however **a risk – particularly where a DSCE fails to act – of deficits in enforcement and distortions of competition** because ISPs could (re-)locate their establishments to Member States with "weaker" enforcement, and by the same token, Member States could also use this to compete for main establishments. **It is** therefore **appropriate for the DSA to permit subsidiary enforcement by the Commission in the case of breaches of obligation by VLOPs**.

The fact that the Commission is supported by the Board in supervising VLOPs means that it has recourse to the expertise of the Member States thereby improving enforcement. However, the Commission – as well as individual DSCs – should be more strictly bound by the Board's requests. In addition, the Commission should also be able make direct requests for support from individual DSCs when expertise is lacking.

Legal Assessment

Legislative Competence of the EU & Subsidiarity

The DSA is rightly based on the internal market competence [Art. 114 (1) TFEU] and, in the overall assessment, is compatible with the principle of subsidiarity (see cep**PolicyBrief** No. 22/2021). In particular, supervision of VLOPs operating EU-wide can be more effectively regulated at EU level, especially as supervision can thus be strengthened by the Commission.

Proportionality with Respect to Member States

The choice of a Regulation rather than a Directive is proportionate because, for one thing, it would not be appropriate to transpose enforcement powers accorded to the Commission into national law. The DSA is nevertheless disproportionate because its relationship to national law and the scope of its blocking effect are unclear (see discussion on proportionality in cep**PolicyBriefs** No. 22/2021 and No. 23/2021).

The fact that the authorities of the Member State of establishment basically **have sole responsibility for enforcement of the DSA constitutes interference with the competence of the other Member States** to enforce EU law**. In view of the likely enforcement deficits, this is** not compatible with the principle of proportionality and therefore **unlawful.** Experience with the General Data Protection Regulation shows that national supervisory authorities are not always able or willing to enforce the law. The DSA does not yet deal adequately with this risk. Thus, **where the DSCE fails to act,** – non-competent – **DSCs in other Member States must also be permitted to take** specific, individual – and in urgent cases immediate – **measures for their** sovereign **territory,** in circumstances regulated by the DSA, such as for the protection of public order and health.

The procedure for cross-border cooperation between DSCs must be extended and **made more stringent** with shorter deadlines. If another DSC or the Board requests the DSCE to take action, it can take up to seven months and thus too long for the Commission to get involved and assess the matter. Furthermore, the parties involved should each be obliged to take action.

The Commission's strict enforcement powers are basically justified as they prevent distortions of competition caused by variations in levels of enforcement against powerful VLOPs operating EU-wide, and the Commission is only able to intervene if the DSCE has requested it or fails to act. **The enforcement procedure against VLOPs is also too protracted, however,** which hampers effective enforcement against VLOPs. **In addition, the Commission should** not only **be** entitled but **obliged** to act, i.e. **to call on inactive DSCEs to take measures** (and not simply "recommend" them to carry out an assessment) – **and if necessary initiate its own proceedings.**

In case of breaches by smaller ISPs, affected **Member States should also** – at least **in certain cases** of relevance still to be defined – **have the right to involve the Board or the Commission as a subsidiary regulator or coordinator where the DSCE remains inactive.** It is not sufficient for the Commission – which can only initiate proceedings itself in the case of VLOPs – to merely request the DSCE again to take measures without further consequences whilst other Member States are unable to act due to the country of origin rule.

Compatibility with EU Law in Other Respects

The wide enforcement powers of the DSCE and the Commission constitute an intervention in the right of ISPs and/or VLOPs to conduct a business [Art. 16 CFR]. Like the ISP's obligations, however, they are justified inter alia for the purpose of protecting conflicting fundamental rights and objectives recognised by the EU as serving the general interest [see cep**PolicyBrief** No. 23/2021].

Impact on and Compatibility with German Law

In Germany, the Federal Office of Justice is responsible for enforcing the obligations of social networks under the Network Enforcement Act; under the State Media Treaty, the state media authorities exercise supervision over the private media service providers. The DSA supersedes these regulations in its scope of application. Germany can entrust the enforcement of the DSA to one or more existing authorities – e.g. the Federal Network Agency or the Federal Cartel Authority – or a new "Federal Institute for Digital Transformation", but can only designate one of them as DSC.

Summary of the Assessment

The fact that the Member State of establishment basically has sole responsibility for enforcement of the DSA facilitates the provision of cross-border services by ISPs. In view of the likely enforcement deficits, however, the associated interference with the competence of the other Member States is unlawful. Where the DSCE fails to act, DSCs in other Member States must also be permitted to take measures for their territory. The procedure for cross-border cooperation between DSCs must made be more stringent. It is appropriate for the DSA to permit subsidiary enforcement by the Commission in the case of breaches of obligation by VLOPs. The enforcement procedure against VLOPs is also too protracted, however. In addition, the Commission should be obliged to call on inactive DSCEs to take measures and if necessary initiate its own proceedings. In case of breaches by smaller ISPs, Member States should also have the right, in certain cases, to involve the Board or the Commission as a subsidiary regulator or coordinator where the DSCE remains inactive.