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

DIGITAL SERVICES ACT
PART I: SCOPE AND LIABILITY EXEMPTIONS

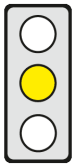
cep**PolicyBrief** No. 22/2021

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 harmonise the responsibilities and accountability of providers of intermediary services (ISPs), including online platforms, and the oversight and enforcement procedures, in order to improve the internal market for such services and 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 DSA will also apply to ISPs that are not based in the EU will level the playing field between EU and non-EU ISPs.

(2) By generally upholding the liability exemptions also for ISPs that take voluntary measures, the "Good Samaritan Clause" removes disincentives to take voluntary action against illegal content. However, clarification is required of the conditions which prevent an ISP from invoking this clause.

Contra: (1) The DSA's relationship to national law and the scope of its possible blocking effect are unclear.

(2) The extension of liability for "active" ISPs unlawfully interferes with their fundamental rights. The DSA must specify when a provider has an "active" role.

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 offering 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)].
    - Access services consist of either transmitting third-party content via a communication network, or providing access to such a network, e.g. Internet access services.
    - Cashing services consist of transmitting third-party content via a communication network, involving the automatic, intermediate and temporary storage of that content – e.g. on a proxy server – for the sole purpose of accelerating the onward transmission of the content.
    - 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.
- **Scope of the Digital Services Act**
  - The DSA applies to IS that are supplied to recipients established or residing in the EU, even if the ISP is based outside the EU, provided there is a "substantial connection" to the EU. This is assumed, e.g., if the ISP targets its activities at recipients in the EU or actually has a significant number of recipients there. [Art. 1 (3), Recitals 7, 8)]
  - The DSA establishes general rules on the provision of IS which do not amend but complement the following legislation, and will only apply insofar as this legislation does not contain more specific rules [p. 4, Recital 9-11]:
    - the E-Commerce Directive ("ECD") [2000/31/EC]);

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

- other more specific sectoral EU legislation, e.g. the Audiovisual Media Services Directive [2010/13/EU], the Terrorist Content Online Regulation [(EU) 2021/784], and the EU copyright law;
- the EU law on consumer protection and on the protection of personal data and privacy, in particular the General Data Protection Regulation (EU) 2016/679 (GDPR).

– In particular, the DSA sets out harmonised
- liability exemptions for ISPs [this cep**PolicyBrief**],
- due-diligence obligations for ISPs, tailored to specific categories of ISPs [cep**PolicyBrief** No. 23/2021],
- rules on oversight, cooperation and enforcement [cep**PolicyBrief** No. 24/2021].

► **Liability exemptions for ISPs**

– The liability exemptions for ISPs will be deleted from the ECD and integrated broadly unchanged into the DSA.
– ISPs that transmit or store illegal content are not liable under EU or national law under the following conditions:
- providers of access services if they do not initiate the transmission, do not select the receiver or the transmitted content, or modify the content [Art. 3],
- providers of caching services if they act expeditiously to remove or block content that was removed or blocked at the initial source of the transmission [Art. 4],
- providers of hosting services if they have no actual knowledge that the hosted content or activity is illegal, are not aware of facts or circumstances from which the illegality is apparent and act expeditiously to remove or block content once they obtain such knowledge [Art. 5].

– Online platforms are however liable under "consumer protection law" if they create the false impression that a product, service or content provided by a third-party trader is provided by the platform itself [Art. 5 (3)].
– Providers of the following services can also benefit from the liability exemptions to the extent that their services qualify as access, caching or hosting services [Recital 27]:
- wireless local area networks (W-LAN),
- domain name services (DNS) and top-level-domain name registries,
- authorities that issue digital certificates,
- content delivery networks such as Amazon Web Services that e.g. improve the functions of other ISPs,
- online communications services such as web-based telephony (voice over IP), messaging and e-mail services.

– ISPs cannot benefit from the liability exemptions if they do not provide their services "neutrally" – because they do not confine themselves to the mere technical and automatic processing of third party content but play an "active role" which enables them to have knowledge of or control over such content [Recitals 18, 20].
– The liability exemptions may also apply to ISPs that undertake voluntary activities aimed at detecting, identifying and acting against illegal content, provided the ISP carries out such activities "in good faith and in a diligent manner" ["Good Samaritan Clause", Art. 6, Recital 25].
– An ISP can obtain knowledge or awareness through own-initiative investigations [Recital 22]. Such activities should not be taken into account when determining whether it can rely on a liability exemption [Recital 25].

► **Monitoring obligations for ISPs and national orders**

– As under the ECD, ISPs still have no general obligation to monitor third party content which they transmit or store, nor to actively seek facts indicating illegal activity [Art. 7, Recitals 16, 28].
– National courts and administrative authorities may however impose specific monitoring obligations on ISPs through injunctions, even where the respective ISP meets the conditions of the liability exemptions [Recitals 24, 28 et seqq]. Such courts and authorities may order ISPs
- to act against – e.g. to remove or block – a specific item of illegal content defined in the order [Art. 8], or
- to provide specific information about individual recipients [Art. 9].

– Orders to act must [Art. 8 (2 a, b), Recital 31]
- explain why the content is illegal, contain an appeal clause and be issued in the language chosen by the ISP,
- be limited to the territorial scope that is strictly necessary, taking into account the rights of third parties and whether the content is also illegal in other Member States.

– An ISP who receives an order must inform the issuing authority how it has complied with the order [Art. 8 (1)].
– Orders relating to specific illegal content or information do not in principle restrict the freedom of ISPs to provide their services across borders. Therefore, national authorities may also address orders to ISPs based in another Member State without the need to justify a derogation from the ECD's country of origin principle. [Recital 33]

Statement on Subsidiarity by the Commission

The conditions for cross-border digital services to develop in the EU can only be harmonised at EU level. This creates legal certainty, reduces compliance costs and is necessary to cover ISPs based outside the EU and to build a coordinated supervisory system that is reinforced at EU level. [p. 6, Recital 4]

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** 14/2021 and 15/2021), the DSA is part of the Commission's proposal on new rules for digital platforms.

Legislative Procedure

15.12.20	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 fact that the DSA will also apply to ISPs that are not based in the EU will level the playing field between EU and non-EU ISPs.

Despite the applicability of the country-of-origin principle, ISPs still have to deal with different national definitions of illegal content, e.g. when they receive a notice of such content from a user and have to decide whether to remove it. The regulatory costs for ISPs may also increase, as France has passed a law according to which the dissemination of "potentially harmful" content can also be a criminal offense and thus illegal. In Poland, too, disinformation could be qualified as illegal by law.

The prohibition of a general monitoring obligation prevents Member States from imposing such an obligation on ISP. Both this prohibition and the liability exemptions allow ISPs to store and distribute user content in principle without prior review. They are therefore important for guaranteeing freedom of expression and of information as a central pillar of the Internet and the Commission is right to keep the liability exemption regime as wide as in the ECD. However, **it remains unclear whether certain types of IS** – e.g. DNS or content delivery networks – **qualify as access, caching or hosting services** and can thus benefit from the liability exemptions**.**

By generally upholding the liability exemptions also for ISPs that take voluntary measures against illegal content**, the "Good Samaritan Clause" removes disincentives to take voluntary action** aimed at detecting, identifying and acting **against illegal content. However**, it must be clarified that ISPs undertaking such activities are not per se exempt from liability; they must remove illegal content of which they have gained knowledge but will not be liable as an "active" provider for other illegal content which they have overlooked or wrongly judged to be legal. **Clarification is** also **required of the conditions which prevent an ISP from invoking this clause because it has failed to carry out such** voluntary **measures "diligently".** Furthermore, it is unclear whether the clause can induce ISPs to "over-block" content. As ISPs have the technical capabilities to remove illegal content and sometimes can even benefit from illegal content, the DSA rightly provides that ISPs may be required to act against specific illegal content.

Legal Assessment

Legislative Competence of the EU

The DSA is correctly based on the internal market competence [Art. 114 (1) TFEU].

Subsidiarity

Overall, uniform obligations to combat illegal content for ISPs established in the EU and in third countries [see cep**PolicyBrief** No. 23/2021], an effective supervisory system [see cep**PolicyBrief** No. 24/2021] and the exemptions from liability already enshrined in EU law, can only be meaningfully regulated at EU level.

Proportionality with Respect to Member States

Although it contains many appropriate regulatory proposals, the DSA is disproportionate and should therefore be revised. Thus, on the one hand, **there is ambiguity about its relationship to national law and the scope of its possible blocking effect.** The fact that the DSA envisages full harmonisation in its regulatory area is supported inter alia by the emphasis on the harmonising purpose and the non-adoption of the opt-out clause, contained in the EC Directive, allowing Member States to determine their own procedures governing the removal of hosted content. On the other hand, the DSA does not regulate some essential issues, such as the question of what content is illegal, when ISPs are liable, when national courts and authorities can issue orders as well as the substantive-law duty of ISPs to delete illegal content. This lessens the DSA's harmonising effect but at the same time reduces its interference in national liability law, and national administrative and procedural law. Clarification is however required that Member States can still regulate the points left unregulated by the DSA, and on the extent to which they are permitted to adopt or retain stricter rules, e.g. on safeguarding media pluralism or to ensuring the protection of minors in relation to the media.

The DSA appears to have included the EC Directive's rules on liability exemptions for ISPs without making any changes, but according to the Recitals, the EC Directive's country of origin principle shall no longer apply to orders to act against illegal content and to provide information, which relate to specific items of illegal content. This makes it easier for authorities and courts to issue orders to block or remove content that is illegal in their country also against ISPs based in other Member States. Whilst the scope of national orders will be limited to what is necessary and the authority issuing the order must take into account the rights of third parties and consider whether the same content is also illegal in other countries, it is still doubtful whether a block limited to certain countries is in fact technically possible. **It is also unclear how cross-border orders**, enabling authorities to exercise sovereign rights in other Member States, **can be enforced or challenged. The DSA must** therefore **provide for procedures which allow** affected **authorities, ISPs and content providers to contest such orders.**

Compatibility with EU Law in Other Respects

As illegal content violating third-party rights – e.g. intellectual property or personal honour – is increasingly being transmitted via ISPs, it is appropriate to impose stricter obligations on ISPs to take action against illegal content. The superficial codification of the of the concept of "active and passive providers", developed by the European Court, [ECJ, C-236/08 ECLI:EU:C:2010:159, Google France, para. 120], in the DSA makes it impossible for "active" ISPs to rely on the liability exemption. **The extension of liability for "active" ISPs** is disproportionate and therefore **unlawfully interferes with their fundamental rights,** i.e. the right to conduct a business [Art. 16 CFR]. **The DSA must specify when a provider has an "active" role** – such as knowledge of, or control over, the content – as there is legal uncertainty on this point. In addition, ISPs that remain inactive but profit substantially from illegal content, should not be permitted to rely on the liability exemptions. The denial of the liability exemption for online platforms that are liable under "consumer protection law" for misleading their users about their contract partner, must also be clarified as the term "consumer protection law" is not clearly defined.

Impact on and Compatibility with German Law

The Telemedia Act, in which Germany has transposed the liability exemptions under the EC Directive, must be amended. The DSA also conflicts with the German Network Enforcement Act [NetzDG] and the amended State Media Treaty [MStV] which impose additional parallel obligations on ISPs. It is uncertain how far Germany will be permitted to uphold these laws after entry into force of the DSA; their conformity with EU law is already contested since these laws diverge from the country of origin principle.

Summary of the Assessment

The fact that the DSA will also apply to ISPs that are not based in the EU will level the playing field between EU and non-EU ISPs. It remains unclear whether certain types of IS – e.g. DNS or content delivery networks – qualify as access, caching or hosting services. By generally upholding the liability exemptions also for ISPs that take voluntary measures, the "Good Samaritan Clause" removes disincentives to take voluntary action against illegal content. However, clarification is required of the conditions which prevent an ISP from invoking this clause because it has failed to carry out such measures "diligently". Although it contains many appropriate regulatory proposals, the DSA is disproportionate and should therefore be revised. Thus, on the one hand, there is ambiguity about its relationship to national law and the scope of its possible blocking effect. It is also unclear how cross-border orders can be enforced or challenged. The DSA must provide for procedures which allow authorities, ISPs and content providers to contest such orders. The extension of liability for "active" ISPs unlawfully interferes with their fundamental rights. The DSA must specify when a provider has an "active" role.