WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

POSITION PAPER

Highlights on the proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) – COM(2020) 825 final

Brussels/Berlin, 1 September 2021

The European Commission published its proposal for a Digital Services Act (DSA)[1] as an update to the Directive on electronic commerce, known as the E-Commerce Directive (ECD)[2] at the end of 2020. eco reacted with its position paper[3] in March and commented on numerous aspects of the proposal.

Since the presentation of the DSA, discussions in the European Council and the European Parliament have picked up and a progress report[4], as well as several (draft) reports, have been published in each case.

While there is clear support for the DSA to modernise the regulatory framework for Internet services, questions regarding, inter alia, the methods and the scope are diverse and still need to be addressed.

eco would like to support the current discussions by highlighting selected core elements or issues, in order to reiterate not only their importance to the Internet industry, but also the concerns regarding the current developments and changes in the course of the discussion.

1. Framework and Scope

The key strength of the ECD was its horizontal and its general approach, which refrained from being too specific. The European Parliament and the Council now have the opportunity to update what has been the cornerstone and basic framework of Internet regulation for 20 years.

The Internet and its services have a multitude of different profiles. However, when it comes to the in-depth content, specific legislation can build upon the general framework. eco has recently seen such proposals being presented. Therefore, the DSA should remain as a general, horizontal framework and neither become a youth- or consumer-protection law nor another copyright law. To prevent further fragmentation of the European Digital Single Market, the DSA – as a regulation –

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0825

[2] **Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), OJ L 178, 17.7.2000, p. 1.**

[3] https://go.eco.de/dsa

[4] https://data.consilium.europa.eu/doc/document/ST-8570-2021-INIT/en/pdf

should not allow the Member States to adopt additional restrictions which go beyond its rules.

The legislators are facing the risk of overloading the DSA with specificities and covering, on the one hand, a wide range of very broad and diverse services providers (which, not least, is to involve micro, small and medium-sized enterprises) and, on the other hand, an overblown list of services (even including, for example, messenger services, search engines, live streaming services). All of this, combined with obligations which are overly burdening and overly specific, could lead to hampering the objective of the Digital Single Market and further pushing away innovative companies.

eco therefore urges the legislators to maintain the DSA as general and horizontal, and not to further expand its scope, but to offer clear rules for the providers effectively in scope. The DSA objective must be revisited with a focus on basic framework conditions and regulations. The vague active/passive distinction should finally be set aside and, instead, clear criteria should be delivered. Obligations should be efficient and balanced, applying only to providers and services that pose a certain risk level. As such, for instance, KYBC requirements should apply to marketplaces but not to all intermediary services providers. This is because transparency obligations which are too far-reaching can lead to the abuse of the system and have a negative impact on services, providers and users. In addition, no provider should prima facie be prevented from deleting or blocking access to any content hosted on its systems.

In addition, having the same extended obligations to which hosting services or even online platforms are subject to imposed on mere conduit, caching or ‘pure’ hosting services would inappropriately add unnecessary burdens to these services.

While the legality of content is defined by law, harmful content is defined by a subjective impression and also handled inconsistently across the Member States. eco supports the Commission’s approach to focus regulatory efforts on illegal content and to address harmful content separately, such as through voluntary or co-regulatory approaches. Then again, it needs to be ensured that legal restrictions on blocking for Internet service providers and voluntary or co-regulatory approaches do not counter each other.

2. Definitions

One of the points of general criticism regarding the ECD was its partial lack of clarity regarding definitions. This was the case, for example, on the point of actual knowledge. Until now, it has not been clearly established as to when the criteria of actual knowledge are fulfilled or when they are actually not. However, the proposed text does not satisfy the expectations for clarification in this regard since, once again, it does not elaborate on the issue. Only in Article 14.3 does the DSA offer an example of notices giving rise to “actual knowledge or awareness”. Yet, by doing so, it creates strong incentives for an excessive removal of content. eco urges the legislators to clarify that actual knowledge can only be the result of an investigation and that a report or flagged content should in no case create a

punishable obligation to remove or disable access to information in any other way than by a court order.

A newly-introduced definition is the one of “active recipients”, which builds the basis for the definition of very large online platforms. However, this remains very unclear. The same recipient or user could easily be mistaken for different users, for example, when s/he uses different devices (mobile, desktop), different connection methods (mobile data or multiple Wi-Fis) or simply different applications to access an online platform (browser[s], a designated app). Only registered users of a service/platform can clearly be identified and distinguished from others.

Finally, the reference in Recital 27 names fundamental services contributing to the technical infrastructure of the Internet (e.g. DNS, CDN or registries) and confirms that these services could benefit from liability protection under the DSA. However, eco would like to highlight that the framework’s clarity would benefit from including these references in the regulatory part of the proposal, specifying into which category of intermediaries the mentioned services fall.

3. Trusted Flaggers

Trusted flaggers have been used by online platforms for a reasonable length of time, with the intention to support their work of finding and evaluating unwanted content on their platforms. Thus far, the choice of partners and procedures for reports was for the online platforms to make, depending on their criteria and their requirements. It is a system highly based on trust between the involved participants.

With the DSA, the legislators propose removing the decision-making from the online platforms and centralising it on a national level by leaving it up to the DSC to define a minimum group of appointed trusted flaggers. This proposal comes without any indication being given as to why a well-established system, developed between trusted flaggers and online platforms, is forced into centralisation on a national level – while most online platforms are working across borders. eco regards these changes as a deterioration.

An entity should not be awarded a trusted flagger status by merely fulfilling some criteria; instead, it should earn its status due to its achieved results. Moreover, it should be up to an online platform working with that trusted flagger to decide on the processing of its reports in terms of priority and verification. Finally, that status should be withdrawn if the quality of the reports or the co-operation does not meet certain standards – even more so if an entity working in its own or its members’ interest should be allowed to apply to be awarded a trusted flagger status.

4. Notice, Takedown and Complaint Procedure

The DSA introduces a relatively detailed notice and action procedure for hosting providers. While eco understands the logic of the approach, we would welcome a mechanism which would allow hosting providers some leeway to reject takedown requests referring to content that is not manifestly illegal, but simply questionable.

Through applying such a mechanism, the severe risk of over-blocking could be minimized, given that hosting providers would otherwise face the risk of liability for not taking down questionable content which they have been made aware of. Finally, eco strongly advocates that the DSA should not allow a request to automatically give rise to actual knowledge in any possible case – especially in regard to Article 14.3 DSA.

eco is concerned that the legislators are putting private companies in the position of a judicial actor. The legal interpretation of content cannot, and most definitely should not, be delegated to an intermediary services provider. Especially considering the fact that the Internet is a global network and that even smaller intermediary services providers often operate internationally, a legal interpretation of content in terms of the respective national law in any possible market constitutes an inextricable challenge.

The situation would be even further exacerbated if some content (e.g. content of particular importance to public policy, public security or public health) or certain users (e.g. persons of public interest or media) would have to be treated differently.

Strictly defined requirements and deadlines (30 minutes, 24 hours, etc.) for reactions regarding content would not be beneficial to either side, but would expose smaller operators in particular to the risk of misjudgement and dramatically increase the likelihood of over-blocking.

Regarding the envisaged responsibility for online platforms to provide the recipient of their service with an internal complaint-handling system: eco would like to highlight that allowing the users to start a complaint procedure up to six months after an action has been taken by the platform is unrealistic and disproportionate. If a recipient of a service does not challenge the decision of an online platform in the short-term, it must be expected that s/he either does not feel treated wrongly, that the relevance of the action is minor, or that the account is no longer active. For an online platform, on the other hand, this long period would increase the number of cases to be brought forward and would mean that data has to be retained. As well as that, in the meantime, the reasoning could face changed realities. eco therefore appeals for the period to be drastically decreased. eco also requests the legislators to consider defining exceptional circumstances in which intermediaries are not obliged to offer redress options, including out-of-court dispute settlement – for example, when the content in question is spam, child sexual abuse material or terrorist content – as well as actions taken based on orders by national authorities.

Furthermore, with regard to Article 18.3 DSA, eco would like to underline that the process of arbitration does not include any protective measures against abuse and, as a consequence, actors in bad faith could flood an intermediary with out-of-court dispute settlement procedures, generating costs (which the online platform would mainly have to bear) and slowing down the process for other, legitimate recipients of the service. This approach appears as unjustifiably imbalanced.

Finally, eco believes that out-of-court dispute bodies should be distinct from regulatory oversight bodies and that the text should clarify this.

5. Transparency Obligations

In its attempt for more transparency, the Commission's DSA proposal introduces obligatory information to be provided in the intermediary services provider's Terms and Conditions (T&C). While, to a certain extent, transparency is an approach to be welcomed, it is only useful when it is adequate and proportionate.

If intermediary services providers are obliged to share detailed information on, for example, measures, tools and algorithms used to address illegal behaviour or content, it might prevent these from working efficiently and offer means of circumvention to malicious users. In addition, while general rules on content moderation have a permanent character, some more granular parts might change according to worldwide developments without an intermediary's immediate influence. As a consequence, an obligation for an excessive level of detail could lead to the T&C becoming an unreliably fluid document.

Regarding the introduction of new and extensive transparency reporting responsibilities: eco does not see a benefit for anyone if excessive reporting obligations lead to an increased administrative, organizational, personnel and financial burden for companies. Therefore, eco advocates for reasonable reporting obligations – which would be completely countered if the obligations were expanded even further beyond online platforms.

Finally, eco considers there to be high expectations but also misunderstanding concerning algorithms, as well as corresponding transparency and its evaluation. On the one hand, it can be observed that legislators use the term mainly for recommender algorithms. These, however, reflect only one field of application. On the other hand, expectations regarding the effect of transparency seem too far-reaching, with one reason for this being that the algorithms' logic is mostly learned from training data and is rarely reflected in its source code.[5]

eco therefore strongly recommends that demands for algorithmic transparency and evaluation obligations be reconsidered and that, in all cases, they are kept realistic and sufficiently specific.

6. Conclusion

The DSA offers the opportunity to close the ECD's gaps and to update the horizontal framework corresponding to the technological developments of the last 20 years. However, the DSA proposal does not deliver, for example, on the need for a clear scope and clear definitions. Legislators should make sure that the list of included services is focused on the ones necessary and that the obligations are in accordance with the intermediary services providers' abilities. The objective of the European

[5] **cf. Harvard Business Review, "We Need Transparency in Algorithms, But Too Much Can Backfire", Kartik Hosanagar and Vivian Jair, 23 July 2018, https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire**

Digital Single Market and the goal of innovation also originating from European companies should further be borne in mind.

The trusted flagger system is a well-developed solution used by numerous platform providers in cooperation with many different partners. The DSA's current attempt to evolve by centralising this tool might be well-intentioned. However, the obligatory character in combination with 27 national pools would lead to a transformation of the current system into an inefficient and counterproductive one.

Regarding the notice and takedown procedure, in combination with the strictly defined deadline to take action and the complaints procedure: eco understands the reasoning behind the legislative approach. However, aside from clear rules, it is necessary to allow hosting providers some leeway on handling complaints – for example, in order to prevent them from only being able to choose between over-blocking or potential liability. Furthermore, the exposure to misuse needs to be taken into account and related measures should be introduced.

In different instances, the DSA sets transparency obligations for intermediary services providers. While a certain amount of transparency can help intermediaries as well as regulators or users, these duties need to be adequate and proportionate. Overly excessive expectations are counterproductive.

Finally, it has to be borne in mind that European regulation can become a blueprint for international legislation and that, in other countries, a more restrictive interpretation could lead to undesired outcomes, justified by the DSA.

About eco

With more than 1,100 member companies, eco is the largest Internet industry association in Europe. Since 1995, eco has been instrumental in shaping the Internet, fostering new technologies, forming framework conditions, and representing the interests of members in politics and international committees. The focal points of the association are the reliability and strengthening of digital infrastructure, IT security, trust, and ethically-oriented digitalisation. That is why eco advocates for a free, technology-neutral, and high-performance Internet.