15 February 2022

Quality over Speed

How to strengthen platform-accountability in the Digital Services Act (DSA)

About HateAid:

HateAid gGmbH is the first consultation centre for victims of online violence in Germany. So far HateAid has consulted more than 1700 victims and supported more than 170 of them by financing litigation. Through this, HateAid enables them to enforce their rights against perpetrators and online platforms. As part of the Landecker Digital Justice Movement, HateAid advocates for more accountability of social media platforms. This position paper has been drafted in cooperation with Dr. Daniel Holznagel.

It's on the table - Lawmakers still can make the DSA better**:**

European Lawmakers have started negotiating the DSA in the so-called Trilogue. With this paper we want to underline the urgent need for further improvements of the DSA in the course of these negotiations. It should be the goal of all parties of the Trilogue to make the DSA an effective and powerful instrument with rules which live up to the high expectations of our society. In that regard, we want to encourage lawmakers to exhaust all possibilities.

In their protocol declarations regarding the Council General Approach several Member States, e.g. Germany[1], have strongly underlined the need for further improvements of the DSA. This should be taken seriously and needs to be pursued: The Lawmakers' mandate is not restricted to finding a compromise between the draft texts of the Commission, Parliament and the Council. Where necessary, lawmakers can and should go beyond the draft proposals.

One aspect is of specific significance for the protection of minors especially in Germany . As it stands now, the DSA would undermine new § 24a of the German Youth Protection Act, which is the - by far - the most relevant due diligence provision for online platforms.

[1] But see also Italy and Spain.

Quality over speed:

One main objective of the DSA is to establish a powerful and clear accountability framework for online platforms regarding action against illegal activities and online violence. This is necessary to not only protect our citizens, but also freedom of expression online and thus our democracies.

However, we are very concerned that the DSA will fail to deliver on this objective. The current DSA is disappointing. Regarding important aspects, the DSA lacks ambition to take the needs of victims of online violence into account. More concerning, certain effective measures under the current status quo will be outlawed by the DSA, without introducing adequate alternatives.

We warn that - facing political pressure - lawmakers opt for hastily agreeing on an immature text that would define our legal framework for decades to come. We are afraid that lawmakers miss the chance of introducing an ambitious level of protection for our citizens, and that the DSA will remain too industry-friendly. If the DSA falls short on user's rights the consequences for victims of online violence would be dramatic. Their protection must be a priority in every attempt to platform regulation as online violence has long become a mass phenomenon. According to our own findings 66 % of EU citizens have already witnessed online violence, and 27,5 % have been personally affected. Young adults are even more vulnerable: 90 % of EU citizens between 18 - 35 % have witnessed online violence and around 50 % have been personally affected already[2]. As a result more and more users withdraw from online discourse out of fear of online violence. Almost every second EU citizen has already been afraid to express their opinion in online debates out of fear to become a victim. Moreover a remarkable number of 92 % of users agree that illegal content should be removed from online platforms and almost 90 % of users in the EU think that we need laws to better control platforms.

Therefore, lawmakers need to insist on serious improvements. From our perspective the motto must be: Quality over Speed.

[2] HateAid EU Survey, 2021: https://hateaid.org/eu-survey/

HateAid's suggestions for the Trilogue:

HateAid has thoroughly studied the amendments to the draft DSA which were suggested by the EP and the Council. We did explain in a separate paper which of the amendments should be supported and which should be rejected, and we kindly refer to that document.

However, as we have explained in the sections above, in certain aspects, the DSA needs further improvements. From our perspective, these further improvements either do not conflict with the existing draft texts, or they are covered by the mandate following from e.g. Germany's protocol declaration.

We therefore urge the parties of the Trilogue to take into account the following suggestions on how to strengthen enforcement of user's rights in the DSA:

Summary:

Detailed Explanation:

1. Recital 18: "Active role" - definition should be in line with recent ECJ Case Law and cover "active role through design"

Art. 3 - 7 DSA transfers the safe harbour provisions from Art. 12 - 15 ECD into the DSA, without substantial changes. These safe harbour provisions grant immunity from liability to platforms of all kinds and sizes, except for a very specific set of "bad actors". It is well established that the liability exemptions are not available when a platform and its user collaborate (deliberate collaboration[3]) or when a platform plays an active role through "knowledge or control" of infringements[4]. The DSA rightfully incorporates both of these exemptions (deliberate collaboration[5] and active role through "knowledge or control"[6]). Regarding these exemptions, we welcome the suggestion in the General Approach to clarify the definition of "deliberate collaboration"[7].

Beyond "deliberate collaboration" and "active role through knowledge or control", another sub-definition of "active role through platform-design", which is established through recent ECJ case law should be incorporated in the DSA: In its joint cases against YouTube/Cyando, the ECJ implicitly acknowledged a sub-definition of an "active role"-provider. It argued that the defendant platform *Uploaded* could not rely on the liability exemptions due to contribution based on platform design and business model. It reasoned that the defendant platform's design incentivized infringements and the operator failed to counter such risks credibly[8]. The DSA should incorporate this logic from the YouTube/Cyando - ruling. This would help to exempt bad actor platforms from the liability exemptions. E.g. porn-platforms not implementing identification mechanisms[9] or when such platforms offer tags like "hidden cam" (which might incentivize users to post sexually abusive material without consent). Such

[3] Art. 14(2) ECD, Recital 44 ECD.
[4] Recital 42 ECD and respective ECJ Case Law, see decisions of 23.3.2010 - C-236/08, C-237/08, C-238/08 - Google France, para 120; decisions in Cases C-324/09 - L'oreal v. eBay; C-291/13 - Papasavvas; C-521/17 - SNB-REACT v. Mehta.
[5] Art. 5(2) DSA and Recital 20 DSA.
[6] Recital 18 DSA.
[7] Suggested Recital 20, sentence 2.
[8] In joined Cases C-682/18 and C-683/18, decisions of 22 June 2021, para 108 has to be read in line with para 102.
[9] Art. 24b EP-proposal.

platforms should be considered as playing an “active role” through their design, thus legitimately exempting them from the safe harbour provisions.

We therefore strongly suggest:

- to amend recital 18 of the DSA, e.g. by adding a sentence after recital 18, sentence 1 as follows: “If the platform’s design incentivizes infringements and the operator fails to counter such risks credibly, this indicates an operator’s active role.”
- to support Recital 20, sentence 2 of the General Approach.

2. Art. 7: The wording of the “no-general-monitoring”-rule should not be modified

Art. 7 transfers Art. 15(1) ECD (so called “no-general-monitoring”-rule) into the DSA. However, slight changes with potentially severe consequences come with it. Given the importance of that provision, the wording of Art. 7 should try to exactly reflect the wording of the current Art. 15(1) ECD. Therefore, as in Art. 15(1) ECD, the word “general” in Art. 7 should be repeated to make it unambiguously clear that “general” refers to both obligations: *to monitor* as well as to the obligations *of seeking facts or circumstances*. This would make clear that, as today, in both instances *specific* obligations might still be in line with European Law[10]. Next to that, the EP proposals to modify Art. 7 (especially amendments 139 and 140 for Art. 7(1) and 7(1a)) regarding monitoring obligations should be rejected.

Leaving the reasoning of Art. 15(1) ECD untouched would safeguard that in reasonable cases, specific obligations to prevent illegal content might still arise, in line with the Case Law of the ECJ (Glawischnig v. Facebook ruling of 3.10.2019 – C-18/18) and - even more so - in line with long standing Case Law of national High Courts[11].

From our perspective, such specific obligations to prevent illegal content are crucial. Without such specific and proportionate obligations, victims of illegal content or illegal activities might end up without any reasonable protection. The DSA would put at risk even the very cautious level of protection that European Law offers to victims of online violence and would therefore

[10] For an in-depth discussion of how the wording in Art. 7 might be rooted in ambiguous grounds of the ECJ-Glawischnig-ruling see, Daniel Holznagel, Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act, Computer und Recht, 2021, 123 (126)).
[11] See, e.g. German Federal Court of Justice, cases I ZR 304/01, I ZR 18/04, I ZR 79/12, I ZR 80/12, I ZR 139/08, I ZR 216/11.

increase the struggle of access to justice.

To give an example (The “Künast”-Case against Facebook): Supported by HateAid, Renate Künast (Member of the German Parliament) is suing Facebook, demanding removal of illegal defamatory content (a fake quote attributed to her). Facebook argues that as a general rule, it does not have to take-down or block copies of such content, but that victims could instead notify Facebook of a specific instance of illegal content. This of course would place the burden on the victims to search and report the content over and over again hoping for action. Given that such content spreads quickly and far, fueled by intransparent algorithms and to hidden places like closed groups or private profiles, this leaves the victims with a lifelong burden to track the content down. Meanwhile they have to endure that there is still defamatory content on the platform which they just haven’t found yet. All this while Facebook has the (technological) resources to find the content effortlessly.

As a conclusion therefore, we urge legislators strongly not to inject any (unintended) modifications into the wording of the no-general-monitoring rule:

- Art. 7 should carefully reflect that the word “general” refers to both alternatives (“to monitor” and “to seek”), e.g. by explicitly including the word before every alternative in the text (as is the case now in Art. 15(1) ECD).
- The EP-proposals on narrowing Art. 7 (especially amendments 139 and 140) should be rejected.

3. Art. 17, 18: User redress: Empower all users to act against wrongful platform decisions

Lawmakers should make sure that all users have access to redress mechanisms established under Article 17 and 18, as suggested in the Council General Approach. Asymmetrically limiting access to these crucial mechanisms only to content uploaders would discriminate against users that unsuccessfully report illegal content.

Opening Art. 17 and 18 to redress by notice senders would help platforms to review their decisions. Such review helps to improve quality in content moderation processes. Moreover,

denying access to notice senders could even provide an incentive to weaken the notice and action procedures and to ignore notifications, as these decisions will remain unchallenged.

We understand that one argument against opening Art. 17, 18 to notice senders is the allegedly feared misuse of complaint mechanisms by "bad actors". Platforms already do have tools to address these problems, e.g., through their Terms of Services, by which such abuse can amount to breach of contract. However, abusive behaviour of a few "bad actors" does not legitimise stripping lawful users of appeals mechanisms. We also want to point out that § 3b NetzDG also allows notice-senders to appeal decisions, yet no indications of abusive behaviour at large scale have been reported.

The possibility of misuse needs to be addressed by looking at how automated decision-making works and leads to wrongful content removal and disabling of legit profiles. The misuse is clearly only possible and attractive because of automated decision-making that lacks human oversight. To be clear: misuse by "bad actors" is a result of bad content moderation by online platforms and should not be used to justify stripping users of their right to redress.

4. Recital 33, sentence 2 should be codified and amended

Recital 33 DSA is interpreting Art. 3(2) ECD, which in itself introduces the so-called country-of-origin principle. Therefore, recital 33, sentence 2 is a very important policy decision, as it would exempt cross-border orders (on specific items of illegal content) from the restrictions of the country-of-origin principle. We welcome this policy decision very much, as otherwise Art. 3(2) ECD leads to an unjustified and probably unintended hampering of enforcement[12].

However, we urge legislators to strengthen this important policy decision of recital 33, sentence 2:

[12] In the field of personality rights infringements (illegal hate speech, defamation, doxxing …) the strict country-of-origin principle is hampering enforcement: the free flow of services is protected, while rights enforcement is far from harmonised and very complicated in cross-border matters. It occurs to us that such consequences were unintended. The lawmakers of the ECD obviously didn't think through the consequences for personality rights infringements - opposed to copyrights infringements, which were in the focus back then and rightfully led to the decision to exempt copyright and related areas from the country-of-origin principle, see Art. 3(3) ECD and its annex.

- To prevent any ambiguities, the reasoning should be codified by amending Art. 3 ECD.
- The reasoning should be expanded to cover situations where authorities order account suspensions (a legislative project of the current German Government[13]).
- On the other hand, **the EP-proposal for recital 33, sentence 2 (amendment 30) should be rejected**, as it would jeopardise the central policy decision of recital 33 and could even prove counterproductive: changing the word “do” by “should” could lead to the interpretation that judicial orders on specific content are indeed affecting the country-of-origin-principle and “should” thus fall under its restrictions.

5. Art. 25: Expand VLOP - Risk Mitigation to relevant “smaller” actors to prevent lack of protection, at least in the field of protection of minors

The definition of Very Large Online Platforms (VLOPs) in Art. 25 refers to the number of recipients of a service. However, there might be “smaller” platforms which require similar attention as VLOPs due to the risks they might pose to society. This e.g. applies to platforms targeted at certain groups (e.g. minors) which do not have 45 Mio users within the Union, but, for example 2 Mio users in a given member state and which should be exposed to ambitious regulation. We therefore argue that these platforms should not be per se excluded from meaningful regulation.

As the DSA aims at legal harmonisation across the Union[14] and to introduce a level playing field[15], it is our understanding that member states will not be able to act, even if a smaller platform poses a serious risk to society. Even worse: Existing ambitious legislation will be overruled. One disheartening example is the German Youth Protection Act, which introduces ambitious risk mitigation standards[16] for platforms with 1 Mio (or more) users, and which will have to be suspended under the DSA.

[13] Coalition Treaty, p. 18.
[14] Explanatory Memorandum, recitals 2 and 4.
[15] Recital 7.
[16] § 24a Jugendschutzgesetz.

At least in the field of protecting vulnerable groups (e.g. minors) and in the context of protection against illegal content, the DSA therefore should include the possibility to expose non-VLOP-platforms to the VLOP-regime of the DSA:

- One possible solution would be to expand Art. 25(1) through covering platforms with a significant number of users in a single member state (e.g., 1 Mio), or
- Another option is to allow the European Board for Digital Services to expand the VLOP-regime by majority decision onto platforms which cause significant societal risks.

This amendment would align with Germany's Statement on the Council General Approach to "safeguard the current high domestic standard based on international requirements … concerning the protection of minors in the media. Under any circumstances, this must be guaranteed by the DSA, particularly through relevant derogation options."

6. Art. 10a: Points of contact: enabling effective communication with users

Points of contact that are accessible not only to authorities but also to recipients of the service are particularly important**.** Although the EP suggests such points of contact (Amendment 180), the Article 10a (new) should be further strengthened to make contact points useful for victims of online violence**.**

For the contact points to serve consumers, they need to be meaningful and accessible. Meaningful implies that users can communicate with online platforms, and this communication does not solely rely on chatbots and automated replies. Furthermore, for accessibility, considering the language diversity across the EU, VLOPs should make sure that users can communicate with their contact points in all the official languages of the EU. It can be especially important for contact point accessibility to younger and older users, as well as minorities.

Moreover, the contact points for users should also serve for delivery of official documents, e.g., evidence or formal requests that are made to initiate legal proceedings.

7. Art. 28: Auditors play a crucial role. They should not be selected by the platforms

For Very Large Online Platforms, the DSA relies heavily on independent auditors to investigate platform functions, behaviours and risks, how to achieve compliance and how to mitigate risks facilitated through platforms (Art. 28). Given the crucial role that the DSA gives to auditors, their independence is of utmost importance. Auditors will be "gatekeepers of finding risks and non-compliance by the platforms", but they will also be gatekeepers of NOT finding risks. As a bare minimum, it must be clarified that not the platforms, but authorities select the auditors. Given our experience with some Member States being very reluctant to initiate meaningful proceedings against platforms, and given that auditors are expected to be as independent as possible, auditors should neither be selected by the platforms, nor the Digital Services Coordinator, but the Board.

8. Art. 41: Enable enforcement against fundamentally non-compliant platforms (e.g. Telegram)

The DSA does not provide effective solutions for enforcement when an intermediary service is fundamentally non-compliant, and when it has no assets or representatives accessible within the Union (so standard enforcement measures are likely to fail). A not so theoretical example might be the service "Telegram".

The draft DSA envisions a power to request termination of access to a service (Art. 41(3)(b)), which might be seen as a minimum-solution against fundamentally non-compliant providers. However, this provision sets very high bars for such a step: the infringement in question must entail a serious criminal offence involving a threat to the life or safety of persons. Given the harmonising nature of the DSA, it is very questionable whether member states could still introduce similar enforcement measures against services which are simply fundamentally non-compliant (e.g., for years ignoring any orders, not implementing the DSA). Moreover, European law does not explicitly explain on which grounds termination of access should be ordered and how it should be enforced. The European Court of Justice has solely clarified that (access) providers might be ordered to deny access to certain infringing services (see cases C-314/12 and C-484/14). Finally, measures by access providers might not always be most effective. Therefore, the DSA should include other options than termination service.

One can think of involving third parties which are in a factual or contractual position to affect a given non-compliant platform. E.g., financial or payment providers (PayPal, Visa), app stores, or technical services providers might be in such positions. As a theoretical example for a measure of last resort, courts might require AppStores to delete the App of a fundamentally non-compliant service or a Court might prohibit advertising partners to engage with such a platform.

We therefore suggest that the DSA should allow the inclusion of third parties in enforcement measures against fundamentally non-compliant services. As the affected third parties are not involved in the infringement but requested to provide emergency relief as a means of last resort (innocent third parties), measures must be strictly proportionate and require high procedural safeguards (e.g. a court order specifying the supportive measures). In specific cases, this might require that third parties receive financial compensation for supporting enforcement.

9. Art. 19: Trusted Flaggers: cut the red tape for NGOs who are trusted flaggers

An effective system of trusted flagging heavily relies on the civil society - often publicly or donor funded NGOs, like HateAid, that have the best incentives to become a trusted flagger. These are organisations with expertise in the respective field, justifying the trust that is put into trusted flaggers.

It is important not to overburden NGOs: too strict requirements for the application process, regarding expertise and following reporting obligations may deter them from becoming a trusted flagger and from fulfilling these functions. Some of the requirements introduced under Amendment 249 of the EP's position are disproportionate and burden NGOs with extensive reporting obligations. This kind of obligations could be especially challenging to fulfil, considering scarcity of funding that many NGOs face or the problem that NGO grants often are designated for a specific purpose, leaving no flexibility for extra tasks. An NGO like HateAid would not have sufficient resources to meet all the requirements suggested by the EP in Amendment 249 and therefore HateAid most likely would not even apply under these circumstances.

Instead, we suggest shifting the burden of reporting requirements concerning functioning of trusted flaggers from NGOs to online platforms, who could easily generate this information (as they have to keep track for their transparency reporting anyway).