8 September 2021

Expert Paper and Policy Proposals

Safeguarding adequate rights enforcement through the Digital Services Act (DSA)

by

Daniel Holznagel

Preface

The European Union is rushing forward with the proposal for a Digital Services Act (COM(2020) 825 final), which will define the online legal framework for years to come.

One main objective of the Digital Services Act (DSA) is to establish a powerful and clear accountability framework for online platforms regarding action against illegal activities, on how to ensure transparency and on how to safeguard users' rights.

This is important. Because today, citizens as well as regulators are in a weak position when they want to hold platforms accountable.

However, in that regard, the current draft of the DSA does not include ambitious improvements. In some areas, the DSA might even slow down enforcement against non-compliant platforms. This is concerning, as in the field of the DSA, we are dealing with gigantic platforms which have unprecedented impact on our citizens, societies, democracies and economies. It is also worrisome that the Council Presidency compromise texts of 4 and 16 June 2021 only attempt to introduce tiny improvements. The draft reports from the European Parliament pick up some of the issues discussed here, but only to a little extent.

Overall, strengthening enforcement through the DSA needs way more attention and major improvements are necessary. In particular, the DSA's focus on how to tackle the spread of illegal content and how to to counter infringements should be improved. We should put citizens and regulators in a position to effectively enforce rights and rules when platforms are non-compliant.

This report suggests specific amendments to the DSA to reach that goal. It specifically focuses on how to strengthen enforcement, oversight, remedies and litigation.

The Author:

Daniel Holznagel works as a judge. From 2017 to 2021 he was a Legal Officer at the German Federal Ministry of Justice and Consumer Protection, where he was involved in drafting the German Network Enforcement Act (NetzDG) and steering the proceeding leading to the first administrative fine under the Act. He regularly advises HateAid and other NGOs on online platform liability issues. Views in this report are his own and do not necessarily reflect those of the experts/organizations acknowledged below.

Acknowledgements:

The author would very much like to thank all experts who shared valuable feedback, ideas and intellectual input (alphabetical order): Josephine Ballon (HateAid), Jutta Croll (Stiftung Digitale Chancen), Mauritius Dorn (Institute for Strategic Dialogue), Julian Jaursch (Stiftung Neue Verantwortung), Johannes Rabe, Alexander Ritzmann (Counter Extremism Project), Melissa Sayiner, Dan Shefet (Cabinet Shefet).

Summary

1. Scope and Definitions

1.1. The DSA should be lex specialis to the AVMSD. This will prevent messy oversight for video content (Art. 1).

1.2. The definition of illegal content needs to be clear and in line with the concept of jurisdiction (Art. 2).

2. Effective Notice and Action

2.1 The DSA should require very clear and user-friendly reporting mechanisms (Art. 14).

2.2 A due diligence obligation should ensure systematic take-down of illegal content (Art. 14).

3. Effective Litigation, Remedies and Prosecution

3.1 The so-called active-role principle should be clarified so bad actors (e.g. "revenge porn" platforms) cannot hide behind liability exemptions (recital 18).

3.2 The wording of the "no-general-monitoring"-rule should not be modified (recital 28, Art. 7).

3.3 Legal representatives should also benefit citizens, not only authorities. Failure to mandate must have consequences. VLOPs should accept documents in all Union languages (Art. 11).

3.4 Notifications to authorities should cover relevant cases (Art. 21).

3.5 Legal representation through organizations should cover all rights resulting from a violation of the DSA (Art. 68).

3.6 Access to Representative Actions should be clarified.

3.7 Compensation for non-material damages should be available.

3.8. The DSA should not determine jurisdiction of Courts (Art. 40).

4. Mindful Transparency and Data Access

4.1. Transparency reporting by platforms should include revenues generated from illegal content (Art. 23).

4.2. Data access must respect the Nemo Tenetur - principle (right to silence) and should strengthen its focus on illegal content (Art. 33).

5. Effective Risk Mitigation

5.1. The Board should have the power to expose platforms with high impact on democratic discourse to the VLOPs - regime (Art. 25).

5.2. Risk assessment should cover risks to gender equality (Art. 26).

5.3. Auditors must be selected and paid for by authorities, not the platforms themselves (Art. 28).

6. Effective Regulatory Oversight

6.1 For reasons of legal certainty, recital 33 (by which orders regarding specific content are exempted from the country-of-origin principle) should be codified (recital 33, Art. 71).

6.2. Allow destination-country Member States to pick jurisdiction in specific cases (Art. 40).

6.3 For VLOPs, the burden of oversight should be shared amongst all Member States, with the Commission providing guidance (Art. 40).

6.4 Third parties should be included in enforcement against fundamentally non-compliant platforms (Art. 41).

6.5 Oversight proceedings should not overcomplicate. Certain steps can be voluntary (Art. 50).

6.6 Commission interruption in oversight must make sense: The Commission might intervene after member state level proceedings, it must do so only on appeal of the Board or other Member States (Art. 50, 51).

1. Scope and Definitions

1.1. The DSA should be lex specialis to the AVMSD. This will prevent messy oversight for video content (Art. 1).

Article 1(5)(b)	
Commission text	Suggestion
5. This Regulation is without prejudice to the rules laid down by the following: (a) … (b) Directive 2010/13/EC; (c) ….	5. This Regulation is without prejudice to the rules laid down by the following: (a) **(b)~~Directive 2010/13/EC;~~** (c) ….

Explanation:

According to Art. 1(5(b), the DSA will be without prejudice to the Audiovisual Media Services Directive (2010/13/EC) = AVMSD, which is to be considered lex specialis (Recital 9 DSA).

This would create problems:

In its Art. 28a and Art. 28b, the AVMSD introduces due diligence obligations for video sharing platforms (VSPs), including obligations to provide reporting (flagging) mechanisms and to protect the public from certain illegal videos. These topics find better, more specific, and more ambitious regulation in the DSA.

But since the AVMSD is more specific on which platforms (VSPs) and which content (video) are covered, it is fair to assume that for such matters, the AVMSD will be lex specialis (this can also be concluded from the DSA Explanatory Memorandum and recital 9).

As a consequence, oversight gets messy. An easy example: YouTube and TikTok qualify as VSPs. Thus, any non-compliance regarding their reporting mechanisms and measures against illegal content will fall under different legal regimes. Different authorities will be in charge, different proceedings and sanctions apply, depending on whether we look at reporting or measures against either video or any other content.

The whole situation gets way more complicated when you consider social networks where video content is not the principal purpose of the service, but is clearly a substantial functionality. The VSP-definition is ambiguous and vague regarding such mixed platforms (Facebook is a prime example). The European Commission tried to clarify this with guidelines, but the guidelines are far from clear in themselves. This will play out as multiple lines of defense for the platforms, making the AVMSD a "platform lawyer's dream" for defending against measures under the DSA whenever video content is involved.

Therefore, Art. 1(5(b) DSA should be deleted. Making the DSA the leading regulation in this field will ensure clarity for platforms and regulators and will prevent that the AVMSD becomes a major bottleneck for enforcement (the EU should not stumble over its own feet).

1.2. The definition of illegal content needs to be clear and in line with the concept of jurisdiction (Art. 2).

Article 2(g)	
Commission text	Suggestion
(g) 'illegal content' means any information,, which, in itself or by its reference to an activity, including the sale of products or provision of services is not in compliance with Union law or the law of a Member State, irrespective of the precise subject matter or nature of that law;	(g) 'illegal content' means any information,~~,~~ which, in itself or by its reference to an activity, including the sale of products or provision of services is – not in compliance with Union law or – ~~**the law of a Member State,**~~ ***for the purposes of Chapter III and IV of this Regulation, the law of a Member State that has jurisdiction, otherwise the law of any member state*** irrespective of the precise subject matter or nature of that law;

Explanation:

The definition of 'illegal content' is crucial for the application of the DSA. But the current definition in Art. 2(g) raises major uncertainties and questions:

Since Art. 2(g) refers to the law of a (!) Member State, the definition must be interpreted in a broad way to refer to any (!) Member State here. If so, then any content that is illegal by the laws of a single or a few Member States would have to be deemed illegal, irrespective of whether the content is deemed legal by the laws of other Member States or even the laws of the Member State which has jurisdiction (Art. 40 DSA).

Example: Holocaust denial is illegal in Germany, but legal in other Member States. For the purposes of Art. 20(1) DSA (suspension of repeat infringers), will Facebook (established in Ireland) have to "count" repeated posts of Holocaust denial? Must the Irish Digital Services Coordinator, due to his jurisdiction (Art. 40(1) DSA), sanction Facebook if the platform fails to suspend accounts of users who repeatedly post Holocaust denial content?

Art. 40 (1) does not yield an answer to this question, it only clarifies which Digital Services Coordinator will be in charge, not what will be the standard for illegality. Art. 3(2) E-Commerce Directive will not help either, as Art. 2(g) DSA would probably trump Art. 3(2) E-Commerce Directive here.

It seems unlikely that such an outcome (Ireland has to take into account German Holocaust denial illegality) is in line with the intention of the DSA.

Therefore, for the purposes of Chapter III and IV, illegality of content through non-compliance with Member State laws should be limited to Member States which have jurisdiction. For other purposes, the definition must stay as it is. This is crucial as otherwise the scope of the liability exemptions in

Chapter II would be restricted as well. The underlying problem is complex: The liability exemptions in Chapter II protect services - a broad definition of illegal content here is helpful for services, in line with the common understanding of the liability exemptions in the E-Commerce Directive and legitimate. The due diligence obligations in Chapters III and IV restrict services - a broad definition of illegal content burdens services here and might go too far (see above, therefore the suggested changes).

2. Effective Notice and Action

2.1 The DSA should require very clear and user-friendly reporting mechanisms (Art. 14).

Article 14(1), (1a)	
Commission text	Suggestion
1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, user-friendly, and allow for the submission of notices exclusively by electronic means.	1. Providers of hosting services shall put mechanisms in place to allow any individual or entity to notify them of the presence on their service of specific items of information ***or activity*** that the individual or entity considers to be illegal content. Those mechanisms shall be easy to access, ***clearly visible, low-threshold,*** user-friendly, and ***located close to the content in question. They should*** allow for the submission of notices exclusively by electronic means. ***1a. The Commission is empowered to adopt delegated acts to lay down specific requirements regarding the mechanisms as mentioned in paragraph 1.*** ***1b. Providers of hosting services shall be encouraged to develop best practice industry standards for mechanisms as mentioned in paragraph 1.***
Explanation: *Art. 14 (1) DSA is a relevant provision to strengthen provider accountability. Since a similar provision was introduced in § 3(1) of the German Network Enforcement Act (NetzDG), lessons learned from there should be taken into account: Under the NetzDG, some platforms introduced complex and obscure reporting mechanisms, which were hard to find. This resulted in a low number of NetzDG-complaints. Moreover, the reporting mechanisms introduced were in addition/parallel to already existing reporting flows, in parts confusing users which channel/button/form would allow them to submit a NetzDG-complaint leading the platform to treat the complaint according to this law. Therefore, Art. 14(1) DSA should require very clear and user-friendly reporting mechanisms.* *Moreover, the Commission should be in a position to specify requirements via delegated acts, Art. 14 (1a). Art. 14(1b) DSA aims at supporting best practice industry standards (e.g. using a common "flag"-symbol).*	

2.2 A due diligence obligation should ensure systematic take-down of illegal content (Art. 14).

Article 14(3a)	
Commission text	Suggestion
	3a. The provider shall maintain an effective procedure to ensure that upon obtaining knowledge or awareness of illegal content through notices that include the elements referred to in paragraph 2, it can act expeditiously to remove or to disable access to the illegal activity or content and to prevent reappearance.

Explanation:

The Commission proposal refrains from determining a due diligence obligation to remove or block illegal content after receiving knowledge.

Therefore, it is suggested to introduce a due diligence obligation to ensure that illegal content is taken down upon obtaining knowledge (and, in line with Art. 7, reappearance is prevented). The provision is constructed as a compliance rule, so only systematic failure to take down content will be sanctionable. This is a safeguard to prevent overblocking: since mistakes in a single case will not lead to a sanction, providers are not over-incentivized to take-down content (NetzDG-model).

Without such a due diligence obligation, the DSA might turn out too weak in its acttion against illegal content. One has to bear in mind that Art. 20(1) DSA (due diligence obligation to act against repeat infringers) is the only other meaningful due diligence obligation with a focus on action against illegal content (besides Art. 27 for VLOPs). But Art. 20(1) might prove far less effective than expected: Art. 20(1) creates high thresholds before an account suspension must be implemented (repeat manifest infringements). This is totally legitimate due to the heavy-weight fundamental rights implications that come with account suspensions. But besides this, Art. 20(1) will be hard to enforce due to several reasons. First, platform decisions to suspend an account can be challenged by attacking every single assessment of the multiple infringements in question. Second, platforms must keep track of past infringements to "count" incidents. This implies risks for platforms due to unsolved data protection issues here. Moreover, once a user is suspended, they would have to keep track of the (suspended!) user to prevent circumvention (parallel accounts). The prediction of a weak Art. 20(1) can also rely on historical lessons: The U.S. Copyright Act includes a repeat-infringer-rule in its liability exemptions (Sec. 512(i)(1)(A)) which does not prove effective due to similar circumstances as described here. This has nothing to do with flaws of Art. 20(1), but the fact that repeat infringer rules can hardly be designed as a strong enforcement measure.

3. Effective Litigation, Remedies and Prosecution

3.1 The so-called active-role principle should be clarified so bad actors (e.g. “revenge porn” platforms) cannot hide behind liability exemptions (recital 18).

Recital 18 DSA	
Commission text	Suggestion
The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally, by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.	The exemptions from liability established in this Regulation should not apply where, instead of confining itself to providing the services neutrally, by a merely technical and automatic processing of the information provided by the recipient of the service, the provider of intermediary services plays an active role. ***Indicators for such an active role might be found where a provider plays a role allowing it to have knowledge or control of the data stored or where the design of its service substantially contributes to or incentivizes infringements or where the provider actively shields users from rights enforcement.*** ~~**of such a kind as to give it knowledge of, or control over, that information. Those exemptions should accordingly not be available in respect of liability relating to information provided not by the recipient of the service but by the provider of intermediary service itself, including where the information has been developed under the editorial responsibility of that provider.**~~

Explanation:

Recital 18 of the DSA incorporates a concept of the European Court of Justice (ECJ): The liability exemptions (Art. 12 - 15 E-Commerce Directive) do not apply to providers which play an “active role”.

However, the ECJ never found an opportunity to explain this concept in further detail. Accordingly, national courts struggle to apply the concept.

Unfortunately, recital 18 DSA “codifies” a very narrow and static interpretation of the “active role” - principle, basically requiring knowledge and control over specific content to establish an “active role” of a platform. Such a narrow interpretation of an “active role” will render the concept meaningless. Modern bad actor platforms never have specific knowledge or control, because they inherently turn a blind eye. This will overprotect bad actors: e.g., revenge porn -, child exploitation and abuse material -, or darknet - platforms.

Moreover, in its recent ruling regarding Cyando and YouTube, the ECJ can be understood in a way that not only “knowledge or control” might qualify a host provider as having an “active role”

exempting it from the safe harbour provisions. Instead, the Court argued that the liability exemptions cannot apply when "communication to the public" (Art. 3(1) of the Copyright Directive 2001/29/EC) is to be found (decision of 22 June 2021, C-682/18 and C-683/18, YouTube/Cyando, par. 108 referring to paras 105 and 106). But the court argues that "communication to the public" might be established from factors well beyond "knowledge or control", e.g. through a platform's (financial) design encouraging users to infringe copyrights (deliberate nature of that platform, para 101). This implies that in such cases, based on the platform's design and beyond the question of knowledge and control, it can be argued that the liability exemptions are not applicable. Therefore, providers might play an active role through their platform-design, irrespective of whether they have knowledge and control over specific infringing content.

Such an interpretation must be very much welcomed as it would exempt bad actor platforms from the safe harbour provisions. Unfortunately, recital 18 would override this more flexible interpretation through a narrow and static definition of "active role".

Therefore, in line with ECJ-jurisprudence, we should opt for a more open language of the "active role" - test, to allow courts to decide on a case-by-case basis whether a platform's design

1. *is promoting, incentivizing or substantially contributing to infringements (e.g. porn platforms allowing anonymous postings and hashtags like "exposed", "hidden cam" or "teen"), or*

2. *does create substantial barriers for enforcement against the direct infringers (e.g. by actively wiping out traces to identify infringers even after manifest infringements).*

Note that such an "active role" concept would in no way determine liability as such. It would merely exclude bad actors from the safe harbour provisions, thus exposing such bad actors to "normal" liability, which still would have to be established by the "normal" doctrines of tort law.

<u>Note on similar proposals</u>: Some proposals suggest that the availability of the liability exemptions should be linked to compliance with the due diligence provisions of the DSA (Amendments 264, 265, 747 in IMCO draft report of 8.07.2021, 2020/0361(COD)). Such proposals seem logical at first glance. However, the connection / causation between threshold (comply with DSA Due Diligence) and protection (liability exemption) seems questionable. E.g., not to comply with transparency obligations does not justify being excluded from liability exemptions in, say, a trademark tort law case against an online platform. Moreover, such abstract and broad threshold (compliance with all (!) due diligence) might overcomplicate proceedings. An example: In civil proceedings, e.g., a trademark case against an online platform, the platform raises the defense of Art. 5 DSA. The court then would have to decide whether or not this defense is available. If Art. 5 DSA would be linked to all (!) due diligence of the DSA, the court might have to examine all these provisions implicitly, which is not practical and hard to justify.

3.2 The wording of the "no-general-monitoring"-rule should <u>not</u> be modified (recital 28, Art. 7).

Recital 28	
Commission text	Suggestion
Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.	Providers of intermediary services should not be subject to a monitoring obligation with respect to obligations of a general nature. This does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislation, in accordance with the conditions established in this Regulation. Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or ***general*** active fact-finding obligation, or as a general obligation for providers to take proactive measures to relation to illegal content.
Art. 7	
Article 7 No general monitoring or active fact-finding obligations No general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.	Article 7 No general ~~monitoring or active fact-finding~~ obligation~~s~~ ***to monitor*** No general obligation to monitor the information which providers of intermediary services transmit or store, nor ***a general obligation*** actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.
<u>*Explanation*</u>*:* *Art. 7 transfers Art. 15(1) E-Commerce Directive (so called "no-general-monitoring"-rule) into the DSA. However, while doing so, slight changes come with it. Given the importance of that provision, the slight changes that come with the wording of Art. 7 should be reviewed. The wording of Art. 7 should try to exactly reflect the wording of the current Art. 15(1) E-Commerce Directive.* *Art. 15(1) E-Commerce Directive establishes the so-called "no monitoring obligation" rule. This rule is of utmost importance as it limits all measures of rights enforcement, be it through civil litigation, orders of the competent authorities or through court orders.*	

So far, Art. 15(1) E-Commerce Directive is a success. It protects platforms from overreaching filter-obligations (see, e.g. ECJ cases C-70/10 and C-360/10). On the other hand, Art. 15(1) gave courts the flexibility to introduce limited filter obligations in specific cases. E.g., the German Federal Court of Justice has delivered numerous decisions requiring big platforms to take proportionate measures to specifically prevent "similar" content after after being notified of illegal content (see, e.g. Bundesgerichtshof, 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).

One might argue that in its Glawischnig v. Facebook ruling of 3.10.2019 – C-18/18, the ECJ interpreted Art. 15(1) E-Commerce Directive quite narrowly. Even if that was the case, it is best to leave the "no monitoring" - rule in its current state and interpretation left to future courts. This is of extra relevance as nothing in the Commission text indicates that modifications were intended.

3.3 Legal representatives should also benefit citizens, not only authorities. Failure to mandate must have consequences. VLOPs should accept documents in all Union languages (Art. 11).

Article 11(2) and (6)	
Commission text	Suggestion
2. Providers of intermediary services shall mandate their legal representatives to be addressed in addition to or instead of the provider by the Member States' authorities, the Commission and the Board on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation. Providers of intermediary services shall provide their legal representative with the necessary powers and resource to cooperate with the Member States' authorities, the Commission and the Board and comply with those decisions.	2. Providers of intermediary services shall mandate their legal representatives to be addressed in addition to or instead of the provider by the Member States' authorities, the Commission and the Board on all issues necessary for the receipt of, compliance with and enforcement of decisions issued in relation to this Regulation***; moreover, they shall mandate their legal representatives to be addressed by third parties, including recipients of services on all issues necessary for litigation and enforcement of rights following from the application of this Regulation, including rights following from decisions not to take decisions according to this Regulation.*** Providers of intermediary services shall provide their legal representative with the necessary powers and resource***s*** to cooperate with the Member States' authorities, the Commission and the Board and comply with those decisions. ***Where a provider fails to properly mandate its legal representative, proper mandate shall be assumed in favour of a party serving documents. Where a provider fails to designate a legal representative, Member States shall allow service through public notification.*** 3. … (unmodified) … 4. … 5. … ***6. Art. 8(1)(a) of Regulation (EC) 1393/2007 shall not apply to very large online***

	platforms if the relevant documents are written in one of the official languages of the Union.

Explanation:

Art. 11 DSA should be expanded to make sure that legal representatives will not only help authorities and the Commission to communicate with third country providers, but citizens should benefit as well.

Effective solutions are necessary where providers fail to designate and/or mandate a legal representative. Failure to do so must not only result in sanctions. Way more effective, failure to mandate must result in fiction of a proper mandate, so documents can be served (even if the provider refuses service). Total non-compliance (no legal representative at all) must result in enabling service through public notification.

In the past, we have seen service of documents slowed down as even big platforms refused to accept a document arguing they would not understand its language, a situation which would allow for refusal to accept documents according to Art. 8(1)(a) of Regulation (EC) No 1393/2007. Indeed even large platforms argue so (e.g. Munich Court of Appeals, decision of 14.10.2019 – 14 W 1170/19, para 37). This leads to ridiculous outcomes, when a platform with millions of users in a given member state through a country specific website (in the member state language) argues not to understand the given language as soon as users want to pursue their rights through litigation. Therefore, at least for very large platforms, Art. 8(1)(a) of Regulation (EC) No 1393/2007 should not apply, as long as the relevant documents are in one of the official languages of the Union.

3.4 Notifications to authorities should cover relevant cases (Art. 21).

Article 21(1)	
Commission text	Suggestion
1. Where an online platform becomes aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available.	1. Where an online platform becomes aware of any information giving rise to a suspicion that a ~~***serious***~~ criminal offence involving a threat to the life or safety of persons has taken place, is taking place or is likely to take place, it shall promptly inform the law enforcement or judicial authorities of the Member State or Member States concerned of its suspicion and provide all relevant information available. 2. … ***3. This Article does not restrict online platforms in voluntarily notifying authorities in other cases.***

Explanation:

Art. 21(1) introduces a very narrow obligation of when platforms will have to inform authorities of criminal offences. The DSA only envisions notification in cases of danger, for the purposes of preventing serious harm. At the same time, Art. 15(2) of the E-Commerce-Directive will be given up (see Art. 71(1) DSA), so Member States may no longer establish obligations for information society service providers to inform the competent public authorities in other cases.

This is a relevant policy decision. Only when threats to persons are involved, platforms might be required to notify. This might be a good policy decision or not. However, if notification obligations are restricted to criminal offences involving threats to persons, it should not be mandatory that the "seriousness" of the criminal offences is established. Such a threshold will create legal uncertainties to platforms. Moreover, it is hard to justify that platforms shall not notify when information amounts to a "normal" criminal offence (!) involving a threat to life or safety of a person (!).

Moreover, it should be clarified that platforms are free to decide (as any citizen) to notify authorities in case they suspect any kind of criminal behaviour.

3.5 Legal representation through organizations should cover all rights resulting from a violation of the DSA (Art. 68).

Article 68	
Commission text	Suggestion
Without prejudice to Directive 2020/XX/EU of the European Parliament and of the Council 52 , recipients of intermediary services shall have the right to mandate a body, organisation or association to exercise the rights referred to in Articles 17, 18 and 19 on their behalf, provided the body, organisation or association meets all of the following conditions: (a) it operates on a not-for-profit basis; (b) it has been properly constituted in accordance with the law of a Member State; (c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.	Without prejudice to Directive 2020/XX/EU of the European Parliament and of the Council 52, recipients of intermediary services shall have the right to mandate a body, organisation or association to exercise the rights referred to in Articles 17, 18 and 19 ***and all other rights and claims, including monetary relief and damages, resulting from decisions taken with regard to this Regulation,*** on their behalf, provided the body, organisation or association meets all of the following conditions: (a) it operates on a not-for-profit basis; (b) it has been properly constituted in accordance with the law of a Member State; (c) its statutory objectives include a legitimate interest in ensuring that this Regulation is complied with.
Explanation: *Art. 68 strengthens a legitimate policy concern. It will enable NGOs and other organizations which have the necessary expertise and resources to support online users when it comes to litigation with intermediary services concerning users' rights.* *The scope of Art. 68 should be expanded to cover all violations of the DSA causing harm to recipients: Representation of recipients through Art. 68 should also cover claims for monetary relief following platform decisions. It should also include situations where a platform refuses to take a decision referred to in Articles 17, 18 and 19. Moreover, it should be expanded to the application of the Regulation as such. E.g., one can imagine users' rights resulting from platform decisions to terminate accounts (Art. 20(1)). In such a situation, citizens should be in a position to mandate a body mentioned in Art. 68.*	

3.6 Access to Representative Actions should be clarified.

Recital 100a (new)	
Commission text	Suggestion
	The due diligence obligations for a transparent and safe online environment as laid down in Chapter III of this Regulation aim at ensuring a safer and more transparent online environment for consumers and citizens. Infringement of these obligations therefore will harm or may harm the collective interests of consumers, Art. 2(1) (EU) 2020/1828. As a consequence, qualified entities in the meaning of Directive (EU) 2020/1828 should be in a situation to bring representative actions before courts or administrative authorities. This will include the right to seek injunctive measures aiming at bringing an intermediary service into conformity with this Regulation. This Regulation does not affect or establish procedural law applicable, including the questions of recognition and jurisdiction.

Explanation:

Art. 72 of the draft DSA adds the DSA to the Annex of Directive (EU) 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers. Art. 72 DSA is very much to be welcomed and should be defended against possible industry interests lobbying otherwise.

Art. 72 is of prominent importance as Art. 68 will "only" help specific recipients to be represented when pursuing subjective rights (the right of a certain recipient to have "her" content/account reinstated). Therefore, powers of representing bodies/organisations according to Art. 68 will be limited to act within the boundaries of the subjective rights that the represented recipient might be entitled to. By common understanding, such rights would only offer limited recourse where specific harm has been caused to that recipient. It is not self-evident, that, absent such harm, recipients would have rights to require the service to be brought into conformity in the first place even if the intermediary service violates the Regulation (Art. 7, 8 and 14(1) of Directive (EU) 2019/770 might be interpreted to grant such rights. But it seems far from clear whether non-compliance with the DSA would amount to non-conformity as referred to in Art. 8(1) (EU) 2019/770).

However, Art. 72 DSA will help: Qualified entities then are entitled to seek injunctive relief against infringements of the DSA, Art. 7(4) (EU) 2020/1828, which means to seek definitive measures to cease an infringing practice or, where appropriate, to prohibit an infringing practice, Art. 8(1)(b) (EU) 2020/1828. However, there is a threshold to such actions: The infringement (in our case: of the DSA) must be of such nature to "harm or may harm the collective interests of consumers", Art. 2(1) (EU) 2020/1828. It must be expected that intermediary services will raise this defense with much effort. Therefore, to make sure that representative action can take place and is not slowed down at

practical level, the recitals of the DSA should make it unambiguously clear that (in doubt) any violation of the DSA's due diligence obligations does indeed harm (or may harm) collective interests of consumers (as is a threshold for representative actions under Art. 2(1) of Directive (EU) 2020/1828).

To prevent misunderstandings, it should be made clear that existing Union law and private international law govern the procedural aspects of the representative actions, especially regarding the question of jurisdiction, see recital 21 of (EU) 2020/1828.

3.7 Compensation for non-material damages should be available.

Article 68a	
Commission text	Suggestion
	Any person who has suffered material or non-material damage as a result of an infringement of this Regulation by a provider of intermediary services shall have the right to receive compensation from the provider for the damage suffered.

Explanation:

While most legal regimes will acknowledge financial compensation for material damages suffered through infringements of the DSA by providers of intermediary services, such material damages and a sufficient causation might often be hard to prove or little in their amount.

Therefore, it should be guaranteed that affected individuals can receive fair compensation even for non-material damages. Such compensation might incentivize affected citizens to sue for respective damages. This is legitimate. It will also serve an overall goal, which is to pressure major online services towards compliance of the law. Such pressure should be highly welcomed, especially as the current draft of the DSA does not put regulators in a position to effectively pressure services towards compliance through administrative sanctions.

3.8. The DSA should not determine jurisdiction of Courts (Art. 40).

Article 40	
Commission text	Suggestion
1. The Member State in which the main establishment of the provider of intermediary services is located shall have jurisdiction for the purposes of Chapters III and IV of this Regulation.	1. The Member State in which the main establishment of the provider of intermediary services is located shall have jurisdiction for the purposes of Chapter***s III and*** IV of this Regulation.
2. A provider of intermediary services which does not have an establishment in the Union but which offers services in the Union shall, for the purposes of Chapters III and IV, ...	2. A provider of intermediary services which does not have an establishment in the Union but which offers services in the Union shall, for the purposes of Chapter***s III and*** IV, ...
3. Where a provider of intermediary services fails to appoint a legal representative in accordance with Article 11, all Member States shall have jurisdiction for the purposes of Chapters III and IV. ...	3. Where a provider of intermediary services fails to appoint a legal representative in accordance with Article 11, all Member States shall have jurisdiction for the purposes of Chapter***s III and*** IV. ...
4. ...	4. ...

Explanation:

The DSA (rightfully) neither aims to establish additional rules on private international law relating to conflicts of law nor does it deal with the jurisdiction of Courts. This should be clarified. The rules of jurisdiction in Art. 40 obviously aim at determining which Digital Services Coordinator is in charge (and which is not). However, by mentioning Chapter III, the DSA could be interpreted in a way to also govern jurisdiction of Courts (!) for private litigation enforcing rights following from platform decisions according to Chapter III (e.g., a dispute between a recipient and a platform regarding the application of Terms and conditions, Art. 12; or even when such rights are enforced through representative action, Art. 72).

Nothing in the DSA hints at such an intention, which would also in no way be legitimate, burden consumers, might have unintended consequences and is also not in line with the concept of the E-Commerce-Directive (see recital 23 and Art. 3 of Directive 2000/31/EC). It is true that some provisions of Chapter III require specification of the Digital Services Coordinator in charge (e.g., who certifies according to Art. 18(2)). However, this does not require to mention Chapter III in Art. 40, because within Chapter III, provisions specify the competent Digital Services Coordinator (see, e.g., Art. 18(2): Digital Services Coordinator of establishment).

4. Mindful Transparency and Data Access

4.1. Transparency reporting by platforms should include revenues generated from illegal content[1] (Art. 23).

Article 23(1)	
Commission text	Suggestion
1. In addition to the information referred to in Article 13, online platforms shall include in the reports referred to in that Article information on the following: (a) ... (b) … (c) ...	1. In addition to the information referred to in Article 13, online platforms shall include in the reports referred to in that Article information on the following: (a) ... (b) … (c) … ***(d) an estimation of the page impressions that included illegal content and estimations of turnover and revenues generated through illegal content and an explanation of the basis and methodology for determining these data.***

Explanation:

Online platforms often make it very clear that they do not want to generate revenues through abusive behaviour of their users, e.g., the spread of illegal content. Such statements are highly welcomed, as well as initiatives of advertisement customers not to invest advertisement budgets on online platforms which attract user activity through the spread of illegal hate speech. Moreover, everyday users might want to make informed decisions on which platforms they want to use based on the fact whether those platforms are resisting economic incentives to profit from illegal content.

To foster such intentions and initiatives and to allow all contractual partners of online platforms to make better informed decisions, online platforms should provide transparency data on the extent of how they are profiting (intentionally or not) from illegal content and in how far they were not able to prevent respective page impressions. Such data might also help understand how companies get better in their voluntary efforts to act against illegal content.

[1] Concept based on a suggestion by Dan Shefet

4.2. Data access must respect the Nemo Tenetur - principle (right to silence) and should strengthen its focus on illegal content (Art. 33).

Article 31	
Commission text	Suggestion
1. Very large online platforms shall provide the Digital Services Coordinator of establishment or the Commission, upon their reasoned request and within a reasonable period, specified in the request, access to data that are necessary to monitor and assess compliance with this Regulation. That Digital Services Coordinator and the Commission shall only use that data for those purposes. 2. Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1). 3. … 4. In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.	1. Very large online platforms shall provide the Digital Services Coordinator ~~***of establishment***~~ ***which has jurisdiction*** or the Commission, upon their reasoned request and within a reasonable period, specified in the request, access to data ~~***that are necessary to monitor and assess***~~ ***on measures taken to ensure*** compliance with this Regulation. That Digital Services Coordinator and the Commission shall only use that data for ~~***those***~~ ***the*** purposes ***of the cessation of an infringement of this Regulation***. 2. Upon a reasoned request from the Digital Services Coordinator of establishment or the Commission, very large online platforms shall, within a reasonable period, as specified in the request, provide access to data ***in a machine-readable and interoperable format*** to vetted researchers who meet the requirements in paragraphs 4 of this Article, for the sole purpose of conducting research that contributes to the identification and understanding of systemic risks as set out in Article 26(1)***, including*** ***(a) an understanding of the dissemination of content, in how far specific groups of recipients are targeted and affected and in how far coordinated efforts are underlying the dissemination of content,*** ***(b) underlying economic incentives for the very large platforms on how to deal with the risks referred to in Art. 26(1), e.g., the turnover and revenues generated through illegal content***. 3. … 4. In order to be vetted, researchers shall be ~~***affiliated with academic institutions, be***~~ independent from commercial interests, have proven records of expertise in the

	fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request.

Explanation:

Art. 33(1) DSA requires very large platforms to disclose "data that are necessary to monitor and assess compliance" with the DSA. Such data might very well be used to justify a sanction for non-compliance with the DSA. If such sanctions serve a repressive purpose (that is: sanction past non-compliance retroactively), such enforced data access might very well amount to self-incrimination which is not compatible with the principle of Nemo Tenetur or the "right to silence" (as acknowledged in Art. 6(2) ECHR and Art. 47, 48 of the Charta of Fundamental Rights of the European Union, see, e.g., ECJ, decision of 2 February 2021 - Case C-481/19). Therefore, it should be clarified that data access according to Art. 33(1) will not be used to justify repressive sanctions.

Art. 33(2) DSA should be expanded to help better understand dissemination of content, underlying structures (e.g., radical organizations targeting specific users). Data access should also allow vetted researchers to better understand the underlying economic incentives of systematic risks of very large online platforms. Online platforms often make it very clear that they do not want to generate revenues through abusive behaviour of their users, e.g. the spread of illegal content. However, economic profits through such content might diminish incentives on how to act against it.

Generally, it does not seem legitimate to exclude researchers from data access who are not affiliated with an academic institution. Valuable insights for democratic discourse as well as further research might as well follow from non-affiliated researchers working at NGOs or as independent journalists. At a practical level, this will prevent complicated disputes whether or not an institution is "academic" and whether or not a researcher is "affiliated" here. Therefore, the proposal above suggests to streamline the definition of researchers eligible for data access.

5. Effective Risk Mitigation

5.1. The Board should have the power to expose platforms with high impact on democratic discourse to the VLOPs - regime (Art. 25).

Article 25	
Commission text	Suggestion
1. This Section shall apply to online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3. 2. ...	1. This Section shall apply to online platforms which provide their services to a number of average monthly active recipients of the service in the Union equal to or higher than 45 million, calculated in accordance with the methodology set out in the delegated acts referred to in paragraph 3. ***After consultation with the Member State of establishment and respecting the right to be heard of an online platform, the Board may, by unanimous decision, decide that this Section also applies to an online platform irrespective of the number of recipients referred to in sentence 1 if that platforms has a similar impact on the democratic discourse within the Union as platforms described in sentence 1.*** 2. ...

Explanation:

The definition of Very Large Online Platforms (VLOPs) in Art. 25 refers to the number of recipients of a service. While this threshold seems legitimate, there might be "smaller" platforms which require similar attention as VLOPs. This might especially prove true for future platforms to come, where it does not yet seem clear whether a number of recipients substantially reflects the impact of a platform on democratic discourse and the needs to expose them to ambitious regulation and oversight. One must also bear in mind that the due diligence obligations for normal (non - very large) platforms, are not ambitious in the Commission draft of the DSA. Therefore, the DSA should include the possibility to include other impactful platforms beyond the criterion of a very large number of recipients.

5.2. Risk assessment should cover risks to gender equality (Art. 26).

Article 26(1)	
Commission text	Suggestion
1. Very large online platforms shall identify, analyse and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include the following systemic risks: (a) the dissemination of illegal content through their services; (b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively; (c) ...	1. Very large online platforms shall identify, analyse and assess, from the date of application referred to in the second subparagraph of Article 25(4), at least once a year thereafter, any significant systemic risks stemming from the functioning and use made of their services in the Union. This risk assessment shall be specific to their services and shall include ***at least*** the following systemic risks: (a) the dissemination of illegal content through their services; (b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and information, the prohibition of discrimination***, the equality between women and men*** and the rights of the child, as enshrined in Articles 7, 11, 21***, 23*** and 24 of the Charter respectively; (c) ...
<u>Explanation</u>: *The scope of the risk assessment required by Art. 26(1) should be broadened to also cover the right to equality between women and men, as protected by Art. 23 of the Charter of Fundamental Rights of the European Union. Such a reference would acknowledge that misogynistic background of online hatred, bullying etc. are very often observed (online hate is not gender-neutral). Moreover, algorithms and platform designs might (unintentionally) include or amplify gender based biases. Finally, it should be clarified that - in line with recital 57 of the draft DSA - risk assessment is not necessarily limited to the rights enumerated in Art. 26(1) (therefore the suggested amendment: "at least").*	

5.3. Auditors must be selected and paid for by authorities, not the platforms themselves (Art. 28).

<table>
<tr><td colspan="2">Article 28</td></tr>
<tr><td>Commission text</td><td>Suggestion</td></tr>
<tr><td>1. Very large online platforms shall be subject, at their own expense and at least once a year, to audits to assess compliance with the following:</td><td>1. Very large online platforms shall be subject, <s>at their own expense and</s> at least once a year, to audits by an auditor or auditors selected by the Board to assess compliance with the following:

(a) …

(b) ...

When selecting the auditor or auditors, the Board may specify the elements to be audited, and the methodology that shall be applied.</td></tr>
<tr><td colspan="2">Article 50(3)</td></tr>
<tr><td>3. ...

Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it may request the very large online platform concerned to subject itself to an additional, independent audit ...</td><td>3. ...

Where the Digital Services Coordinator of establishment has concerns on the ability of the measures to terminate or remedy the infringement, it may request the very large online platform concerned to subject itself to an additional, independent audit by an auditor or auditors selected by the Board ...</td></tr>
<tr><td colspan="2"><u>Explanation:</u>

For very large online platforms, the DSA relies heavily on independent auditors to investigate platform functions, behaviour and risks, how to achieve compliance and how to to mitigate risks facilitated through platforms.</td></tr>
</table>

Given the crucial role that the DSA gives to auditors by de-facto outsourcing oversight to the 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.

Acknowledging a de-facto oversight role of auditors: Authorities should select and pay auditors

Under the draft DSA, it is likely that platforms can select and must pay the auditor. It is highly likely that they will prefer to choose an auditor which is very capable of stirring up a lot of dust without suggesting substantial improvements or an auditor who identifies needs for change in areas that a platform wants to change anyway, without touching thorny questions. At least when choosing whether or not to re-mandate an auditor, platforms will think about such questions. Such a scenario must be a public good / regulator's nightmare, as a competent regulator that wants to take action against non-compliance then not only faces the gigantic platforms and their legal resources, but also finds itself in a position to argue against an audit which seemingly whitewashes the platform.

As a bare minimum, it must be clarified that not the platforms, but authorities select the auditors. Given our experience with some Member States of establishment 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. This would also acknowledge that the auditor plays a crucial role in regulating platforms which affect all Member States and their citizens.

Moreover, to strengthen trust in the independence of auditors, the authorities, not the platforms, should pay the auditors. Given that the auditors serve de-facto oversight functions, it might also be more in line with general principles of law to have authorities contract with the auditors and pay for them (a reimbursement clause might be added).

Audits might cover specific elements instead of covering a whole platform:

It should be clarified that audits do not necessarily need to cover all elements of a platform, but instead might focus on specific issues. Cover-it-all audits bear the risk of producing lengthy publications on topics which are not relevant, e.g., when an auditing report describes all the functions of a platform, which risks might arise here and which measures are taken and so on. Such an approach might waste resources and distort the view regarding which issue is the most pressing at a specific place in time and on a specific platform. Moreover, different auditors might have different expertise, depending on which functions of platforms are to be audited.

To give an old world example to illustrate: German authorities might initiate audits of "Volkswagen", but it might instead choose to focus: initiate audits of motor functions regarding exhaust manipulation.

6. Effective Regulatory Oversight

6.1 For reasons of legal certainty, recital 33 (by which orders regarding specific content are exempted from the country-of-origin principle) should be codified (recital 33, Art. 71).

Article 71	
Commission text	Suggestion
Art. 71 Deletion of certain provisions of Directive 2000/31/EC 1. Articles 12 to 15 of Directive 2000/31/EC shall be deleted. 2. References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 3, 4, 5 and 7 of this Regulation, respectively.	Art. 71 Deletion of certain provisions of ***and amendments to*** Directive 2000/31/EC ***1. The following sentence is added to Article 3(3) of Directive 2000/31/EC: "Paragraphs 1 and 2 shall also not apply to Orders to act against illegal content and to provide information."*** 2. Articles 12 to 15 of Directive 2000/31/EC shall be deleted. 3. References to Articles 12 to 15 of Directive 2000/31/EC shall be construed as references to Articles 3, 4, 5 and 7 of this Regulation, respectively.

Explanation:

For reasons of legal certainty, the important and rightful policy decision in recital 33 DSA should be codified.

Recital 33 DSA is interpreting Art. 3 of the E-Commerce-Directive, which in itself introduces a fundamental pillar of today's legal framework for online platforms: the so-called country-of-origin principle.

Overall, the country-of-origin principle creates a one-stop-shop solution to the benefit of industry: the rationale is that online platforms only need to understand and follow the laws (and orders) of the Member State where they are established. It is clear that in areas of law with little harmonization and where cross-border enforcement is far from effective (e.g., intermediary liability for hate speech), this results in a very industry-friendly regime (free flow of services, but no free flow of protection / enforcement).

Certain areas of law, where it had been acknowledged that harmonization and cross-border harmonization are not ripe enough to rely on a strict country-of-origin principle, were exempted from the principle through Art. 3(3) E-Commerce-Directive, e.g. Copyright law.

As we have learned during the last 20 years, we should have exempted some more areas of law which need cautious protection. One such field is to act against specific instances of infringing content, or for authorities to request certain information from a platform.

Therefore, recital 33 is an important policy decision. It will allow authorities and courts to order against platforms in specific cases without being bound by the country-of-origin principle. However, for reasons of legal certainty, recital 33 should be codified. Otherwise we risk that the courts might not find this a good enough legal basis to modify Art. 3 E-Commerce-Directive.

As an additional comment: It seems very likely that recital 33 will get under industry attack during the legislative process of the DSA. Legislators should resist such pressure. Online platforms can be expected to follow national orders in specific cases (which always can be appealed to the independent courts). If legislators feel the necessity to limit recital 33 for proportionality reasons, it might be acceptable to limit its effect to intermediaries which do not qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.

6.2. Allow destination-country Member States to pick jurisdiction in specific cases (Art. 40).

Article 40 (1.a.) - (1.e.)	
Commission text	Suggestion
1. The Member State in which the main establishment of the provider of intermediary services is located shall have jurisdiction for the purposes of Chapters III and IV of this Regulation.	1. ... ***1a. Irrespective of paragraph 1, Member States may exercise jurisdiction if the following conditions are fulfilled:*** ***(a) The measure is necessary for the prevention of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, sex, religion or nationality, and violations of human dignity concerning individual persons, the protection of public health, public security, including the safeguarding of national security and defence;*** ***(b) The measure is proportionate to those objectives;*** ***(c) The Member State has notified the Commission of its intention to exercise jurisdiction and the Commission has published this intention in the Official Journal of the European Union.*** ***1.b. The Commission shall examine the compatibility of the notified measures with Community law; where it comes to the conclusion that the measure or parts of the measures are incompatible with Community law, the Commission notifies the Member State; which then must refrain from the intended measure accordingly.*** ***1.c Measures taken in accordance with paragraph 1a. shall be limited in its effects to the territory of that Member State.*** ***1d. Member States must ensure that the principle of ne bis in idem is respected.***

	1e. Paragraphs 1a. shall not apply to online providers of intermediary services that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC.

Explanation:

Article 40 should be amended to allow Member States to derogate from Article 40(1) under specific circumstances. In specific circumstances, authorities from destination countries should be allowed to take up action against larger platforms which are established within another member state.

Current law already allows destination countries to take such action in specific cases, Art. 3(4) E-Commerce-Directive. One might argue that, since Art. 1(5)(a) DSA leaves Art. 3(4) of the E-Commerce-Directive intact, that even under the Commission draft of the DSA such derogations shall be possible in specific important cases. However, given the language of Art. 40(1) DSA, it will be very questionable how courts will interpret this question.

If courts were to interpret Art. 40(1) DSA to introduce a strict country-of-origin principle, this will have significant consequences. Especially when it comes to infringements causing serious harm (e.g., in the field of protection of minors against molesting, abusive behaviour, child exploitation and abuse material), Member States must be in a position to pick-up jurisdiction for specific cases to ensure a high level of protection and to fulfill obligations to ensure minimum protection following from national constitutional backgrounds or where a specific connection to that member state is established (e.g., incitement to hatred against minorities in a specific country, Holocaust denial in Germany).

Therefore the current logic of Art. 3(4) E-Commerce-Directive must be stabilized and clarified. Art. 40(1) DSA should be amended to allow Member States to derogate from Art. 40(1) DSA under specific circumstances.

Derogations should be strictly limited to what is necessary for important policy concerns of destination countries and its consequences must be limited to the respective territory. Small companies and start-ups should be excluded. As an additional procedural safeguard, Member States need to notify derogations to the Commission, which will evaluate the conformity of such a measure.

The proposal results in the following framework:

1. *start-ups: for the application of the DSA, only and with no exemptions need to understand whether content is illegal according to their home-country law (or Union-law).*
2. *bigger platforms: generally only need to understand whether content is illegal according to their home-country (or Union-law). If a Member State has notified the Commission to exercise jurisdiction in a specific case, e.g., regarding the ban of Holocaust Denial, the platforms need to consider this too when applying the DSA (geoblocking).*

6.3 For VLOPs, the burden of oversight should be shared amongst all Member States, with the Commission providing guidance (Art. 40).

Article 40	
Commission text	Suggestion
3. Where a provider of intermediary services fails to appoint a legal representative in accordance with Article 11, all Member States shall have jurisdiction for the purposes of Chapters III and IV. Where a Member State decides to exercise jurisdiction under this paragraph, it shall inform all other Member States and ensure that the principle of ne bis in idem is respected.	3. ... ***3a. For very large online platforms, all Member States may exercise jurisdiction. Where a Member State decides to exercise jurisdiction under this paragraph, it shall inform the Member State mentioned in paragraph 1 and the Commission; paragraph 1a.(c) applies accordingly. A Member State exercising jurisdiction must ensure that the principle of ne bis in idem is respected.*** ***When several Member States want to initiate proceedings regarding an identical issue, they might request the Commission to make a guiding decision on the question of jurisdiction. At any given time and irrespective of Articles 46(2) and 51, the Commission might initiate its own proceedings and request the Member States to abandon their proceedings.***

Explanation:

According to the DSA, the Member State where a platform is established has jurisdiction to conduct oversight in the first place.

However, when it comes to very large online platforms, it is not realistic to rely on a single country of origin being responsible for oversight. Regarding very large online platforms, we must prevent cherry-picking of regulators, and me must acknowledge that oversight over very large (gigantic) platforms might overwhelm any single Member State - therefore we should share this burden from the beginning among all Member States:

1. *The Commission cannot counter-balance overwhelmed regulators: The DSA envisions the Commission as an additional regulator of last instance for very large platforms. However, a lengthy procedure would need to be gone through before the Commission could finally issue*

a sanction. This lengthy procedure will offer the platforms multiple lines of defense and to adjust their behavior before they have to fear a final sanction. Moreover, the Commission is not budgeting to build up a super-agency. Thus, it cannot be expected that the Commission will have the role of a "super-regulator" which will be in a position to counterbalance a passive or overwhelmed country of origin.

2. *Cherry-picking of regulators: Ireland, where Facebook, YouTube, Twitter and the likes are established, has been either unwilling or overwhelmed by the task of conducting oversight for all the Dublin-based mega-platforms. Given the importance of very large platforms, we cannot stick to a regime where platforms "cherry-pick" their regulator by choice of their seat, resulting in a race to the bottom for oversight.*

3. *Prevent a "cat and mouse game": If only the country of establishment has jurisdiction, platforms might run away from their regulator. Even if, e.g., Ireland might some day build up meaningful regulatory resources, then, by a simple change in its Terms of Services, an "Irish" very large platform might switch its seat to, say, Luxembourg. Including all Member States into oversight over very large platforms would outrule such a scenario.*

4. *If you are going against Goliaths, take all the Davids you can get: Moreover, we can skip blaming Ireland. In the field of compliance with the DSA, we are going against gigantic platforms with unprecedented impact on our citizens, societies, democracies and economies. To police such huge platforms' compliance requires large resources and might easily overwhelm any single national regulator. Neither Ireland, nor other single Member States can do it alone. Therefore, we should try to get as many national authorities into the ring that we can, if they are willing to spend the resources necessary.*

At least for very large platforms, we therefore suggest to include all Member States to contribute to oversight, acting as "agents" of the Commission, as suggested above. The resulting scenario (proposals 6.2 plus 6.3) is:

1. *Start-ups are protected by a strict country of origin - principle.*

2. *Bigger platforms might face destination country jurisdiction in specific cases.*

3. *Very large platforms are exposed to combined oversight of all Member States.*

6.4 Third parties should be included in enforcement against fundamentally non-compliant platforms (Art. 41).

Article 41	
Commission text	Suggestion
3. Where needed for carrying out their tasks, Digital Services Coordinators shall also have, in respect of providers of intermediary services under the jurisdiction of their Member State, where all other powers pursuant to this Article to bring about the cessation of an infringement have been exhausted, the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the power to take the following measures:	3. Where needed for carrying out their tasks, Digital Services Coordinators shall also have, in respect of providers of intermediary services under the jurisdiction of their Member State, where all other powers pursuant to this Article to bring about the cessation of an infringement have been exhausted, the infringement persists and causes serious harm which cannot be avoided through the exercise of other powers available under Union or national law, the power to take the following measures:
(a) require the management body …	(a) require the management body …
(b) ... request the competent judicial authority of that Member State to order the temporary restriction of access of recipients of the service concerned by the infringement or, ...	(b) ... request the competent judicial authority of that Member State to order the temporary restriction of access ***to*** ~~**of recipients of**~~ the service ~~**concerned by the infringement**~~ or, ...
	(c) ***request the competent judicial authority to order proportionate measures to be taken by other persons than the provider of the intermediary services, including the cessation of contractual or factual relationships with the provider, if these measures, alone or taken together, are potentially capable of bringing about the cessation of an infringement.***

Explanation:

The DSA does not provide solutions for enforcement when an intermediary service is fundamentally non-compliant, with no assets or representatives accessible within the Union. 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)). However, this provision is somehow misconstructed as it focuses on the restriction of access of recipients (!) and not the service in itself. Therefore, it is suggested to amend Art. 41(3)(b).

More importantly, European law does not explicitly explain on which grounds termination of access should be ordered and how it should be enforced, though the European Court of Justice has clarified that (access) providers might be ordered to deny access to certain infringing services (see cases C-314/12 and C-484/14). But measures by access providers might not always be the most effective. One can think of other third parties which are in a factual position to stop supporting transactions with a given infringing 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 to delete the Telegram App from an AppStore.

The concept of including innocent third parties is not new to common legal regimes. It is known to all modern enforcement measures (imagine the seizure of bank accounts, which requires the banks to cooperate; a more modern example can be found in third party injunctions according to Art. 11 sentence 3 of the Enforcement-Directive (2004/48/EC)).

In line with that, the proposal suggests that such third parties can be included in enforcement measures. As the affected third parties are not involved in the infringement but requested to provide emergency relief as a means of last resort, measures must be strictly proportionate. In specific cases, this might require that third parties receive financial compensation for supporting enforcement.

6.5 Oversight proceedings should not overcomplicate. Certain steps can be voluntary (Art. 50).

Article 50(2)	
Commission text	Suggestion
4. When communicating the decision referred to in the first subparagraph of paragraph 1 to the very large online platform concerned, the Digital Services Coordinator of establishment shall request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or remedy the infringement. The measures set out in the action plan may include, where appropriate, participation in a code of conduct as provided for in Article 35.	4. When communicating the decision referred to in the first subparagraph of paragraph 1 to the very large online platform concerned, the Digital Services Coordinator of establishment ~~**shall**~~ ***might*** request it to draw up and communicate to the Digital Services Coordinator of establishment, the Commission and the Board, within one month from that decision, an action plan, specifying how that platform intends to terminate or remedy the infringement. The measures set out in the action plan may include, where appropriate, participation in a code of conduct as provided for in Article 35.
Article 50(3)	
3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services Coordinator of establishment. Within one month following receipt of that opinion, that Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement.	~~**3. Within one month following receipt of the action plan, the Board shall communicate its opinion on the action plan to the Digital Services Coordinator of establishment. Within one month following receipt of that opinion, that Digital Services Coordinator shall decide whether the action plan is appropriate to terminate or remedy the infringement.**~~
Explanation: *The oversight proceedings for very large platforms in the DSA are innovative, but they are also pretty complicated and lengthy. To simplify and accelerate the process, requesting an action plan (and the Board opinion on it) should not be obligatory. E.g., in clear cases, the Digital Services Coordinator should not be bound to request an action plan. Note that at any given time, platforms are free to voluntarily deliver action plans to demonstrate their willingness to end infringements. During pending proceedings, Digital Services Coordinators are always in a position to take voluntary action plans into account, e.g. coming to the conclusion that sanctions are not necessary.*	

6.6 Commission interruption in oversight must make sense: The Commission ***might*** intervene after member state level proceedings, it ***must*** do so only on appeal of the Board or other Member States (Art. 50, 51).

Article 50(4)	
Commission text	Suggestion
4. The Digital Services Coordinator of establishment shall communicate ... (a) … (b) … (c) ... Pursuant to that communication, the Digital Services Coordinator of establishment shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the very large online platform concerned, without prejudice to Article 66 or any other measures that it may take at the request of the Commission.	4. The Digital Services Coordinator of establishment shall communicate ... (a) … (b) … (c) ... ~~**Pursuant to that communication, the Digital Services Coordinator of establishment shall no longer be entitled to take any investigatory or enforcement measures in respect of the relevant conduct by the very large online platform concerned, without prejudice to Article 66 or any other measures that it may take at the request of the Commission.**~~
Article 51	
Commission text	Suggestion
1. The Commission, acting either upon the Board's recommendation or on its own initiative after consulting the Board, may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the very large online platform that: (a) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment did not take any	1. The Commission~~***, acting either upon the Board's recommendation or on its own initiative after consulting the Board, may***~~ initiate***s*** proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the very large online platform that: (a) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment did not take any

investigatory or enforcement measures, pursuant to the request of the Commission referred to in Article 45(7), upon the expiry of the time period set in that request;	investigatory or enforcement measures, pursuant to the request of the Commission referred to in Article 45(7), upon the expiry of the time period set in that request;
(b) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment requested the Commission to intervene in accordance with Article 46(2), upon the reception of that request;	(b) is suspected of having infringed any of the provisions of this Regulation and the Digital Services Coordinator of establishment requested the Commission to intervene in accordance with Article 46(2), upon the reception of that request;
(c) has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time period for the communication referred to in Article 50(4).	~~**(c) has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time period for the communication referred to in Article 50(4).**~~
	1a. The Commission, acting either upon the Board's recommendation or on its own initiative after consulting the Board, may initiate proceedings in view of the possible adoption of decisions pursuant to Articles 58 and 59 in respect of the relevant conduct by the very large online platform that has been found to have infringed any of the provisions of Section 4 of Chapter III, upon the expiry of the relevant time period for the communication referred to in Article 50(4).
	In this case, the Commission might take interim measures. This might include ordering that the Digital Services Coordinator must preliminarily stop any enforcement measures in respect of the relevant conduct.
2. Where the Commission decides to initiate proceedings pursuant to paragraph 1, it shall notify all Digital Services Coordinators, the Board and the very large online platform concerned.	*2.* Where the Commission ~~***decides to***~~ initiate***s*** proceedings pursuant to paragraph 1 ***or 1a.***, it shall notify all Digital Services Coordinators, the Board and the very large online platform concerned.

Explanation:

For very large online platforms, the DSA designs a two-step oversight mechanism. Whenever the relevant Member State authority (Digital Services Coordinator) has ended its proceedings (finding that the platform violated the DSA or not) then its power to take any enforcement measures automatically comes to an end (Art. 50(4)). After that (handbrake on enforcement has been pulled), in a second step, the Commission may step in and act as a regulator of a second instance, Art. 51(1).

This is a very odd design of the oversight mechanisms. It will render oversight highly ineffective.

It is a long-living tradition of oversight proceedings, that after a regulator found infringements, it might then enforce that decision. Courts or regulators of second instance might (after appeal) reverse that decision or temporarily order a halt to enforcement. It is very odd that the draft DSA makes it a default-rule to halt enforcement, meaning that enforcement is automatically put on hold even in the clearest of cases after the finest of proceedings.

All this becomes even more questionable due to Art. 51(1), according to which the Commission "may" decide to initiate proceedings, as is also shown by recital 97 ("The Commission should remain free to decide whether or not it wishes to intervene"). At least when the Board or other Member States (which might be affected by a platform's behaviour) request so, Commission intervention should be mandatory.

This requires changes:

1. *Don't stop enforcement as a default rule: We therefore suggest that the Digital Services Coordinator, after finding a violation of the DSA, should be in a position to go on and enforce its findings (e.g., execute penalties). Therefore, Art. 50(4) sentence 2 should be deleted. Note that in such a case, the platform's ability to seek intervention through the courts is in no way affected.*

2. *The Commission might put enforcement on hold on a case-by-case basis: If the Commission decides to start its own proceedings after the Digital Services Coordinator has found an infringement, it might (or might not) temporarily put enforcement measures on hold, as suggested in Art. 50(1a), depending on the likelihood of a final finding of infringement and on the necessity and consequences of preliminary enforcement.*

3. *The Commission must intervene when Member States or the Board protest: However, when the Commission is asked by Member States or the Board, it should be obligatory to start proceedings (see suggestions Art. 50(1)(a)-(b)). In other cases, the Commission might have discretion whether or not to step in (Art. 50(1a) of the suggestion) or whether to leave potential review to the courts (on appeal by the platforms).*