Submission to the consultation on

Draft Guidelines for Article 28 of the Digital Services Act

Dr. Martin Husovec

Associate Professor of Law, London School of Economics (LSE)

Any initiative to flesh out the meaning of Article 28 DSA through a soft-law instrument is a positive step forward to protect the rights of children. Children and companies alike will benefit from more conceptual and practical clarity about how to implement the provision. This submission outlines four important framing considerations that might be relevant in the process of drafting the guidelines:

1. **Article 28 should be implemented holistically**
2. **Article 28 should clearly distinguish two steps: applicability and obligations**
3. **Article 28 should be drafted as more top-down guidance**
4. **Any definitions of harmful content to minors should be based on other legal instruments**

1. Article 28 should be implemented holistically

Article 28 of the DSA is one of the most enigmatic provisions of the DSA. It was introduced as a spin-off of the dark patterns provision in the legislative process. It embodies a clear democratic mandate tasking even less big platforms to consider the interests of minors.

Despite the proclaimed goals of seeking 'to ensure a high level of privacy, safety, and security of minors', **the implementation of the provision cannot be limited to privacy, safety, and security for several reasons**. The best interests of a child dictate that all their rights must be equally balanced.

Firstly, all provisions of the DSA are subject to the EU Charter of Fundamental Rights. Article 28 DSA is no exception. Thus, when providers protect the *safety* of minors, they cannot disregard their right to freedom of expression (Article 11 CFR) or right to education (Article 14 CFR); when providers protect the *security* of minors, they cannot ignore their right to seek information (Article 11 CFR) or to protect their privacy and personal data from others (Article 7 and 8 CFR), including family members; when providers protect their *privacy*, they cannot undermine their right to assembly (Article 12 CFR), or freedom to pursue their careers (Article 15 CFR). The balancing that the providers are required to undertake thus cannot be made 'appropriately and proportionally' without thinking about all other human rights of a child.

Secondly, any guidance that will not address **all rights of minors** is bound to undermine 'the best interests of a child' by over-emphasizing some interests. Children daily face many other practices that undermine their interests, such as protection of their security at the expense of their privacy vis-à-vis parents, or exclusion from major services that are appropriate to their evolving capabilities. The appropriate balancing is impossible to make when children's right to freedom of expression (Article 11 CFR), education (Article 14 CFR), right to seek information (Article 11 CFR), or right to assembly (Article 12 CFR), and freedom to pursue their careers (Article 15 CFR) are not equally taken into account.

It is therefore recommended that despite the language of Article 28 DSA, the provision is construed holistically as encapsulating all human rights of a child, and the best overall interests of a child.

2. Article 28 should clearly distinguish two steps: applicability and protection questions

From the perspective of legal systematic, Article 28 is an exception to the rule in the DSA that online platforms that are not very large, are not legally obliged to conduct risk assessments. In the absence of Article 28, the main obligations of online platforms concern content moderation.

The provision applies to potentially thousands of services of various kinds, ranging from adult sites, social media, gaming and dating apps, to small discussion forums, food delivery apps, online marketplaces, or short-term rental platforms. At the moment, there is no comprehensive way how to check which companies are regulated by the DSA as online platforms. There is a lot of diversity among the platforms, some with high risks, others with low risks for minors, with unclear distribution among them.

When drafting the guidance on Article 28 DSA it is important to keep in mind that the provision consciously foresees two stages: (1) applicability inquiry and (2) obligations inquiry. In other words, digital services that qualify as online platforms must first fall into the scope because they are 'accessible to minors', and only then, such providers can be subject to obligations of the provision. Thus, not all online platforms are subject to Article 28 obligations. This first filter is a conscious design choice that stands in contrast with how the protection of children works on very large online platforms. VLOPs, in contrast, must consider the interests of minors in every case. For this reason, any other minor-specific obligations for non-VLOPs are also always explicit (see e.g., Article 14(3)) and use the qualifiers on the applicability (e.g., Article 14(3): 'directed at' or 'predominantly used', or Article 28(2): 'when they are aware').

The applicability inquiry is not well explained by the DSA. Recital 71 attempts to define the applicability by invoking four explicit situations: A) 'when its terms and conditions permit minors to use the service', B) 'when its service is directed at' minors or C) when the service is 'predominantly used by minors' and D) 'where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes'. Arguably, A) is only a subtype of B) because it concerns a conscious decision to target minors. Arguably, D) is only a subtype of C) because it concerns a situation when services are factually being used in significant amounts, even though this was not necessarily intended by the platform.

Thus, the two basic situations are: (1) targeting minors, or (2) predominantly being used by minors. While targeting might be easier to discern in some cases, more difficult cases concern when minors use services, but the question is whether there is enough of them to trigger Article 28. The word predominantly is not defined by the DSA, and it is not clear if it refers to the overall user base or children population. Arguably, given the example D, it could relate to the latter, and thus have a broader meaning. This still leaves the question of threshold undetermined. The regulators should improve the clarity of the provision by setting the thresholds in their soft-law instrument. These could depend on the type of the service (e.g., its risk profile), and a number of users using the services. The regulators could think of creating safe-harbour-type thresholds, presumptions, or even registration processes to increase the clarity of who is definitely covered by Article 28.

The regulators could also finance surveys that would interview children about their use of digital services and try to measure the prevalence of the use of particular digital services. Such surveys could

be conducted on services, or outside of them, e.g., in schools or similar settings. To avoid strategic behaviour and complicated enforcement, it is important to suggest ways of determining the applicability of Article 28 that are independent of the platforms' own measurements.

Only once the thresholds are met, Article 28 obligations, especially the implicit risk assessment, should be triggered. The first stage of the applicability should be strictly separated because excessive risk assessment for low-risk services can incentivise companies to further exclude children from their user base. This would be certainly detrimental to the best interests of children.

It is therefore recommended that the guidance includes explicit thresholds for different categories of services, and these are continuously revised in light of the survey data, that is procured by the regulators. These thresholds could be accompanied by safe-harbour-type registration or presumptions in order to increase the clarity about who is definitely regulated by Article 28.

3. Article 28 should be drafted as more top-down guidance

Given that Article 28 must be narrower than obligations imposed on very large online platforms, which must assess and mitigate risks posed by the design, use and functioning of the services (Articles 34-35), the legitimate question is how narrower.

Article 28 DSA has developed as a spin-off of the dark patterns provision (Article 25 DSA). There is therefore a good historical argument that the provision should focus on mitigation of risks by the design of services. This is also supported by examples made in Recital 71 that explain the provision. Thus, one possible approach would be to limit the scope of Article 28 to design interventions by platforms, such as changes to interfaces, defaults, provisions of tools, and adjustment of features. However, the systemic and historical arguments do not have to be conclusive.

The key consideration should be rather **clarity of expectations**. Two dozen VLOPs are expected to figure out solutions to societal problems together with the ongoing dialogue with the European Commission. However, given potentially thousands of online platforms and their diversity, no such dialogue is likely with 27 different national regulators. Hence, online platforms, unlike VLOPs, should be first and foremost **better guided by the regulators**, whatever the scope of Article 28. In that sense, the drafting technique should differ substantially in style from the one adopted in the Election Integrity Guidance.[1]

The risk inherent in drafting a vague guidance is that the regulators might replicate all their expectations from VLOPs and extend them to all online platforms. This could go counter to the asymmetric design of the DSA that is meant to regulate non-VLOP platforms differently. It could also undermine the rights of children who might end up being excluded from even more services.

Clarity of the regulatory expectations serves minors because it incentivises companies to admit that they have children among their users, include them in their design considerations, and truly grapple with the ensuing obligations head-on.

Given that platforms that could fall under the scope include less risky and general purposes services, such as online marketplaces, food deliveries, and short-term rental marketplaces, there is a real risk that unclear rules will facilitate further exclusion of under-18s from indispensable digital services.

[1] https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes

Already today, it is striking that many services that are arguably within the capabilities of more mature children, such as 16 to 18 years old, still explicitly exclude them from the services. Minors who in many countries can vote, marry, and purchase real estate are excluded from using simple digital services, such as some short-term rental services, and online marketplaces. This negative exclusionary effect should be equally considered.

The guidance could aim to **increase the inclusion of children** in services that correspond to the evolving capabilities of their age group. While a lot of political attention is on services where children should be excluded from the use (e.g., the adult sites), much more difficult scenarios are the majority of digital services that could be used by children but need to be adjusted for them.

Article 28, similarly to Article 35, implies certain discretion of companies to design the most appropriate measures. The regulators can, however, consider **recommending standard measures**.

The consultation of children should be at the heart of these changes. The measures could involve **changing the choice architecture** (e.g., changing the default rules or features, including content moderation, and recommender systems), **adding features** (e.g., further empowerment tools to block users, or content, or disabling certain features), and, in justified cases, **subtracting features** (e.g., when certain features are too risky for minors of the respective age groups).

The design interventions should consider the minors' best interests by analysing the design of the services against the usual vulnerabilities of specific age groups. Age-sensitive design interventions, such as empowerment by adding features, can help children to better cope with risks, and thus improve their resilience to risks in the long run, including after they grow to become risk-conscious adults. Without age-appropriate risk, it is hard to gain resilience.

Age-assurance and age-verification technologies are likely to be among the most controversial aspects of the proposed guidance. These design interventions, as all the others, should consider the impact on the participation of minors in society. Overbroad mandatory deployment of such technologies across all online platforms, regardless of their risk profiles, can incentivise companies to close off even bigger parts of the ecosystem to children.

It is recommended that the drafting technique places more emphasis on clarity and top-down guidance of the regulatory expectations than the usual VLOP-focused documents*.*

4. Any definitions of harmful content to minors should be based on other legal instruments

The DSA does not prescribe what content cannot be online. It leaves the formulation of rules on illegality to parliaments (Article 3(h)), and contractual rules to platforms (Article 14(1)).

However, to address risks to minors, it is difficult not to respond with reference to certain categories of content. The regulation of audiovisual media includes a rule that obliges member states to ensure that 'audiovisual commercial communications provided by media service providers (..) shall not cause physical, mental or moral detriment to minors' (Article 9 AVMSD). Moreover, 'the video-sharing platform providers', mindful of their lack of editorial control or obligation to generally monitor content, have an obligation to 'take appropriate measures to comply' with the harmful content requirements for audiovisual commercial communications and user-generated videos of their users (Article 28b

AVMSD). Such content harmful to children can 'only [be] made available in such a way as to ensure that minors will not normally hear or see them' (Article 6a AVMSD).

Articles 6, 9 and 28b AVMSD, implemented in national law, are forms of content rules that the DSA broadly anticipates. The independent regulators who are competent to supervise AVMSD have a mandate to guide companies in how they should understand the notions of 'physical, mental or moral detriment to minors'.

Based on the fact that many design interventions under Article 28 are connected with different categories of content, e.g., self-harm content, or promotion of anorexia, it is understandable that a link between such categories and Article 28 needs to be established. However, any content guidance is guidance under the AVMSD, not DSA. While Article 28 is a measure of full harmonisation, the content rule of audiovisual content harmful to minors is harmonised by AVMSD. Moreover, for the services that do not fall under the definition of video-sharing services, or content that is not audiovisual, legal mandates regulating such content for children depend on largely unharmonized national law.

Thus, inevitably, even though harmonising such categories of content might be beneficial, there are important competence questions to consider.

It is therefore recommended that the content rules referred to in the guidance are explicitly based on the specific legal basis outside Article 28, such as AVMSD, and limited by such legal basis.