Doc. Dr. Iur. Mgr. Martin Husovec

The Registrar
General Court
Court of Justice of the EU
Luxemburg

Statement in Intervention
by Stichting "ARTICLE 19"
in Technius v Commission (Case T-134/24)

Table of Contents

A. Equal treatment and legal certainty of AMARs (fourth and fifth plea)

(1) Technius claims that the Commission selected Similarweb's data to calculate Stripchat's average monthly active recipients (AMARs), and thereby also underlying methodology, and thus is under an obligation to justify it. The Commission, on the contrary, argues that it was Technius that decided to rely on this specific methodology (paras 21 ff., Defence). Based on the information available in the file, the Commission is entirely right. The Commission accepted Similarweb's data – relied on by Technius – as a credible method of calculation of AMARs. The true dispute is about whether the Commission was entitled to reject the discounting criterion applied by Technius to the initial data, i.e. a particular 'bounce rate'. However, the suit filed by Technius goes well beyond this when it argues:

- that Article 33 cannot serve as a valid legal basis for the Contested Decision because in the absence of a delegated act, it is not sufficiently foreseeable (the fourth plea), and
- that the Commission violated the principle of equal treatment (the fifth plea).

(2) Technius indirectly objects to the arbitrariness of the threshold introduced by Article 33(1) and the unpredictability of AMAR counting. It needs to be emphasized that any legislative threshold is somewhat arbitrary. The medium-size company threshold in Article 19 DSA can equally be said to be arbitrary. Why would a company of 10 employees with a turnover of 10.1 million have to comply with online platform obligations, such as verification of traders (Article 30), while a similarly-sized company with a 9.9 million euro turnover does not? The answer is simple. Because the legislature had to set a threshold somewhere. Technius further argues that the application of this threshold by the Commission violates the principle of equal treatment and legal certainty. The situation, in its view, was exacerbated by the lack of a delegated act.

(3) Article 33(3) states that a delegated act 'may' be adopted. In the absence of a delegated act, companies enjoy considerable discretion in user counting according to Article 3(p) DSA. This discretion is fully in line with the entire risk management framework that asks companies to be active participants in the regulatory dialogue. The discretion of Technius is visible in the language of Article 33(4) which says that "[t]he Commission shall take its decision based on data reported by the provider of the online platform or of the online search engine pursuant to Article 24(2), or information requested pursuant to Article 24(3) or any other information available to the Commission". The following paragraphs make it clear that only if the data is not reported, or does not seem credible, the Commission will use other data sources.

(4) Technius bases its argument on the fact that it could not properly construe the meaning of the relevant threshold and that other companies might count the users differently. However, it was up to Technius to develop and present credible methods for user counting that remain reasonable against the background of instructions in Article 3(p) DSA. Understandably, counting requires the adoption of several proxies (e.g., discounting multiple visits by the same person or organisation, and irrelevant incidental, non-human, and non-EU visits). However, it was Technius that adopted a particular counting method within its discretion. From the file it appears that the Commission fully accepted the numbers of Technius, it only disagreed about the credibility of the 'bounce rate'. In this regard, ARTICLE 19 fully supports the arguments presented by the Commission.

(5) Thus, the case does not require the Court to consider the appropriateness of user counting, as the Commission accepted the overall submitted numbers. It only requires the Court to consider the justifiability of the discounting proposed by Technius.

(6) Furthermore, while Article 33 is a 'may' provision, the Commission undoubtedly must improve the foreseeability of the system going forward. The Commission is clearly under an obligation to operate the DSA system according to the principles of good administration (Article 41 of the EU Charter). This includes, where appropriate, making binding, or non-binding clarifications at the

right time. Therefore, it is not unreasonable to expect that once the evidence is established, and the public is consulted, the Commission ought to prepare a delegated act to improve the foreseeability of the law, and the level playing field. However, Technius is complaining about the early months of the application of an entirely new law, during which the Commission hardly could have had sufficient evidence, knowledge, and time to consult anyone on a universal methodology that could work for different types of services.

(7) The Commission acted in light of the obligation to operate the DSA system according to the principles of good administration when it rejected a 'bounce rate' that has no support in the DSA. Because the Commission's designation process is the only mechanism through which companies that meet the threshold can become subject to the enhanced obligations of the DSA, the Commission has a **strong duty to the public to thoroughly investigate the claims of the companies that allow them to escape the designation**. If the Commission stays passive, the public has only a very limited means to request the designation of intermediaries as VLOPs and VLOSEs – namely by seeking a declaration of an infringement by the Commission according to Article 265 TFEU.

(8) In such a case, the public would have to provide sufficient evidence. There is little doubt that the companies are in the best position to collect and analyse evidence that establishes AMARs. The entire DSA framework is built on the idea that companies have frequently superior information compared to the public, and regulators. Thus, the Commission is under a strong duty to investigate the numbers provided by the companies and designate them as VLOPs and VLOSEs where the requirements are met. Limiting the Commission's ability to do so would undermine the effectiveness of the regulatory system that is meant to force the hand of companies to disclose relevant information in the public interest.

(9) To conclude. The Commission is obliged to accept all AMARs estimations of companies that are credible considering the submitted evidence and to reject any discounting factors that have no basis in the DSA. In this case, the Commission has done just that.

B. Systemic risks related to Stripchat (sixth plea)

(10) In its sixth plea, Technius contends that the designation of its platform as a VLOP constitutes an infringement of its freedom to conduct a business as protected under Article 16 of the Charter, as well as a violation of the principle of proportionality enshrined in Article 52 of the Charter. The applicant's argument rests on the assertion that Stripchat "does not pose the systemic risks of very large online platforms that the Regulation (EU) 2022/2065 is intended to address". Specifically, the applicant argues that "[a]s Stripchat is focused on adult entertainment, the

Applicant's service is very limited in terms of subject matter and content disseminated. On Stripchat, there are no political discussions, echo chambers or issues of free speech".

(11) This argument is based on three critical misconceptions. They concern (i) the way the DSA operates in identifying and designating those intermediaries subject to enhanced due diligence obligations; (ii) the systemic risks the DSA seeks to address and the extent to which Stripchat indeed has the potential to contribute to such risks; and (iii) the risks to freedom of expression posed by Stripchat, both in the context of online platforms disseminating pornographic content and in the broader context of freedom of expression concerns, such as those related to advertised content, dark patterns or other issues. Each of these will be addressed in turn to illustrate the deficiencies in the applicant's argument.

(12) First, the applicant fundamentally misunderstands how the DSA operates. The DSA requires that any VLOP and VLOSE with more than 45 million AMARs comply with enhanced due diligence obligations. This requirement stems from the recognition that the systemic risks associated with the services provided by VLOPs and VLOSEs are, due to their sheer number of users, different in scope and impact from those caused by smaller platforms, thereby justifying the need for enhanced due diligence and heightened regulatory oversight.

(13) **The assessment and identification of systemic risks under the DSA are tasks explicitly assigned to the platforms**. They must be based on a careful, thorough, and detailed assessment of the societal risks posed by their systems and processes. This again resolves huge information asymmetry between the public and regulators on the one hand, and the companies on the other. The DSA does not require or allow the regulator to make a categorical ex-ante determination whether a VLOP's specific systems and processes pose a systemic risk and, on that basis, exclude such platforms that exceed the user threshold from the scope of its obligations. The applicant's interpretation is at odds with the co-regulatory model established by the DSA, under which primary responsibility for risk assessment lies with the platforms and is then subject to scrutiny by the Commission.

(14) Second, Technius' argument reflects an incorrect understanding of the "societal risks" that the DSA seeks to address and of the two key enhanced due diligence obligations imposed on VLOPs and VLOSEs – risk assessment and risk mitigation. The Digital Services Act aims to ensure a 'safe' and 'trusted online environment' (Article 1(1)) to enable individuals to fully enjoy their fundamental rights online. These rights extend well beyond freedom of expression. Indeed, Article 1(1) of the DSA specifically refers to the aim of the DSA being **the protection of all the fundamental rights enshrined in the Charter** (see also Article 34(1)(b) DSA).

(15) The systemic risk provisions in Articles 34 and 35 of the DSA are central to achieving this objective. Article 34, in particular, addresses a broad, non-exhaustive range of fundamental rights at risk. For example, it explicitly mentions systemic risks posed by platforms to the fundamental rights of children (Article 24 of the Charter), and the respect for private and family life (Article 7 of the Charter). It also lists as systemic risks any actual and foreseeable negative effects in relation to gender-based violence, the person's physical and mental well-being or protection of human dignity. Adult content platforms, such as Stripchat, fall squarely within the scope of these provisions.

(16) Additionally, VLOPs are specifically required to address the risks associated with the dissemination of illegal content. This obligation directly applies to platforms disseminating adult content, where the potential for unlawful activity is both tangible and significant. Recital 12 of the DSA mentions as illustrative examples the instances of "sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking".

(17) There can therefore be no doubt that adult platform sites are meant to be subject to the enhanced due diligence obligations imposed by the DSA for VLOPs. The mechanisms designed for users (e.g., Chapter 3), and civil society organisations (e.g., Articles 21, 22, 40, 86, 90, etc.) must remain effective when supervising these digital services.

(18) This is not merely hypothetical. Special obligations of Section 5 of Chapter 3 of the DSA require additional transparency, data access, and risk management from the companies whose services are designated as VLOPs. The plaintiff is now obliged to give access to researchers to study and analyse various risks posed by its services. The risks, such as child sexual abuse, sexual slavery, and sexual harassment, including sextortion videos, are all too real on adult sites. Moreover, adult services can often be convenient ways for bad-faith actors to publish non-consensual intimate or sexual images of those whom they want to harass, or abuse.

(19) Third, Technius is mistaken in asserting that its platform could not possibly pose systemic risks to freedom of expression. The dissemination of pornographic material is inherently intertwined with freedom of expression. The content moderation rules and practices employed by adult sites may significantly restrict the expression rights of their users, raising questions of proportionality and fairness.

(20) In addition, more poignantly, ARTICLE 19 has been active for years on the issues of gender-based violence and other similar forms of abuse – specifically because they pose serious risks to freedom of expression. Online abuse is often motivated by the goal of suppressing voices. For instance, it is a proven fact that female journalists are disproportionately exposed to sexualised and

other forms of abuse online. Such abuse often takes the form of (a) sharing content portraying women as sexual objects, (b) impersonating a woman's online presence and/or using the content to discredit her or damage her reputation, or (c) non-consensual distribution of intimate or sexual images of a woman. Thus, compliance with risk management and data access obligations by adult sites with large user bases like Stripchat can act as an important safeguard protecting women against retaliation (for evidence, see also Annex A.5 of the (original) Application).

(21) Furthermore, Stripchat's potential risks are not limited to those specific to platforms disseminating pornographic content. As the Commission outlined in its Defense, Article 34 of the DSA explicitly addresses systemic risks stemming from a platform's systems and processes. These risks are not solely tied to the nature of the content but also to the design and operation of the platform itself. For instance, issues related to advertised content, the use of dark patterns, hidden subscriptions, and data-sharing practices present significant risks to a range of fundamental rights, including freedom of expression. ARTICLE 19 has similarly underscored the potential adverse implications of these practices on freedom of expression.

(22) In conclusion, Stripchat is capable of posing societal risks that justify the imposition of enhanced due diligence obligations under the DSA. These obligations are within the legislative purview of the DSA and cannot be in principle considered an infringement on the applicant's right to conduct a business under Article 16 of the Charter or a violation of the principle of proportionality under Article 52 of the Charter. For this to be true, the obligation to assess risks that are in the DSA's scope, and subsequently to act upon them, would have to be in itself in violation of the EU Charter. Given that many other areas of law are subject to similar obligations (e.g., data protection law, or finance), it is hard to see this argument as anywhere near convincing.

(23) That is not to say that actions adopted on the basis of Articles 34 and 35 DSA can never amount to violations of Articles 16 or 52 of the EU Charter. However, it is only individual obligations imposed by the European Commission on the basis of those provisions, such as commitments, interim measures, or fines, that can constitute such interference. Articles 34 and 35 DSA emphasise that the Commission must comply with fundamental rights in order to enforce them lawfully:

- Article 34 states that '[the] risk assessment shall be specific to [VLOPs and VLOSEs] services and *proportionate* to the systemic risks, taking into consideration their severity and probability' (emphasis ours)

- Article 35 states that VLOPs 'shall put in place reasonable, *proportionate* and effective mitigation measures, tailored to the specific systemic risks identified' (emphasis ours)
- Recital 30 also requires that Article 8 DSA is complied with when applying the above provisions ('Nothing in this Regulation should be construed as an imposition of a general monitoring obligation or a general active fact-finding obligation, or as a general obligation for providers to take proactive measures in relation to illegal content').

(24) The DSA's design sufficiently distinguishes by severity, probability, and extent of risks. It does it on the level of actual obligations that VLOPs owe to the public. Thus, it is incorrect to say that the DSA fails to appreciate these aspects. **While the DSA does not consider severity, probability, and extent of risks as relevant for designation, after the designation, it adjusts the scope of materials obligations based on these factors.** Thus, if it is true that Stripchat poses fewer risks to adults, children, consumers, and others, this will translate into a much less extensive need to act to mitigate such risks (Articles 34 and 35).

(25) The main design principle of the DSA is it is impossible to foresee upfront all the risks that specific services might pose to the public. The legislature adopted the DSA in response to these large **information asymmetries** surrounding digital services. The designation process therefore only uses the number of users as the only proxy for likely impact on society. This does not imply that all types of digital services with the same numbers will be subject to the same substantive mitigation obligations. The scope of actual obligations will depend on the actual assessment of the risks that must be carried out by companies like Technius, and the findings of researchers, auditors, and regulators. The DSA, through the designation process, only "**onboards**" Technius among the more scrutinised digital services due to its market success in the European Union. The enhanced scrutiny of designated services entails a certain level of compliance costs. But that is a price that Technius pays for serving large parts of the European population.

C. Order sought

(26) Based on the above, ARTICLE 19 supports the European Commission in its request to the General Court to **dismiss** the action of Technius in its entirety.

3-12-2024
Košice, Slovakia

Kind Regards
Martin Husovec, attorney at law