POSITION PAPER ON THE DIGITAL SERVICES ACT (DSA)

TOGETHER AGAINST COUNTERFEITING (TAC) ALLIANCE

March 2021

The Commission's proposal for a **Digital Services Act (DSA)** Regulation represents a step forward to create a safe and trustworthy online ecosystem. However, **the Together Against Counterfeiting (TAC) Alliance calls on the European Parliament and the Member States to raise the level of ambition of the text to fully ensure a counterfeit-free online environment.** Among others, we encourage policymakers to further strengthen the text by clarifying the distinction between active and passive intermediaries and adding adequate obligations to implement proactive and stay-down measures against illegal content.

The manufacturing, supply and trade of counterfeit goods is a criminal offence under EU law. Yet, online counterfeiting continues to put European consumers' safety at risk and undermine their trust. In 2019, counterfeit products represented 6,8% of all EU imports by value[1], growing by almost 40% compared to 2016[2]. Just looking at eleven economic sectors, the EUIPO found counterfeiting represented a EUR 50 billion annual revenue loss for rights holders (6.4% of EU direct sales for these sectors), translating into 671 435 jobs[3] losses, and € 14.57 billion worth of unpaid taxes and social contributions for EU governments. The situation has further deteriorated during the pandemic, which led to an increase in online scams advertising fake and dangerous medical equipment.

Today, no physical store owner selling counterfeits would escape being held accountable. The DSA should guarantee the same principles, to ensure that "what is illegal offline be illegal online". This is not about restricting freedom of expression but merely to ensure that traders only sell legal goods in a trustworthy and safe environment for consumers.

THE DSA: A GOOD REGULATORY BASIS TO BETTER FIGHT AGAINST COUNTERFEITING ONLINE...

The DSA puts forward some encouraging proposals that will help better address illegal content:

- **The Know Your Business Customer (KYBC) principle and the obligation for all intermediaries to appoint a legal representative in the EU**, will help fight against the anonymity of sellers online and support businesses and authorities in adequately tracing back and prosecuting those conducting illegal activities. However, the scope of the KYBC provision should be widened *(see section below)*.
- **The harmonisation of notice and action procedures for hosting service providers across the EU, as well as the possibility to notify several illegal listings in one notice** will certainly help address the existing framework's lack of efficiency. The obligation for hosting service providers to send a confirmation of receipt of the notice and later, to inform the notifier of the decision taken are clear improvements..
- **The creation of additional obligations for "very large online platforms"** (VLOPs) will be useful to assess the systemic risks of their services being misused for disseminating illegal content and the need to mitigate those risks effectively. However, these requirements should not be limited to the largest intermediaries and should also apply to other platforms *(see below)*.

... BUT A PROPOSAL THAT NEEDS TO BE SIGNIFICANTLY IMPROVED TO BE FULLY EFFECTIVE

Having outlined the above, many provisions are still insufficient to curb the growing presence of counterfeits online and to ensure a safe digital environment. TAC members believe that the following areas should be either clarified, improved, or considered altogether in the context of the upcoming negotiations in the European Parliament and the Council.

1. EXTENDING THE KNOW YOUR BUSINESS COSTUMER (KYBC) PRINCIPLE

The KYBC principle, as laid down in Article 22 of the proposal, should apply to all online intermediaries engaged in the promotion of a product, including those providing B2B services (such as advertising or domain registrars), and not just to online marketplaces or consumer-facing platforms. In addition to consumers knowing whom they are buying from, intermediaries should know the identity of their commercial partners (whom they are receiving money from). Many platforms are already implementing such mechanisms and have the technical means to do so. This principle also exists in several other sectors (e.g. payment service providers and other obliged entities under the Anti-Money Laundering Directive) and is essential to bringing more accountability and transparency across the supply chain. Without a verified identity, consumers and right owners will be deprived of effective redress mechanisms.

Furthermore, the provision should be strengthened, as the current text leaves room for business users to escape KYBC obligations by simply presenting themselves as private sellers. The article should include safeguards to ensure private sellers are genuine. This would also contribute to fighting tax evasion and money laundering committed by fraudulent online businesses.

1. OECD, EUIPO, Illicit Trade - Trends in Trade and in Counterfeit and Pirated Goods, 2019
2. OECD, EUIPO, Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact, 2016
3. EUIPO, Status Report on IPR infringement, 2020
4. EUIPO, Status Report on IPR Infringement, 2019

Finally, we believe Article 22 should include a process to ensure the information collected and verified by the intermediary is updated if and when necessary, and require the intermediary to keep the verified information for as long as necessary under applicable statutes of limitations[5].

2. ENSURING COUNTERFEITS AND THEIR SELLERS "STAY DOWN"

Harmonised notice and action procedures should not be solely based on reactive efforts. The process is very burdensome and time-consuming for rightsholders, as the treatment period of our notices varies from a couple of hours to a month, or to no treatment at all. Most importantly, once taken down, illegal goods almost instantaneously reappear, often on the same platforms, and consumers are left exposed.

The measures and protections against traders' repeated misuses (Article 20) are a first response. However, these obligations should be (i) strengthened and (ii) complemented by an obligation for intermediaries to make sure illegal content stays down:

(i) Article 20 should be amended, to introduce a permanent suspension of repeated offenders, not just suspension for a "reasonable period of time", and a threshold for automatic suspension -and eventually ban- of their account. Most counterfeit sellers are repeat infringers, acting at commercial scale, often combining the sale of counterfeits with other criminal activities. Today, some online platforms already implement such policies, applying for example a "three-strikes" rule against repeat infringers. It is therefore easy for all intermediaries to apply this policy. Furthermore, a minimum set of information to be included in platforms' terms and conditions, as set out in paragraph 4 of Article 20, should be clearly laid down in the Digital Services Act or subsequent guidelines, in particular to clarify which practices constitute a "misuse".

(ii) In addition to suspending illegal traders, the DSA should include a "best effort" requirement for all hosting service providers to prevent the reappearance of illegal listings. TAC members report daily a large number of reappearing illegal goods, which often take the form of similar ads leading to the same website URL or to identical content and websites that keep reappearing on the same platform, including under different names ("back-up accounts"). These suggested *stay-down* measures should apply when content has already been removed by the platform in absence of any appeal. Where appropriate and where there is a defined distribution channel, platforms should also target identical or equivalent content, as already outlined in case law Eva Glawischnig-Piesczek v. Facebook[6]. This is the most effective solution to manage and prevent the reappearance of illegal goods and related content (e.g. creative visuals), and a crucial step to ensure consumers do not perpetually face products that can endanger their health and safety.

3. INTRODUCING STRENGTHENED PROACTIVE MEASURES AGAINST ILLEGAL CONTENT

TAC members regret that the proposal does not include a general requirement for all intermediaries to proactively detect and remove illegal content.

The introduction of stronger proactive obligations for Very Large Online Platforms (VLOPs) will not be sufficient to tackle the counterfeiting phenomenon in its entirety. A more stringent regime should be applied to ***all*** online platforms.

First, we call for extending the scope of Articles 26 and 27 to *all* online platforms, namely the obligations to mitigate *"any significant systemic risks stemming from the functioning and use made of their services"*. Some intermediaries already implement such measures and, in general, they have the ability, the know-how and the means to adopt them. Risk assessment is proportionate to the size of the platform and should not constitute a burden for smaller players. Platforms should always take action to mitigate a systemic risk after identifying it, as it is the same for consumers, regardless of the size of the platform.

Second, the voluntary measures provision in Article 6 should be clarified, as it currently does not incentivize intermediaries to put their best efforts against illegal content. In effect, it rather provides them a safe harbour for their wilful blindness, as the scope of the liability exemption and its conditions remain unclear, vague and unnecessarily broad.

We therefore recommend to better define the scope of the voluntary measures provision, by clarifying that intermediaries can continue to benefit from a liability exemption only if they implement specific measures in response to or to mitigate the effects of illegalities or risks identified in accordance with Articles 26 and 27, provided these articles apply to all online platforms (see above). Such a provision would ensure an effective and horizontal framework for all players, to avoid giving an unfair advantage to less virtuous platforms. It would also be proportionate, flexible and future-proof, as intermediaries could adjust their tools as new services and practices emerge.

5. In the current version of the proposal, the online platform is required to delete the information once the relationship with the trader is terminated, which makes it impossible for consumers or rights owners to bring action against an identified seller once his account has been terminated.

6. C-18/18, Eva Glawischnig-Piesczek v Facebook Ireland Limited: the jurisprudence lays down that "it is legitimate for the court to be able to require that host provider to block access to the information stored, the content of which is identical to the content previously declared to be illegal, or to remove that information". It further indicates that stay-down obligations are not considered "excessive" and against the absence of a general monitoring obligation, "in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified (...), and (...) does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies.

4. STRONGER SANCTIONS SHOULD BE APPLIED

The DSA proposal lays down various sanctions for non-compliance with the Regulation, which are at the moment only financial. We believe these will not be a sufficient deterrent.

The Commission's proposal identifies very clearly that the exemption from liability for intermediaries is conditional (Article 1.1.a), but it is not clear from the text how this exemption could be lost. **It is important to clarify that the exemption is not simply assumed, and impossible to remove from intermediaries who systematically do not comply with the obligations in the DSA.** Digital Services Coordinators should be able to include this in the list of possible sanctions in situations where intermediaries repeatedly fail to implement key parts of the law, such as effective notice and action, or proper verification of sellers.

In the offline world, a physical shop found to be selling counterfeits would immediately face legal actions; such a measure would simply put online shops on an equal footing, and ensure "what is illegal offline is also illegal online".

5. RIGHTSHOLDERS SHOULD BE ELIGIBLE AS TRUSTED FLAGGERS (ARTICLE 19)

Brand owners are the ***best*** placed to assess the validity and scope of protection of their IP rights, as each of them have the "particular expertise and competence" to detect infringements on their own products. **They should benefit from the trusted flagger status as long as appropriate safeguards remain in place**. Many platforms already have similar systems, allowing for faster takedown processes and less administrative burden for both brands and platforms. As part of those existing programs, trusted rightsholders need to have a solid track record of high-quality infringement reporting. Based on our members' experience, such schemes have also helped platforms better allocate their resources and allowed them to tackle more complex types of illegal content.

6. THE DSA SHOULD IMPROVE CONSUMER INFORMATION

Fighting counterfeiting is a matter of consumer protection, and the EU and national authorities should improve information to consumers on their online purchases. **TAC suggests introducing additional notification requirements for platforms to inform consumers who have bought identified counterfeit products on their website.**

7. TYPES AND ROLES OF INTERMEDIARIES SHOULD BE BETTER DEFINED

We welcome the clarification in the proposal's recitals that **intermediaries playing an "active" role** should not benefit from the exemption of liability, in line with the European Court of Justice's jurisprudence. However, this role should be defined in the core proposal, to ensure legal certainty. A definition could be added to Article 2, based on existing jurisprudence (e.g. L'Oréal-eBay case[7]).

In addition, we suggest to clarify which category **domain name registrars and registries** belong to. We believe they should be considered as hosting providers and be subject to the same obligations, as they can play an active role in preventing the (re)appearance of counterfeits online.

Similarly, **search engines** should also face the same obligations as hosting providers. They have so far failed to develop effective reporting systems for de-indexing fraudulent websites selling counterfeits in search results. These websites, often advertising on social media, copy the aesthetics of brand owners' official sites and product catalogues and continue to mislead and put consumers at risk.

ABOUT US

The **Together Against Counterfeiting (TAC) Alliance** brings together almost 100 companies from all industrial sectors, with the support of over 20 trade associations and NGOs. Our purpose is to raise awareness about the impact of the worrying growth of counterfeiting and push for the adoption of immediate, horizontal and ambitious legislative solutions at European level.

Learn more about the Alliance: https://tacalliance.eu/

7. C-324/09 L'Oréal SA and Others v eBay International AG and Others: : the jurisprudence considers an operator plays an "active role", "which gives it knowledge of or control over the data relating to the offers for sale", "when it provides assistance such as optimising the presentation of the online offers for sale or promoting those offers". When an operator has played an active role of that kind, it can no longer rely on the exemption from liability laid down in Article 14(1) of the E-Commerce Directive (2000/31/EC)