DIGITAL SERVICES ACT/ REVISION OF THE E-COMMERCE DIRECTIVE COMMENTS FROM AFEP

As part of the Digital Services Act, the Commission intends to revise Directive 2000/31 on electronic commerce by the end of the year. This 20-year-old legislative framework imperfectly responds to new digital behaviours and uses (new distribution channels for the benefit of businesses of all sizes, strong growth in volumes of trade and illegal content) as well as the emergence of new and powerful economic players (platforms, social networks, etc.).

AFEP asks for **an update of this text to strengthen its legal certainty** while preserving some of its most structuring principles. To do so, it supports the drafting of **a regulation** to harmonise these new provisions and to reinforce consumer confidence within the single market, which must be equivalent to the one within physical trade.

This review is an opportunity **to clarify the conditions that must be met by digital players to qualify as hosts so to be subject to an appropriate liability regime**.

1. Confirm certain principles and definitions

- The definition of **information society services**: it includes any service normally offered for remuneration, remotely by electronic means and at the individual request of a recipient of services.

- The definition of "**illegal content**"[1]: it includes any information which is not in compliance with Union law or the law of a Member State concerned. It is key for the e-commerce review and the Digital Services Act to focus on illegal content and not harmful content, which should be dealt with separately. Focusing on illegal content, as defined by the Commission 2018 recommendation, would allow more legal certainty as well as faster and easier implementation of measures.

- Maintain the **principle of limited liability** (Articles 12, 13 and 14 of the directive) of hosting service providers while clarifying its scope.

- Preserve the **principle of no general monitoring obligation** (Article 15) to protect simple technically neutral intermediate operators ("passive hosts"[2]) while adapting it to the digital boom. **In this context, clarifications are proposed (see III).**

2. Extend the scope of the E-commerce directive to hosting services providers established outside the EU and to providers of all sizes

- **Extension of the scope to hosting service providers established outside of the EU**

The e-commerce directive is currently based on the country of origin principle (Article 3). It requires Member States to ensure that information society services provided by a service provider established in their territory comply with national provisions without restricting the free movement of these services between states.

1. Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online.
2. The role of which is, according to recital 42 of the E-commerce directive, "mere technical, automatic and passive".

Therefore, providers established outside of the EU but providing services on European territory are not subject to the obligations of the directive.

To ensure effective protection of European consumers and holders of intellectual property rights, as well as the conditions for fair competition between players in e-commerce, it is necessary to **extend the scope** to services supplied to **recipients on European territory, by a provider who is not established in the Union**[3].

- **Extension of the scope to hosting services providers of all sizes**

The future text should apply to all actors, **regardless of their size**, if they are engaged in hosting services that are likely to create risks for the recipients of the service. The ***erga omnes* application** of the rules on electronic commerce will make it possible to fight the proliferation of intermediaries taking advantage of the sale of counterfeit products to grow at the expense of the economy in general and of consumer protection in particular.

However, the scope of these obligations should be proportionate, adaptable to the size of the company and to the degree of control it has over the content/goods that it hosts.

3. Clarify the concept of host and the corresponding liability regime by establishing a duty of vigilance

If the **principle of limited liability** of hosting providers must be maintained (articles 12 to 14), the evolution and the complexity of digital actors for the last 20 years **require clarification of this legal framework.**

The numerous economic benefits of digital technology are indeed accompanied by a proliferation of illegal content on the Internet (incitement to hatred, child pornography, counterfeiting, parallel trade). This requires a **review of the qualification of a host**, to better define the actors who can benefit from a modified liability regime. This revision must take into account the case-law of the CJEU and impose a **duty of vigilance on the concerned digital market players to secure their online services activities**.

An update is therefore required in the following ways:

- Consider the Internet as a commercial vehicle where the rights of any interested party (consumers, holders of intellectual property rights, etc.) must be ensured with a **level of protection equivalent to that existing in physical sales points**: as in any commercial relationship, **professional sellers using digital platforms** acting under a pseudonym must be able to be **identified**[4] **through verification of the concerned platform** ***(Know your business Customer principle);***
- Subject all online platforms with the ability to moderate content and disseminating content to the public to an **obligation of means**, to **prevent the appearance and reappearance of illegal content, goods and services**, as massive contents on platforms do not allow for an obligation of results. Measures should be imposed on platforms to introduce a "**notice and stay down" mechanism**. The 2019 ruling of the CJUE (C-18/18 Glawischnig-Piesczek v Facebook) determines that obligations can be imposed on platforms to proactively monitor content and then interpret if it is 'equivalent' to content that has been previously found to be illegal This, however, should be **only an obligation of means and not results**, so to allow flexibility and proportionality for platforms.

3. See in this sense the 2018 Recommendation which defines a hosting service provider "irrespective of its place of establishment, which directs its activities to consumers residing in the Union" and the proposal for a Commission regulation on the fight against terrorist content online, which applies "to hosting service providers offering services in the Union, irrespective of their place of main establishment"
4. "What is illegal offline is also online", Communication from the European Commission on combating illegal content online, 28 September 2017.

- All platforms should be transparent about their content policies, measures and effects. to the regulators upon requests. Automated tools used to detect illegal content, goods or services are useful and already implemented by major platforms. However, these tools can encompass bias, either voluntary or not, and allow the upload of content which should be blocked. In order to tackle this issue, more effective cooperation and audit mechanisms between the competent regulatory authority and the very large gatekeeping platforms should be implemented so that such platforms are regularly able to explain how these tools detect illegal content and demonstrate that they are not biased.
- Integrate the case-law establishing the conditions under which intermediaries would become active hosts, hence not able to claim the protection of article 14 and thus calling into question their non-liability, when they distribute/make their content accessible to the public and:

  – their activity goes beyond simple storage and transmission of data: they have visibility and control over this data by selecting, using, modifying and/or editing it to optimize or promote it[5] or
  – they refuse control over the processed content while this control is technically and contractually[6] possible;

Consequently, passive intermediaries, in particular cloud infrastructure services, should maintain their non-liable scheme. Cloud infrastructure services have indeed no control over hosted content due to legal (contractual clauses) and technical (lack of access and encrypted data) barriers.

- Assess the responsibility of active hosts as soon as they have fulfilled their duty of vigilance for all their activities, implying an obligation of means to remedy the violations of rights on their platform. To do this, the hosts must set up an adapted vigilance plan, the practical modalities of which must be established by the national authorities and regulators concerned, in consultation with the stakeholders. This vigilance plan is based on the following four principles:

  – identify the risks: list the risks identified (internal "risk mapping", generated by the active host itself, and external risks, induced by the users of the platform) and the use of appropriate tools (impact studies, risk analyses, etc.);
  – prevent infringements: application of effective ex-ante measures on a voluntary basis (consistency of the bundles of concordant indices resulting from a collaboration program with rights holders, for example), proportionate and specific (depending on the business model, of the technical capacities of the service provider such as filtering or blocking ...);
  – remedy the negative consequences: recognition of the facts, commitment to improvements, possibility for the active host to use its influence so that the business relationship evolves and thus put an end to the violation of intellectual property rights;
  – report on the way they remedy it: obligation of regular transparency on the measures adopted based on numerous indices (origin of the product declared by the seller, the reputation of the seller, identification, etc.) vis-à-vis the intellectual property rights holders, as soon as they have notified the host of illegal content or participate in a collaboration program with the host.

  The introduction of this duty of vigilance would thus induce a responsibility of active hosts not for the existence of illegal content on their sites but because of the absence of implementation of a vigilance plan, which would include both ex-ante control measures and reactivity after notification. In the event of litigation, it would be up to the judge to assess the implementation of his duty of vigilance concerning the content in question, per with the most recent case-law. AFEP is opposed to the "good Samaritan

5. CJUE, March 23, 2010, Google vs LVMH. In 2011, the CJEU considered regarding a marketplace that "the said operator plays an [active role] when it provides assistance which consists in particular in optimizing the presentation of offers for the sale in question or in promoting it". CJEU, July 12, 2011, L'Oréal c / eBay.
6. Certain hosts such as cloud services between companies (B2B Cloud) and cloud infrastructures do not hold any contractual rights over how these contents are treated or made available to the public by their customers or the end-users of their clients ; or do not have the technical capacity to delete content stored by their customers or by the end-users of their services. These hosts, therefore, remain passive.

clause". The platforms are not sufficiently encouraged to set up proactive measures to fight against illegal contents. It would give online intermediaries exemptions from liability for any proactive removals they may decide to make, while not being necessary more efficient, and without any type of control on the measures taken. It would put at risks the users that the legislation seeks to protect.

- If fines are to be used, they must be deterrent, effective, proportionate and applied on a case by case basis, instead of automatically. Different criteria would be considered as aggravating factors (intentional infringement, failure to take measures to mitigate the damage incurred…). Effective enforcement should target third-country players to the same extent as the players established in the Union.

*

ABOUT AFEP

Since 1982, AFEP brings together large companies operating in France. The Association, based in Paris and Brussels, aims to foster a business-friendly environment and to present the company members' vision to French public authorities, European institutions and international organisations. Restoring business competitiveness to achieve growth and sustainable employment in Europe and tackle the challenges of globalisation is AFEP's core priority. AFEP has around 113 members. More than 8 million people are employed by AFEP companies and their annual combined turnover amounts to €2,600 billion.

Emmanuelle Flament-Mascaret - Director of Business Affairs and Intellectual Property
concurrence@afep.com

Justine Richard-Morin – Deputy Director for European Affairs
j.richard-morin@afep.com