# DIGITAL SERVICES ACT
# AFEP POSITION ON THE COMMISSION'S PROPOSAL

**AFEP welcomes the Digital Services Act proposal**. The 20-year-old e-commerce Directive framework imperfectly responded 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.

AFEP welcomes the extension of the scope to service supplied to **recipients on European territory, by a provider who is not established in the Union**. It will ensure the effective protection of European consumers and holders of intellectual property rights, as well as the conditions for fair competition between players in e-commerce.

AFEP also supports the extension of the scope to service providers of all sizes. 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 illegal products to grow at the expense of the economy in general and of consumer protection in particular. However, the scope of these obligations should remain proportionate, adaptable to the size of the company and to the degree of control it has over the content/goods that it hosts.

Finally, it is key for 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.

AFEP proposals, detailed in the annexe, can be summarised as such:

- **Clarify the concept of host**, including of neutrality, and the **corresponding liability regime** (Articles 3 to 5);
- **Liability must be determined not for the existence of illegal content on their sites, but for the failure to implement a vigilance plan**, which would **include both ex-ante control measures obligations for all intermediaries and reactivity after notification**. In that sense:
    - In any commercial relationship, **professional sellers using digital platforms** acting under a pseudonym must be able to be **identified**[1] **through verification of the concerned platform** (***Know your business Customer principle***). AFEP supports the **obligation**

[1] 1. What is illegal offline is also online", Communication from the European Commission on combating illegal content online, 28 September 2017.

for all intermediaries to identify service providers prior to them engaging in commercial transaction and/or promotion of a product/service. *AFEP, therefore, recommends that Article 22 (Traceability of traders) be moved to Section 1 of Chapter III.*

- Subject all hosting intermediaries 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 CJEU (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. *See AFEP proposal to Article 14.*
- Provisions from Section III should target all online platforms, with adjustments allowed for micro and small enterprises so to avoid excessive burden. The European Commission could advise on these adjustments.
  Moreover, except for cloud providers, all platforms should have to identify significant systemic risks stemming from the functioning and use of their services. The resulting mitigation measures should however remain reasonable, proportionate and tailored to the risk identified and the size, role and level of product information hold by the provider. The European Commission could advise on these assessment, mitigation measures and reporting. *See AFEP proposals to Section 3 and 4 of Chapter III.*

- To secure online commerce and ensure that there is no bias, additional transparency obligations are needed for very large online platforms on their recommender and moderation systems, upon request of the regulator (Commission or Digital Services Coordinators). *See AFEP proposal to Article 31.*

**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 more than 110 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 Economic Law - concurrence@afep.com
Alix Fontaine – EU Policy Advisor - a.fontaine@afep.com

# DIGITAL SERVICES ACT
## Annex: AFEP proposals

- Chapter I: General provisions

| Commission's proposal | AFEP proposals |
|---|---|
| Article 2<br>Definitions<br><br>(i)'dissemination to the public' means making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties; | Article 2<br>Definitions<br><br>(i) 'dissemination to the public' means making information available, at the request of the recipient of the service who provided the information, to a potentially unlimited number of third parties, ***without further action by the content provider being required, irrespective of whether those persons actually access the information in question;*** |

*Justification*

The definition of "Dissemination to the public" in Article 2(i) and its interpretation in the corresponding Recital 14 must be clearly consistent with the agreed wording of the Terrorist Content Regulation (TCO, Recital 10a).

The DSA should provide clear guidance by clarifying that cloud service providers do not perform an act of communication to the public within the meaning of the DSA. In this respect, an alignment with the notion of dissemination to the public in the TCO Regulation should be made. It says that in its Recitals that "providers of services such as cloud infrastructure, which are provided at the request of other parties than the content providers and only indirectly benefit the latter, should not be covered."

- Chapter II: Liability of providers of intermediary services

| Commission's proposal | AFEP proposals |
|---|---|
| Article 5<br>Hosting<br><br>1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider:<br><br>(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or<br>(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content. | Article 5<br>Hosting<br><br>1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service the service provider shall not be liable for the information stored at the request of a recipient of the service on condition that the provider:<br><br>(a) ***has no visibility to the information stored and*** does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or<br>(b) upon obtaining such knowledge or awareness, ***be it from its own investigations, notices submitted to it by individuals or entities, or injunctions,*** acts expeditiously to remove or to disable access to the illegal content ***or (c) it provides the services neutrally.*** |

*Justification*

**AFEP welcomes the keeping of the principle of limited liability**. The DSA largely restates the safe harbours from liability for intermediary services—namely, caching services, mere conduits, and hosting services—set out in the e-commerce Directive. **Chapter II includes the conditions under which these providers are exempt from liability**.

**However, better clarification can still be reached on some of the conditions,** including of **neutrality**, that must be met by digital players to benefit from limited liability, with better consideration of criteria from European case law (L'Oréal C-324/09, The Pirate Bay C-610/15, GS Media C-160/15…) and from the Communication 555/2017 on tackling illegal content online from the Commission.

Building on this notion of neutral hosting provider provided by the CJEU, hosts with no visibility to content, such as **cloud providers**, should automatically benefit from the limited liability principle. **A Recital could be added in that sense in addition to our proposal in Article 5.**

Moreover, it is important that a **hosting service provider should not claim safe harbour protection when**:

- it plays **a non-neutral role** instead of confining itself to providing the services neutrally
- provides the **service itself,** as underlined in Recital 18,
- or **collaborates with a recipient of the service**, see Recital 20.

This point however has to be **cumulated with the main principles of due diligence –see Art. 14 and section 3.**
To be certain of the neutrality of the provider and to support accountable digital behaviours, **Digital Services Coordinators (DSCs) should be entitled to have access to all data requested for their investigation to make sure that very large online platforms are DSA compliant**. See our proposals to Art. 31.

| Commission's proposal | AFEP proposals |
|---|---|
| Article 6<br>Voluntary own-initiative investigations and legal compliance<br><br>Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 solely because they carry out voluntary own initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation. | Article 6<br>Voluntary own-initiative investigations and legal compliance<br><br>Providers of intermediary services shall not be deemed ineligible for the exemptions from liability referred to in Articles 3, 4 and 5 solely because they carry out voluntary own initiative investigations or other activities aimed at detecting, identifying and removing, or disabling of access to, illegal content, or take the necessary measures to comply with the requirements of Union law, including those set out in this Regulation.<br><br>*This Article is without prejudice to the rules laid down in Articles 4 and 5 and to obligations of due diligence for all providers under Chapter III of this Regulation.* |

*Justification*

AFEP does not call into question this Article but proposes that the **liability be determined not for the existence of illegal content on their sites, but for the failure to implement a vigilance plan, including mandatory ex ante measures**.

The **platforms are today not sufficiently encouraged to set up proactive measures to fight against illegal contents.** A non-balanced Article 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. Such unclear legislation on what intermediaries have to do could hence result in intermediaries being the judge and jury of the efficiency of their voluntary measures and in insufficient results. It would put at risks the users that the legislation seeks to protect.

Illegal content online has become a matter of consumer protection, and intermediaries need to prevent the appearance of such content. **Pro-active measures obligations -of means- must therefore be reintroduced for all non-neutral intermediaries and not only very large platforms**, in order to balance this Article. **See our amendments to Article 6 and to Chapter III in that sense.**

- Chapter III: Due diligence obligations for a transparent and safe online environment

  - Section 1: Provisions applicable to all providers of intermediary services

| Commission's proposal | AFEP proposals |
|---|---|
| Article 22<br>Traceability of traders<br><br>1. Where an online platform allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information:<br><br>(…) | Article ~~22~~ *13a*<br>Traceability of traders<br><br>1. Where an ~~online platform~~ ***intermediary service provider*** allows consumers to conclude distance contracts with traders, it shall ensure that traders can only use its services to promote messages on or to offer products or services to consumers located in the Union if, prior to the use of its services, the online platform has obtained the following information:<br><br>(…) |

*Justification*

AFEP supports the obligation for all intermediaries to identify service providers prior to them engaging in commercial transaction and/or promotion of a product/service.

AFEP therefore recommends that Article 22 be moved to section 1.

- Section 2: additional provisions applicable to providers of hosting services, including online platforms

| Commission's proposal | AFEP proposals |
|---|---|
| Article 14<br>Notice and action mechanisms<br><br>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.<br><br>(…) | Article 14<br>Notice and action mechanisms<br><br>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.<br><br>(…)<br><br>*7 (new) All providers of hosting services with the ability to moderate content and disseminating content to the public should be subject to an obligation of means to prevent the appearance and reappearance of identical or equivalent illegal content, goods and services, as massive amount of contents and the limits of the technical tools do not allow for an obligation of results.*<br><br>8 *(new) All providers of hosting services should inform users who have bought illegal product or content, once it has been definitely removed from their platform following a valid notification from a trusted flagger.* |

*Justification*

AFEP recommends an **obligation of means** to remedy the violations of rights: although no general monitoring obligation should be introduced, **all provider of hosting services should implement pro-active measures to detect illegal content**, according to their size and role and the level of product information they hold.

Specific tools based on objective criteria exist that detect the illegality of content before its publication and that do not conflict with the general monitoring ban, and the EU courts have already determined that **stay-down measures are not contrary to the no general monitoring obligation**.

IP concerns are also essentially different from freedom of speech issues, including the way they can be dealt with technically.

AFEP therefore supports the **introduction of a "notice and stay down"** obligation for all providers of hosting services in article 14 in order to avoid the specific reappearance of identical or equivalent illegal content (in line with CJEU judgment Oct 2019, Eva Glawischnig-Piesczek vs. Facebook). This **obligation should be an obligation of means and not of results**, given the quantity of content hosted and the existence of specific but nevertheless limited technical tools.

Providers of mere conduit and caching services are however prohibited (as they are subject to net neutrality rules) from actively searching for illegal content and would instead react to injunctions issued by public authorities.

AFEP moreover proposes that all providers of hosting services also have an **obligation to inform users that illegal content** has been removed **following a notice from a trusted flagger**.

(i) The inclusion of "illegal" wants to recall the DSA's right goal which is the fighting against the sales of illegal products or content.
(ii) To avoid any difficulty for providers of hosting services, this information would be only effective when the removal from the platform is non-contestable and definitive.

See Art 19. 2- b) related to the addition of IP right-holders companies within the definition of a trusted flagger.

- Section 3: additional provisions applicable to online platforms

| Commission's proposal | AFEP proposals |
|---|---|
| Article 16<br><br>Exclusion for micro and small enterprises<br><br>This Section shall not apply to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC | Article 16<br><br>***Adjustments*** ~~Exclusions~~ for micro and small enterprises<br><br>This Section shall ~~not~~ ***also*** apply ***in a proportionate, adapted manner*** to online platforms that qualify as micro or small enterprises within the meaning of the Annex to Recommendation 2003/361/EC |

*Justification*

These **provisions should apply to all platforms, with adjustments allowed for micro and small enterprises** so to avoid excessive burden. The European Commission could advise on these adjustments.

| Commission's proposal | AFEP proposals |
|---|---|
| Article 19<br><br>Trusted flaggers<br><br>1. Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.<br><br>2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions: | Article 19<br><br>Trusted flaggers<br><br>1. Online platforms shall take the necessary technical and organisational measures to ensure that notices submitted by trusted flaggers through the mechanisms referred to in Article 14, are processed and decided upon with priority and without delay.<br><br>2. The status of trusted flaggers under this Regulation shall be awarded, upon application by any entities, by the Digital Services Coordinator of the Member State in which the applicant is established, where the applicant has demonstrated to meet all of the following conditions: |

| | |
|---|---|
| (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;<br><br>(b) it represents collective interests and is independent from any online platform;<br><br>(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.<br><br>(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner. | (a) it has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content;<br><br>(b) it represents ***IP right holders and/or*** collective interests and is independent from any online platform;<br><br>(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner.<br><br>(c) it carries out its activities for the purposes of submitting notices in a timely, diligent and objective manner. |

*Justification*

The Regulation should also make clear that trusted flaggers, as defined in Article 19, would include IP right-holders companies.

| Commission's proposal | AFEP proposals |
|---|---|
| Article 26<br><br>Risk assessment<br><br>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:<br><br>(a) the dissemination of illegal content through their services;<br>(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 | Article ***24 a***<br><br>Risk assessment<br><br>~~***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, ***proportional to their size and role and the level of product information they hold*** and shall include the following systemic risks:<br><br>(a) the dissemination of illegal content through their services;<br>(b) any negative effects for the exercise of the fundamental rights to respect for private and family life, freedom of expression and |

| | |
|---|---|
| child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively;<br>(c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.<br><br>When conducting risk assessments, very large online platforms shall take into account, in particular, how their content moderation systems, recommender systems and systems for selecting and displaying advertisement influence any of the systemic risks referred to in paragraph 1, including the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions. | information, the prohibition of discrimination and the rights of the child, as enshrined in Articles 7, 11, 21 and 24 of the Charter respectively;<br>(c) intentional manipulation of their service, including by means of inauthentic use or automated exploitation of the service, with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security.<br><br>When conducting risk assessments, ~~*very large*~~ online platforms shall take into account, in particular, how their content moderation systems, recommender systems and systems for selecting and displaying advertisement influence any of the systemic risks referred to in paragraph 1, including the potentially rapid and wide dissemination of illegal content and of information that is incompatible with their terms and conditions. |

*Justification*

It should be mandatory for all platforms to identify significant systemic risks stemming from the functioning and use of their services. The **resulting mitigation measures should however remain reasonable, proportionate and tailored to the risk identified and the size, role and the level of product information hold by the provider.** The European Commission could give advice on these assessment, mitigation measures and reporting.

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, with the most recent case-law.

**We therefore propose for Article 26 (risk assessment) and Article 27 (mitigation of risk) to be moved to Section 3, so to apply to all online platforms and amended accordingly. Auditing of report (Article 28) could be left to very large online platforms online.**

| Commission's proposal | AFEP proposals |
|---|---|
| Article 27<br>Mitigation | Article ***24b***<br>Mitigation |
| 1. Very large online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26. Such measures may include, where applicable:<br><br>(a) adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their services, or their terms and conditions;<br>(b) targeted measures aimed at limiting the display of advertisements in association with the service they provide;<br>(c) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;<br>(d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19;<br>(e) initiating or adjusting cooperation with other online platforms through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively. | 1 ~~*Very large*~~ Online platforms shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 26. Such measures may include, where applicable:<br><br>(a) adapting content moderation or recommender systems, their decision-making processes, the features or functioning of their services, or their terms and conditions;<br>(b) targeted measures aimed at limiting the display of advertisements in association with the service they provide;<br>(c) reinforcing the internal processes or supervision of any of their activities in particular as regards detection of systemic risk;<br>(d) initiating or adjusting cooperation with trusted flaggers in accordance with Article 19;<br>(e) initiating or adjusting cooperation with other online platforms through the codes of conduct and the crisis protocols referred to in Article 35 and 37 respectively. |
| 2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:<br><br>(a) identification and assessment of the most prominent and recurrent systemic risks reported by very large online platforms or identified through other information sources, in particular those provided in compliance with Article 31 and 33;<br>(b) best practices for very large online platforms to mitigate the systemic risks identified. | 2. The Board, in cooperation with the Commission, shall publish comprehensive reports, once a year, which shall include the following:<br><br>(a) identification and assessment of the most prominent and recurrent systemic risks reported by ~~*very large*~~ online platforms or identified through other information sources, in particular those provided in compliance with Article 31 and 33;<br>(b) best practices for ~~*very large*~~ online platforms to mitigate the systemic risks identified. |

| | |
|---|---|
| 3. The Commission, in cooperation with the Digital Services Coordinators, may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations | 3. The Commission, in cooperation with the Digital Services Coordinators, may issue general guidelines on the application of paragraph 1 in relation to specific risks, in particular to present best practices and recommend possible measures, having due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties involved. When preparing those guidelines the Commission shall organise public consultations. |

*Justification*

*Co-ordinated amendment. See the justification of the previous amendment.*

- Section 4: additional obligations for very large online platforms to manage systemic risks

| Commission's proposal | AFEP proposals |
|---|---|
| Article 31<br>Data access and scrutiny<br><br>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. | Article 31<br>Data access and scrutiny<br><br>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~~ ***without undue delay***, 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.<br><br>***1a Upon request of the Digital Service Coordinator or the Commission, very large online platforms shall provide them access to the detail of their*** |

| | |
|---|---|
| | *recommender and moderation systems, for the sole purpose of explaining how they are set to detect illegal content and demonstrating that there is no risk of bias.*<br>*When a bias is detected, very large online platforms should correct it expeditiously following requirements from the Digital Services Coordinator or the Commission.*<br>*Very large online platforms should be able to demonstrate their compliance at every step of the process pursuant to this Article.* |
| 2. Within 15 days following receipt of a request as referred to in paragraph 1 and 2, a very large online platform may request the Digital Services Coordinator of establishment or the Commission, as applicable, to amend the request, where it considers that it is unable to give access to the data requested because one of following two reasons:<br>(a)it does not have access to the data;<br>(b)giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets. | 2. Within 15 days following receipt of a request as referred to in paragraph 1 and 2, a very large online platform may request the Digital Services Coordinator of establishment or the Commission, as applicable, to amend the request, where it considers that it is unable to give access to the data requested because ~~*one of following two reasons*~~:<br>~~*(a)*~~it does not have access to the data;<br>~~*(b)giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets.*~~ |
| 3. Requests for amendment pursuant to point (b) of paragraph 6 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.<br><br>The Digital Services Coordinator of establishment or the Commission shall decide upon the request for amendment within 15 days and communicate to the very large online platform its decision and, where relevant, the amended request and the new time period to comply with the request. | 3. Requests for amendment pursuant to point (b) of paragraph 6 shall contain proposals for one or more alternative means through which access may be provided to the requested data or other data which are appropriate and sufficient for the purpose of the request.<br><br>The Digital Services Coordinator of establishment or the Commission shall decide upon the request for amendment within 15 days and communicate to the very large online platform its decision and, where relevant, the amended request and the new time period to comply with the request. |

*Justification*

AFEP supports the transparency and explanatory requirements of Articles 12, 28, 31, 54 and 57.

However, the impact assessment of the Commission showed that the lack of transparency in terms of how very large online platforms (VLOP) shape, rank and target information and advertising leads to major information asymmetries that affect behaviours and choices in the economy.

More effective cooperation and audit mechanisms between competent national and European regulatory authorities (the Digital Services Coordinator and the Commission) and the very large online platforms (VLOPs) should hence be implemented, upon request of the regulators, so that very large online platforms are regularly able to explain how automated tools detect illegal content and demonstrate that they are not biased. This additional algorithm transparency should target moderation and recommendation algorithms.

This disclosure should include all the data regarding the creation and the settings of these algorithms, such as corresponding datasets, explainability of algorithms, accountability and close cooperation with the Digital Services Coordinator (DSC) or the Commission. Should an algorithmic bias be detected, very large online platforms should correct it expeditiously, following requirements from the DSC or the Commission.

DSCs should be entitled to have access to all data requested for their investigation to make sure VLOPs are DSA compliant. Vetted researchers should be able to conduct studies on the DSA and thus require data to VLOPs. Nonetheless only the DSCs being national regulatory authorities (NRAs) provide the required guarantee to deal with highly sensitive data. Trade secret could be opposed to vetted researchers but is not justified for NRAs which already deal regularly with trade secrets to ensure proper compliance. An exception granted to VLOP would not be justified and would introduce a major loophole in the DSA implementation.

***