The Digital Services Act: Clarifying and Updating Responsibilities for Digital Services in the Single Market

At a glance summary

- The Commission should amend the eCommerce Directive to add new obligations to hosting providers who are actively involved in dissemination of information to the general public
- The DSA must preserve the underlying liability exemption for passive online intermediaries that is the foundation of a successful digital economy and target new obligations at large platforms who play an active role in dissemination of information or product/services
- "Active" hosting service providers should be required to take proactive measures:
    - Reform of notice and takedown rules (harmonisation, user friendliness)
    - Remove content identified as illegal by automated means or human flagging
    - Labelling, delisting/demotion of false or misleading claims
    - Increased use of fact checkers, trusted flaggers
    - Proactive monitoring to ensure that identical or similar instances of the same material are not re-uploaded by any user
    - Removal of fake accounts
    - Education and awareness raising and transparency reporting
- National regulatory authorities should enforce compliance with the new obligations and have the right to request data/impose fines for non-compliance.

Detailed views

The eCommerce Directive will soon be twenty years old. Since the law was adopted in 2000, the digital ecosystem has changed dramatically, with advent and evolution of social media platforms, which now act as primary channels for content, communication and commerce for millions of users. While the Directive has proved remarkably durable, its fundamental tenets and assumptions are now being tested to the very limit. This is primarily happening as new services and digital platforms enter the market that do not easily conform to the definitions and allocation of roles and responsibilities enshrined in that legislation. Legal ambiguities inherent in the Directive have been further compounded by a sprawling body of case law from the European Court of Justice, and attempts to legislate at a national level absent EU intervention, creating a patchwork of overlapping legal regimes attempting to regulate disseminate of illegal content within the Single Market.

We believe the Digital Services Act presents us with a generational opportunity to update the regulatory framework for digital services in Europe. Reopening and reinterpreting key legal concepts within that framework, to ensure they are fit for purpose and reflect the reality of how content is created and shared across the digital ecosystem today, with rights and responsibilities fairly attributed to digital services providers within the EU. Get this right and we believe the legal framework can endure for the next twenty years, preventing national fragmentation, preserving fundamental rights while at the same time ensuring a safer and healthier digital environment for EU citizens.

Our response to the DSA consultation is underpinned by three core legal principles:

- **Country of Origin Principle:** The country of origin principle is a cornerstone of the liability framework of the Digital Single Market and, as such, any new regulatory framework should maintain this principle. This should go hand in hand with the effort to further harmonise obligations across Member States. All service providers offering services in the EU should be subject to the EU rules, irrespective of their place of main establishment.
- **Liability Exemptions:** The underlying legal principle that certain online intermediaries (such as ISPs and other network access, caching and cloud services providers) are not directly liable for content they transmit or store at the request of users should be preserved. This is necessary to ensure the new rules are balances and proportionate, and target more far reaching obligations on service providers who are best placed to act. Vodafone considers that the definition of hosting service provider should be split into active and passive services. Active services should be subject to additional obligations to address illegal content over and above the current requirement to remove content once notified. Failure to comply should result in fines.
- **Prohibition on General Monitoring:** The prohibition on imposing a general monitoring obligation set out in Article 15 of the eCommerce Directive should be further clarified under the Digital Services Act to ensure an effective balance between fundamental rights to free expression, and the protection of end-users. Compatibility with Article 15 has to be ensured if active hosting service providers are obliged to take targeted pro-active measures to detect and remove illegal content.

Targeted & proportionate obligations: a new regime for Active Hosting Service Providers

When re-designing the regime of responsibility and liability in the Internet ecosystem, particular concern should be given to where the actual harm occurs and which participants are closest to counter such harm.

There should also be no change to liability regime for mere conduits under article 12 or caching under article 13. ISPs/caching providers should not be liable for content that they deliver, transmit or temporarily store as they have no control over this material (and indeed are prohibited from actively blocking content without a legal requirement to do so under the Open Internet Regulation). Under the eCD, ISPs are not subject to a notice and take down regime, but can receive blocking injunctions from a relevant authority/court. The Commission should issue guidance on the imposition of blocking injunctions to underline that such injunctions should always be a last resort (and in theory diminish over time as other actors take more responsibility for removing content).

The Commission should reopen and amend article 14 of eCD for hosting service providers recognising the emergence of a new category of 'active' hosts who play a direct role in dissemination, organisation and monetisation of end user content. Hosting service providers who do not cross this threshold should be subject to the same liability regime (safe harbour + notice and take down).

Active hosts should be subject to a binding legal obligation to ensure that their services are safe for users, through the application of a number of proactive measures that can prevent the dissemination of illegal content, goods and services and minimise the propagation of harmful material on their platform.

Application of these additional measures hinges on whether an online intermediary is playing an ‘active’ of ‘neutral/passive’ hosting function. Vodafone considers an active hosting service to

exhibit the following characteristics: instead of confining itself to providing a service neutrally by a merely technical and automatic processing of the data provided by its customers, the hosting service provider plays an active role of such a kind as to give it knowledge of, or control over, those data, for example by tagging, organising, promoting, optimizing, presenting or otherwise curating specific content for profit making purposes.

In this respect, the DSA should reinforce the cascade of responsibilities in fighting illegal content, as outlined in Directive 2004/48/EC of the European Parliament and of the Council (Enforcement Directive), emphasizing that notice-and-take-down mechanism should be the primary instrument in the removal of illegal content addressing hosting service providers. Blocking injunctions at the network layer, issued by a competent authority aiming at preventing access to illegal content, should only be considered as last resort, where action closer to the content owner has failed.

From reactive to proactive: a new Duty of Care for active hosts

Active hosting providers, as defined above should move from a reactive system whereby they are reliant on user notification before taking action to ensure the non-availability of illegal material to instead adopt proactive measures to ensure that illegal content that has been notified to them is not persistently re-uploaded. Proactive steps should include the following:

- Provide transparent and user-friendly mechanisms for users to report or flag illegal content or behaviour related to its dissemination
- Establish networks of or otherwise engage with "trusted flaggers" in a transparent manner;
- Remove content identified as illegal by automated means or human flagging;
- Prevent search results from returning illegal content;
- Prevent the monetisation of illegal content
- Expeditious removal of content aimed at immediate incitement to violence;
- Targeted monitoring to ensure that identical instances of the same material are not re-uploaded by any user or that similar instances are not uploaded by the same user;
- Establish mechanisms for reporting illegal activity to relevant authorities

The use of automated tools can be a practical solution to detect and address illegal online activities at scale. This will help protect users, keep them safe in the Digital Single Market and assist companies affected by problems related to the distribution of illegal products and content. However, deployment of automated tools for the detection of illegal material presents a risk of over deletion and over-removal of content, in the event that the automated system identified false positives. There is also a risk of under-deletion in the event that the automated system returns false negatives, and fails to detect illegal material. In both cases, the risk stems from a lack of human oversight, and contextual understanding. For this reason Vodafone recommends that automated content detection systems are used in a transparent and accountable way, be subject to monitoring and adaptation on a systematic and constant basis, and include appeal and redress mechanisms. Automated content deletion tools should also be deployed in combination with adequately resourced and supported human content moderation teams.

The experience of the pandemic has served to demonstrate that social media platforms have the tools at their disposal to take a more proactive approach to the dissemination of illegal content, primarily through increased use of automated detection tools. However, this has been balanced by the introduction of an improved and simplified appeals processes to ensure that legitimate, non-infringing content is swiftly put back if wrongly flagged and removed. Based on this

experience, we think it is reasonable to expect that a more proactive approach should be enshrined in law via the DSA.

Illegal vs. Harmful content

For the sake of legal certainty, proportionality and preservation of fundamental rights, a clear distinction should be made between rules applicable to illegal content from content which is harmful but legal. We believe that the DSA should not aim at establishing rigid definitions for harmful content as in practice, content can change from harmful to illegal very quickly, as we experienced with disinformation relating to COVID and 5G, leading to damage to masts and attacks on engineers (as set out below in more detail)

Imposing additional obligations on active hosting providers will have a positive effect on both illegal and harmful content. We think the DSA should include measures that reduce the incentives that exist for content sharing platforms to host harmful content that is not necessarily illegal, limited primarily to obligations around algorithmic transparency, accountability and user control.

Oversight and enforcement

Effective monitoring of platforms' compliance with the new framework demands thorough information on the actions taken by platforms to meet their obligations. Competent authorities would benefit from high quality, comparable information of actions undertaken by platforms, in order to effectively supervise their compliance and intervene as necessary. Timely, accurate data would also inform the assessment of the functioning of the DSA framework. Data requested from platforms should be comparable across players and across Member states.

The consequence for failing to apply these obligations should be to subject such online platforms to sanctions, without removing the underlying liability exemption. In case the breach is repeated, increasing sanctions (e.g. fines) should be foreseen (as per in the GDPR), resulting in the loss of the liability exemption if the infringement of the obligation of removal occurs to be systemic.