Alliance for Healthy Infosphere

Key Principles for the EU Digital Services Act

POSITION PAPER, March 2021

Digital space is plagued by a range of deficiencies from the proliferation of hate speech to dissemination of disinformation and harmful information to vulnerable audiences by a plethora of domestic as well as foreign actors. These phenomena have a detrimental impact on the quality of democracies as they continue to undermine trust in public institutions, contribute to a growing polarisation of societies and undermine fundamental values underpinning democratic societies.

Recognising these serious harms, Alliance for Healthy Infosphere composed of 11 think tanks, civil society initiatives, academic bodies and private companies across 6 EU member states appreciates the EU's efforts to address these problems through instruments such as the Digital Services Act (DSA) and the European Democracy Action Plan.

However, after conducting thorough analysis of the Digital Services Act, the Alliance believes a few guiding principles must be strengthened in the Act, if it is to be truly efficient, fair and democratic.

1) TRANSPARENCY & USER EMPOWERMENT

While the effort to establish robust reporting obligations on the very large online platforms is appreciated, it is important that the principle of **binding data transparency** is implemented robustly where possible. It is not only important for risk assessment and mitigation, but also for **user empowerment**. Only when the user has complete information about veracity of information displayed, microtargeting practices or ad spending, can s/he make truly informed decisions in the online sphere.

Informed consent

Strengthening the principle of transparency within DSA can be specifically addressed in Articles 12, 13 and 36 by requiring digital platforms to ask for users' **informed consent each time T&Cs are being updated**. T&Cs should further include specific details on criteria based on which the user has been microtargeted with advertising as well as clear and simple procedure for opt-in mechanism into such practices. **By default, the user should be required to opt-in for any principles of targeted advertising** and be automatically assumed as wanting to opt-out.

Timeliness

Development of voluntary **codes of conduct** further as alluded to in Article 36 will contribute to better transparency and user empowerment, however, given the seriousness of the situation of harmful content proliferating on digital platforms, **it should not take several years** for these processes to start and can run parallel to the development of the DSA.

Similarly, the requirement for digital platforms to implement timely changes after risk assessments and auditing (Articles 27 and 28) should be clearly formulated as **binding requirements**.

Communication

It is essential that digital platforms develop **efficient communication lines with users by way of investing into user services personnel**, instead of users having to rely on not properly operating AI systems. Any user with a complaint or report to raise need to be **guaranteed communication with digital platforms' representatives**, including the need for establishing **human review** of flagged content (Article 14).

Access to Data

Where possible, access to data needs to be guaranteed to vetted researchers including institutions not affiliated with universities. Access to **data in compliance with the GDPR needs to be shared with users as well**, particularly when it comes to **advertising** practices, where interoperable **ad libraries containing detailed information on all ads** need to be developed. Similarly, relevant databases (Article 15.4) should be made available to researchers.

2) WORDING & DEFINITIONS

To guarantee fair and democratic digital environment, the Act needs to develop **essential definitions** for phenomena it alludes to several times such as **inauthentic behaviour, harmful content and most importantly, disinformation.**

Disinformation & other harmful phenomena

As the Act works with these terms, avoiding the definition will lead to information vacuum in which all stakeholders will adopt their own definitions and subsequently create significant barriers for reporting obligations, assessment of systemic risks as well as their management. The Act should not steer clear of these terms, as it is essential that digital platforms, and large **digital platforms in particular, provide full disclosure on the extent to which these harmful phenomena proliferate**. Such definitions are essential for transparency and user empowerment purposes.

Exactness

In its current form, DSA formulations are rather vague with a risk of stakeholders impacted by the Act interpreting its wording differently, thus minimising the positive impact of the Act. For example, when referring to user account suspension, clarification is needed as to after how many instances of not complying with the T&Cs can users account be suspended. Similarly, **wordings such as 'significant risk'** (Article 26) **are vague** and will be interpreted differently by different entities, creating potential loopholes for avoiding compliance with the regulation.

When discussing requirements of digital platforms to disclose information on advertising, it is absolutely essential that vague terms such as disclosure of 'meaningful' ad parameters are replaced with 'all', providing it is GDPR-compliant.

Very Large Online Platforms

Defining very large online platforms based on European user base is helpful, but it does not address the issue of platforms gaining dominant position on the market of a specific member state, or several member states. We recommend defining very large online platforms also based on the proportion of

its user base as compared with the number of citizens in a given member state. Platforms which are clearly dominant in one or more member states should be subject to stronger obligations in the sphere of reporting, risk assessment and risk management.

3) ROLE OF CIVIL SOCIETY & RESEARCH INSTITUTIONS

The DSA in its current form suffers from Western-centric approach whereby it equates practices standardised in the Western European countries with default standard for the whole European Union. This is most obvious in **Articles 19 or 31, which are discriminatory towards research institutions** which are not affiliated with academic institutions. The draft **Act potentially excludes plethora of relevant experienced institutions from the civil society sector** which, for example in CEE, have been carrying out high quality research into disinformation and influence operations for years.

Inclusion of CSOs

The Act must clearly address and include vetted researchers from any institution which can provide meaningful track record and provide references for its activities, while these should not be defined based on narrow standards. Similar standards need to apply to trusted flagger status, with NGOs and CSOs having equal opportunity to apply.

4) INDEPENDENT OVERSIGHT BODY

One of the crucial issues is the current lack of independent oversight body which could truly guarantee that any rights and responsibilities as formulated in the Act are not misused by major stakeholders, be it on European and national level or by digital platforms. While the provisions specified in the Act are relevant, their independent enforcement is unlikely in the current formulation.

Digital Services Coordinators

As Digital Services Coordinators are to be nominated by member states and will yield significant powers which can have serious repercussions for freedom of speech, their Board and DSCs themselves should be subject to independent oversight. Such oversight cannot be fulfilled by the European Commission itself, as it needs to be politically independent, and hence the need for a new independent European body arises.

Trusted flaggers & suspension of user accounts

The Act suggests that digital platforms should have the power to remove trusted flagger status from institutions, as well as to suspend accounts of 'wrongly reporting' user accounts (Article 20). Given that platforms will face substantial scrutiny, it is in their interest to retain trusted flaggers which may potentially not be very critical or even to suspend accounts of those who correctly point out digital platforms' failures to remove illegal content. This is particularly likely in non-English speaking member states where the AI assessing problematic content is not working properly and where digital platforms fail to remove instances of hate speech.

Conflict of Interests

Rather than improving their systems, the DSA in its current formulation creates an incentive for digital platforms to retaliate against trusted flaggers or users. Their reporting obligations and decision-making powers on these issues are in **clear conflict of interest**. Digital platforms should not have the sole

power to remove a trusted-flagger status from an institution, nor to suspend user accounts based on false reporting without the user having the chance to raise the issue with the above-proposed independent oversight body.

5) REPORTING

Reporting obligations described in the DSA need to be strengthened if the principles of transparency and user empowerment are to be truly meaningful.

AI operation & efficiency

Digital platforms must be required to provide details not only on the proportion of AI-assessed, versus human-assessed content, but also on the success rate of AI assessments broken down by language. This would highlight areas for progress needed in each of the EU languages.

Disinformation

Reporting requirements described in articles on risk assessment, risk management and auditing should include harmful phenomena, with a particular emphasis on disinformation. While disinformation is not subject to content removal based on DSA, it should be subject to transparency, research and mitigation measures. Without such focus, DSA will miss a unique opportunity to obtain information on how influence operations are conducted across the EU.

Country-specific focus

DSA needs to clearly state **country-specific reporting obligations** by digital platforms, as even detailed information will not be insightful without being able to have a grasp on situation pertaining to each member state. Furthermore, **risk assessments should also be carried out with focus on impact in each member state.** EU member states are diverse, and their information environments will be affected by harmful phenomena in different ways.

Digital Advertising

Digital platforms need to develop truly **comprehensive repositories of all advertising**, with political advertising and issue-based advertising being subject to even stronger reporting obligations, given the nature of its potential impact on the political and social development in a country.

Ad libraries

The provisions of DSA on digital advertising are currently weak, as they postulate that digital platforms are only required to retain information on ads placed for one year (Article 30). This is insufficient from both user and research perspectives. Such **repositories should retain ads for at least a decade**, so that advertising campaigns and developments can be properly tracked.

Furthermore, **ad repositories need to contain detailed information on microtargeting, reach of the campaigns and precise amounts of spend per each ad placed**.

Alliance for Healthy Infosphere, March 30, 2021