Commentary of the Union of Entrepreneurs and Employers (ZPP) on the progress of work on the Digital Services Act

Digital Services Act (DSA) will soon amend the E-Commerce Directive that has been in place for more than 20 years. Work on the new regulation has been ongoing continuously since late 2020. The trilogue - a trilateral negotiation between key EU institutions - is expected to conclude early this month. However, we are now seeing the emergence of numerous proposals that were not included in the negotiators' original mandate.

The disproportionality of the crisis response mechanism

Among the most recent proposals is the Crisis Response Mechanism (CRM), which was created to enable institutions to counter Russian disinformation attacks efficiently. We welcome that the EU institutions take decisive steps to fight against Russian propaganda. Nevertheless, we have some doubts as to whether introducing the proposed provisions in DSA at this stage of the negotiations is the best way to tackle this problem.

At the request of the French Presidency, the Commission has proposed introducing provisions that could force large technology companies to quickly adapt their platforms and increase the number of staff moderating content during major crises such as natural disasters, terrorist attacks or war. The new DSA Article 25(a) would empower the Commission to require specific actions only based on a recommendation from a Council of European National Regulators. Paris has suggested that a two-thirds majority of regulators would be needed. Technology companies' efforts to tackle disinformation or problems related to a specific crisis would be legally limited to three months. At the same time, the Commission would have to keep its decisions transparent.

This proposal has been protested against by 24 citizens' organisations, who point out in their open letter that the European Commission should not be empowered to declare an EU-wide state of emergency unilaterally. Furthermore, these organisations note that the CRM is far from respecting international human rights standards of legality, legitimacy, necessity and proportionality, and they call for reformulation.

Moreover, the new Article 25a of DSA is intended to empower national digital coordinators to require smaller platforms to comply with risk mitigation obligations that usually fall on very large platforms only. Such a provision appears to place a disproportionate burden on smaller platforms, whose ability to comply with the requirements mentioned above will be limited in practice, especially in the short term.

Ultimately, attempts to combat Russian disinformation may be undermined by other provisions found in DSA. Article 15(2) requires platforms to provide information on the facts and circumstances as well as the means used whenever content-related activities are undertaken. This will provide disinformation actors with full knowledge of how platforms combat disinformation and reduce the visibility of harmful content. As a result, in an effort to increase transparency, DSA will make it easier for bad actors to fool security systems and, consequently, more complex to fight disinformation. In the current situation, the EU institutions should create instruments that allow platforms to fight against disinformation actions carried out by third countries on a massive scale, rather than introducing new solutions to a horizontal regulation such as DSA at such a late stage.

Return of the ban on targeted advertising

In a plenary vote in the European Parliament, MEPs rejected a complete ban on targeted advertising. As a result, they voted to restrict the targeting of minors and targeting using sensitive data. We welcomed the EP decision. We believe it strikes the right balance between user protection and business rights. A total ban would have hit SMEs, depriving them of a cost-efficient way to reach their customers and severely limiting their growth opportunities. Therefore, we watch with concern the amendments tabled by MEPs aimed at achieving a de facto ban on targeted advertising.

Before discussing the EP's latest proposals, it is first necessary to draw attention to the so-called 'known minor problem'. Platforms would have to verify minors' age to be able to restrict the use of targeted advertising. In the absence of general age verification on the Internet, platforms have to process user traffic data to determine age based on activity. Paradoxically, a ban on targeting could, in theory, lead to more tracking of children's online activities.

To address this issue, the EP proposed an amendment to Article 24(1)(b), which states that 'compliance with the obligation set out in the first subparagraph shall not entail the processing by online platforms of additional personal data on minors in order to verify the age of the recipient of the service'. Whilst we recognise the need to promote child safety through data minimisation, we believe that a provision worded in this way will be difficult to implement in practice and will reduce targeted advertising across all age groups. We propose that the provision be amended to prohibit excessive, rather than an additional, collection of personal data for age verification purposes.

Moreover, MEPs propose to extend the ban if the platform has doubts about whether the recipient is a minor (Article 24(1)(c)). This also means expanding the prohibition to the user when age verification is not possible. Given the current state of technology, such a provision could lead to a de facto ban on personalised advertising. This provision should be limited to cases where the platform has serious grounds, not just doubts, to believe that the recipient is a minor to avoid negotiators walking out their mandate. A provision worded in this way will simultaneously protect minors.

Extension of know-your-business-customer

As a final point, attention should be drawn to the proposal to extend the know-your-business-customer rule, which obliges Internet Service Providers (ISPs) to collect information that identifies business users in order to verify their identity. KYBC aims to improve online security by halting certain entities from using legitimate services to conduct illegal business anonymously. Assuming that the list of information required to be obtained from ISPs is proportionate and not an unreasonable administrative burden, the proposal should be viewed positively. However, during the January negotiation rounds, it was proposed to extend this principle to all types of ISPs, thus covering market places and social media, instant messaging, or streaming services.

In order to understand the implications of the KYBC extension, it is important to remember that DSA, like the E-Commerce Directive, is based on a prohibition of general internet monitoring. Such an injunction has been rejected from both the E-Commerce Directive and DSA, as it undermines fundamental values such as freedom of expression and could lead to censorship (i.e. excessive blocking or removal) of lawful content. Extending the KYBC to all intermediate service providers means extending it to all content that appears on the Internet. Therefore, it is hard to imagine in practice how the application of such a rule would take place without general monitoring of the Internet while still meeting DSA's stringent requirements for human factors provision.

The Union of Entrepreneurs and Employers actively participated in the work on the Act and, from the very beginning, called for solutions that would not overburden digital businesses. At the end of DSA negotiations, we maintain this call and urge policymakers not to place impossible demands on digitally active companies.

Union of Entrepreneurs and Employers
ul. Nowy Świat 33
00-029 Warsaw
T: +48 22 826 08 31
E: biuro@zpp.net.pl
www.zpp.net.pl
NIP: 522-295-88-64