Brussels, 19 November 2021

Dear Members of the IMCO Committee,

Ahead of the next shadows meeting on the Digital Services Act (DSA), EDRi and its 45 member organisations would like to share ideas and recommendations for a DSA that protects people and enables the EU pioneer successful platform regulation globally.

Please also have look at our more detailed "DSA Guide to 2,297 amendment proposals".

## Avoid excessive centralisation of power that will lead to democratic deficit

The current compromise amendment for Article 55 establishes a special set of interim measures to be used by the European Commission against Very Large Online Platforms (VLOPs) in case of non-compliance with the DSA. Interim measures include immense powers such as the power to remove content or to restrict access to an online interface as well as to order domain registries or registrars to delete a fully qualified domain name. Yet from a democratic standpoint of separation of powers, it is highly problematic to allow the European Commission as political executive body of the EU to take on a quasi-judicial role. In any democracy, only independent and impartial judicial bodies should should have the power to limit the free expression of people offline and online, based on the law. It should never risk being a politically charged executive decision. Such a centralisation of power would lead to serious democratic deficit. Therefore, it is of the utmost importance to make sure that power is distributed between institutions so they can operate as checks and balances and make sure there is no abuse of power.

## Protect freedom of expression and safeguard the limited liability model

The European Parliament must ensure that online intermediaries are not held liable for user-generated content simply because they receive notices about potentially illegal content from users. Those user notices are often unreliable and will in many if not most cases not safely establish actual illegality. Safe for manifestly illegal content, actual knowledge of illegality by intermediaries should only be assumed if they are presented with a court order. In addition, the DSA should acknowledge the need for flexibility, uphold freedom of expression, and abstain from introducing fixed time periods for the removal of content that has not yet safely reliably to actually be illegal under the relevant national jurisdiction. Online intermediaries should be given sufficient flexibility and time to respond to the most urgent notices first.

## Regulate unwanted online tracking

Surveillance-based online advertising threatens our democracy by allowing anyone who can afford it to engage in the micro-targeted manipulation of the public debate. The majority of the data economy behind surveillance ads is controlled by big data firms, including Google and Facebook. They soak up advertising revenue and dominate the ad market due to their direct access to virtually unlimited amounts of highly intimate data about billions of people.

The ad tech industry has devised countless ways to gain people's consent for pervasive corporate surveillance by tricking them with unusable cookie banners, unreadable privacy policies, and deceitful interface designs. These so-called 'dark patterns' make it impossible for users to make an informed choice and make use of the rights and protections they have under the law. The DSA must put an end to the cheating data industry that destroys trustworthy online advertising and instead empower a European advertising ecosystem that respects users, publishers and advertisers.

## Regulate and ensure interoperability for algorithmic recommender systems

Algorithmic recommender and curation systems decide who is able to see what kind of content online. At the moment, Big Tech's algorithms are optimised for only one thing: grab user attention for as long as possible to make people stick to their screen. The design of these algorithmic recommender and curation systems in dominant online platforms like Facebook and YouTube know that more engagement is best reached by showing people scandalising, divisive and even hateful content—and that is what they do based on the personal data they know about us.

The default option for such recommender systems should therefore always be set to "no use of personal data" and companies should not be allowed to 'nudge' users – with the use of dark patterns – to provide personal information for that purpose. At the same time, a high level of transparency vis a vis users is the minimum baseline to ensure that people can make informed choices and protect themselves against the threats described above. Users must therefore be able to modify the optimisation parameters of these systems. Finally, the DSA must create the market conditions for diversified and decentralised recommender systems to exist and for which Very Large Online Platforms (VLOP) should guarantee interoperability.

## Strengthen mandatory human rights impact assessments

The DSA should oblige Very Large Online Platforms (VLOP) to conduct mandatory ex ante human rights impact assessments (HRIA) in line with the UN Guiding Principles on Business and Human Rights, which should be coupled with strong transparency requirements about such measures. This would enable human rights groups to raise concerns or bring complaints against measures that unduly interfere with fundamental rights.

## The role of trusted flaggers

Trusted flaggers (TF) are entities with specific expertise and dedicated structures for detecting and identifying unlawful online behaviour. Online behaviour flagged by trusted flaggers is often treated with priority. Such flaggers can only be 'trusted' however, if they act independently from online platforms, commercial entities, and law enforcement agencies, and if have the collective interests of the public and the protection of fundamental rights as their mission.

## Protect users' privacy and anonymity

The Digital Services Act should affirm users' informational self-determination and right to privacy and confidentiality of communications. The DSA should therefore never force companies to analyse and indiscriminately monitor users' communication and abstain from including private messaging services in the scope of the DSA. People using many of these popular services (e.g. WhatsApp, Signal, or Threema) rely on end-to-end encryption and have enhanced security and privacy expectations. In addition to this, the DSA should respect a user's decision to not share their identity publicly by establishing a right to anonymity.

We remain at your disposal for any questions or comments you may have on these recommendations. We wish you a successful finalisation of the IMCO negotiations and that the Committee's DSA report further improves the Commission proposal where needed.

Best regards,

Diego Naranjo
Head of Policy, European Digital Rights (EDRi), on behalf of:

European Digital Rights (EDRi)
Bits of Freedom – Netherlands
Civil Liberties for Europe - EU
Electronic Frontier Foundation (EFF) - US/International
Panoptykon Foundation - Panoptykon
Xnet - Spain