Digital Services Act

The EDRi guide to 2,297 amendment proposals

Contents

Published by European Digital Rights (EDRi) in October 2021

Authored by: Jan Penfrat, EDRi Senior Policy Advisor

Edited by: Gail Rego, EDRi Senior Communications and Media Manager

This paper has received substantive input from EDRi members and observers, in particular through written submissions by:

Access Now
Amnesty International
Electronic Frontier Foundation
IT-Pol Denmark
Panoptykon Foundation

Executive summary

Various committees in the European Parliament have tabled amendments to the European Commission's proposal for a Digital Services Act (DSA). In the lead committee for Internal Market and Consumer Protection (IMCO) alone, Members of the European Parliament (MEPs) proposed almost 2,300 changes to the law.

This EDRi policy paper aims at providing a guide that supports Members of the European Parliament in understanding which amendments are beneficial for people and an open rights-respecting European digital sphere. At the same time, it also points out the amendments that would merely protect the profits of Big Tech or enable abuse of power in people's digital lives. This policy paper builds on previous policy positions established by the EDRi network and takes those forward to anchor them into the current debates and proposals.

As the starting point of any rights-respecting internet regulation, EDRi strongly recommends protecting the conditional liability regime established by the eCommerce Directive. Although online intermediaries, and especially social media platforms need to be regulated, pushing them towards unverifiable and hyper-fast removal of online content that someone has alleged to be illegal on the internet is not going to help the EU fight the harm that these platforms are causing. This also means that the so-called 'trusted flagger' — organisations with special expertise and mandate to find and notify potentially illegal online content — should only be awarded to entities that defend the public interest. That excludes commercial actors such as right holders. Finally, law enforcement agencies must strictly adhere to their legal due process when fighting crime, which should exclude them from the "trusted flagger" status.

The DSA should enable people to control the kind of online content they wish to read, watch and share. Currently there are no limits as to how platforms' algorithms disseminate, amplify or suppress online content for their billions of users worldwide. As a result, these algorithms are optimised for maximising user 'engagement', that is to keep people clicking, liking, and sharing no matter what. Facebook's own research has shown "that content that is hateful, that is divisive, that is polarizing, it's easier to inspire people to anger than it is to other emotions", explains Facebook whistleblower Frances Haugen, who has alerted the public about the harms these algorithms are inflicting. Algorithms optimised for user engagement will tend to promote hateful content and disinformation, even when platforms take specific measures to remove such content (as Facebook claims to do). "Facebook has realized that if they change the algorithm to be safer, people will spend less time on the site, they'll click on less ads, they'll make less money," Haugen says.

The DSA should also reduce the enormous amounts of personal data that allow social media platforms to target harmful content to users in the first place. Ending surveillance advertising is an absolute prerequisite for building a healthier, rights-respecting online environment designed for people instead of data brokers and other data-hungry corporations. That does not mean that online advertising is bad in and of itself, but it must be done without spying on everyone, everywhere, all the time. At the very least, the DSA must lead to a healthier internet without surveillance advertising and, for example, introduce a mandatory fair consent screen that is independently designed by the Commission to stop the dishonest ad tech industry from tricking people into giving consent. This would need to be combined with automated and binding Do-Not-Track signals built into every browser and operating system.

In order to ensure that platforms, regulators and the public detect potentially dangerous functions such as discriminatory or inciting algorithms before they can do harm, the DSA should oblige Very Large Online Platforms (VLOP) to regularly assess the human rights impact of their services. Assessing human rights impact rather than 'risks' provides both providers and regulators with a higher degree of certainty as to what it is the assessment should measure. The international human rights law framework also provides clearer guidelines on what negative impact looks like.

The DSA is a huge opportunity for the EU to become a global leader in modern online platform regulation. To achieve this, however, it must look **beyond mandating quick content deletion and fix what's really broken: the attention-grabbing, user-exploiting business model** of most of today's monopolistic, hyper-centralised, and ad-driven social media platforms. We can do better than this. But to build a healthier online ecosystem for Europe, the DSA must not tear down our fundamental rights.

Protect content moderation and limited liability

761	Introduces clear text without harmful deadlines
763	Adds clarification on how fast platforms need to act
785	Limits the risk of abuse of content moderation
789+ 790	Sets minimum standards for own-initiative content detection by platforms
793+ 797	Clarifies the importance of end-to-end encryption and how it relates to content moderation
794	Sets useful obligations for 'Good Samaritans'
1053-1056	Prevents wrongful or abusive notices from falsely triggering intermediary liability

71	Consolidates big tech power and leads to the removal of legal speech
105	Turns Big Tech platforms into arbiters of truth
106	Technically impossible to comply with in practice
110	Protects accounts that spread illegal content
758	Introduces entirely inappropriate removal deadlines of 30 min.
784+ 791	Creates vague conditions under which intermediaries could be randomly held liable
795	Creates legal uncertainty with unclear terms
1,057	Hands over judicial powers to the DSCs
1,058+ 1,063	Falsely assumes every notice sent to platforms is correct

The DSA proposal contains a modernised set of rules that define when online intermediaries such as Facebook and Twitter, but also small discussion forums and start-ups, can become legally liable for content uploaded by their users.

The European Commission proposed to maintain the general rule according to which intermediaries are not liable for user-generated content unless they have actual knowledge about illegal online activity. This knowledge, however, should not be assumed simply because an uninformed or begrudged internet user (or worse: masses of online trolls paid for by a foreign government) allege something to be illegal. In order to protect freedom of expression and prevent the system to be gamed by foreign actors that want to disrupt our elections, online platforms must have enough time and flexibility to truly assess the validity of each notification they receive. This is particularly true for smaller platforms, which we so dearly need as healthier alternatives to Big Tech.

Studies analysing the time that illegality assessments of online content actually require found that "the expectation that tens of thousands of complex hate speech complaints will be processed within hours or days — while trying to uphold due process and freedom of expression — may be unrealistic at best. At worst, this could entail systemic 'collateral damage' to the online ecosystem of information and opinion."

In addition, online intermediaries should not be required to scan every single social media post, image or video for potential infringements in any of the 27 jurisdictions in the EU. Any obligation to generally monitor all user content should remain prohibited as it has been under the eCommerce Directive.

For this to work, however, the DSA must ensure that notices about potentially illegal content that are sent by random strangers on the internet do not automatically trigger legal liability. EDRi therefore recommends **supporting IMCO AM 1053, 1054, 1055, and 1056** which would prevent exactly that.

For the same reasons, we recommend **rejecting IMCO AM 784, 791, 794, 1058 and 1063** which would create immense legal uncertainty for users and platforms alike as to when exactly liability kicks in. Those amendments use vague and largely undefined requirements for liability protection such as "diligent operator", "adequately precise" notice. Or they falsely assume that every notice received by an intermediary is correctly flagging illegal content. In practice, many of the notices are and will continue to be legally invalid: Many people would flag content they dislike or disagree with or believe should be illegal.

In addition, intermediaries should be given sufficient flexibility and time to respond to the most urgent notices about the most harmful illegal content first. This is incredibly important especially for smaller online platforms and start-ups in order to prevent the removal of legitimate speech out of fear of legal liability. Imposing stringent removal deadlines forces intermediaries to treat incoming notices chronologically, no matter how small the harm of some of the content may be, instead of focussing on the most horrific criminal content first, such as child sexual abuse material and terrorist content. EDRi therefore recommends **supporting IMCO AM 761 and 763** and **rejecting IMCO AM 105, 758**, and similar proposals.

At the same time, especially very large online platforms such as Facebook, Youtube, and Twitter should not be discouraged from searching their systems for potentially illegal online content, especially if it is manifestly illegal, on their own initiative. Such voluntary activities should not be punished with the threat of legal liability but should be performed with the highest ethical standards and in compliance with applicable EU and national law. That is why we recommend **supporting AM 785, 789, 790, 793, 794, and 797**.

Regulate unwanted online tracking

735, 737, 738 Better defines 'dark patterns' and enables their effective regulation

746 Prohibits tracking based advertising and creates conditions for contextual advertising

972+ 1,013 Introduces conditions for fair consent choice and creates an obligation to respect communication of consent through automated means

1,014 Prohibits the use of dark patterns

1,019 Prohibits tracking based advertising

1,125 Prohibits the use of dark patterns and creates an obligation to respect communication of consent through automated means

1,485 Prohibits the use of dark patterns that trick people into giving consent

1,495 Waters down transparency requirements

1,509 Will lead to increased exposure of sensitive data from children for the purpose of age verification that can easily be circumvented

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 vastly unlimited amounts of highly intimate data about billions of people.

While the ad tech industry argues it provides "more relevant advertising" to people, representative studies and real-word data consistently show that people don't want it. **When given a real choice, 83% of respondents in a YouGov poll in Germany and France said they don't want their personal data used to target them with political ads and 57% of respondents said they don't want to be targeted that way with any ads at all**, either commercial or political. In the same vein, when Apple introduced its App Tracking Transparency tool, which provides an easily understandable consent screen for users to say 'Yes' or 'No' to apps that want to track them, 96% of users chose to say No.

Surveillance-based online advertising is so dangerous that even intelligence agencies like the CIA and the NSA reportedly use ad blockers to protect their computers from malware. "The U.S. Intelligence Community has implemented network-based ad-blocking technologies [...] to block unwanted and malicious advertising content," the Intelligence Community's Chief Information

Officer said to members of the U.S. Congress.

The harms that the ad tech industry inflicts and the risks that it creates cannot be remedied by the GDPR's consent framework alone. 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.

That is why 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. To achieve this, we recommend **supporting IMCO AM 746, 972, 1013 and 1019** that aim at replacing Big Tech-dominated surveillance ads with an ecosystem that does not require the pervasive tracking of users.

At the same time, EDRi recommends **opposing IMCO AM 1495** which attempts to water down the already weak advertising transparency requirements devised by the Commission proposal. We also **oppose the half-baked approach of IMCO AM 1509** which says it protects children from online tracking while in reality forcing them to reveal their age and potentially other personal information to the very same platforms they ought to be protected from.

As a bare minimum, and if all of the above strong regulations fails, the DSA should introduce the most stringent transparency rules for the deceitful ad tech industry, such as proposed by IMCO AM 1486, 1487, 1488, 1489, 1490, 1492, 1497, 1498, 1504 and 1505.

Strengthen mandatory human rights impact assessments

1,549 Specifically includes technology design, value chain and business-model choices as factors to be taken into account during the risk assessment

1,552 Clarifies what risk assessments should be about

1,553 Requires human rights impact assessments

1,560-1,561 Includes systemic problems like advertising ' business models that fund illegal online content

1,562-1,566 and 1,570-1,572 Completes the list of human rights to be included in any assessment

1,574 Includes negative impact caused by intentional functionality of a platform service

1,581 Includes negative impact caused by technological design and business choices

1,591 Requires the assessment of actual impact

1,593 Includes experts and people concerned in the risk assessment process

1,596 Clarifies that risk assessments should not lead to a general monitoring obligation

1,600 Requires human rights impact assessments

1,608 Acknowledges the role of the tracking advertising industry in exacerbating negative impact

1,754 Enables vetted non-profit and media organisations to acquire access to platform data for the purpose of researching systemic risks

1,555-1,556 Unduly broadens the scope of the mandatory assessments

1,603 Gives the Commission as EU executive arm too much power

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. With these impact assessments VLOP must identify, cease, prevent, mitigate, monitor and account for the impacts on any human rights that their platforms are responsible for. The advantage of an impact assessment instead of a mere 'risk assessment' is the increased clarity and precision of what the assessment is supposed to measure. As a result, platforms can more effectively be held accountable for failing to protect their users and society as a whole from negative impacts.

A risk assessment-based approach can, however, be acceptable if and as long as it is firmly rooted in the established international human rights framework, including the EU Charter of Fundamental Rights. This can ensure that clear definitions are set as to what exactly it is that the platforms are assessing and that the results cannot be abused to coerce private platform providers into actions not foreseen by law.

A summary or redacted version of the HRIA should always be made publicly available and all information for the purposes of independent audits should be communicated to all relevant stakeholders, including regulators and enforcement bodies, in a continuous manner.

In addition, the assessment of all operations of VLOP, including their use of automated decision making or 'AI' systems, should equally be based on an analysis of their human rights impact instead of being limited to a mere risk mitigation exercise. The burden of proof should be on VLOP to demonstrate that their services as a whole, as well as their individual products and technical tools do not violate human rights. The HRIA should determine the impact that the aforementioned products and services have on users' and society's ability to exercise human rights, and thereby determine which safeguards must be assigned to the specific impacts established in the process. The mitigation of risks can come as a complementary step once the full range of impact on human rights has been determined by the HRIA.

Risks identified and the measures taken to avoid or mitigate those risks must be fully documented, and updated throughout the lifecycle of systems and operations deployed by VLOP. We caution against any regulatory mode that is based on a rigid binary distinction between low and high systemic risks. As discussed within the context of the GDPR, a significant loophole was left open by allowing the data controller to determine alone whether a system poses a high risk and whether a data protection impact assessment is needed. This enables a scenario in which risks could in fact be downplayed, leading to a reduction in user safeguards.

Additionally, during the GDPR negotiations, the EU data protection authorities further recalled that "rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved". We must therefore avoid a situation in which responsible VLOP can shirk their responsibilities by ignoring rights.

Finally, the outcome of mandatory HRIA can significantly vary depending on who conducts them. The DSA should therefore introduce a contestability mechanism allowing independent stakeholders such as human rights organisations and equality bodies to challenge the outcome of an HRIA if there is a sufficient evidence that the operations of a VLOP have negative effects on the exercise of fundamental rights.

Regulate algorithmic recommender systems

130	Mandates profiling to be switched off by default
1,481	Increases transparency of recommender systems
1,518	Increases transparency of recommender systems, switches off profiling by default and empowers users to modify the parameters of such systems
1,690	Switches off profiling by default
1,691+ 1,692	Facilitates access to information about recommender systems
1,694+ 1,699	Empowers users to modify the parameters of recommender systems
1,696	Increases transparency of recommender systems
1,700, 1,703, 1,707, 1,806	Empowers users to choose 3rd party recommender systems and boosts competition
1,705	Creates useful conditions where access to 3rd party recommender systems may be limited
1,706	Prohibits the commercial use of 3rd party data
1,708	Regulates differential treatment in pricing

1,517	Gives special treatment to poorly defined categories of reporting, easy to abuse
1,702	Attempts to use the cover of trade secrets and IP ' to prevent meaningful transparency

Algorithms that deliver ads have been found to discriminate against marginalised groups simply by the way in which they were designed, even when the advertiser did not intend it; recommender systems notoriously promote divisive, sensationalist content, leading to the erosion of public debate; and a recent study from Mozilla documented people's experiences of the "rabbit hole" effect: recommendations of increasingly extreme content.

Platforms such as Google and Facebook often frame these issues as unintended consequences of otherwise fair and useful personalisation systems and promise to "do better" in the future. But these cosmetic interventions do not have the potential to address the harmful logic of these systems which results from platforms' commercial interests. As these corporations make profit mainly from targeted advertising, their overarching business goal is relatively simple: to display as many ads as people can handle without discouraging them from using the platform. They must grab and maintain users' attention in order to maximise the time they spend on the platform, because more time equals more data left behind and more ad impressions. These goals are deeply

embedded in the design of the algorithmic systems in use and in themselves lead to individual and societal harms.

The Digital Services Act (DSA) must therefore enhance the transparency and accountability of algorithms used by dominant platforms and increase users' control over the information they share and access online. As useful as the application of such data in recommendation systems may be in some cases, the potential for abuse through hidden nudging, targeted and mass manipulation is high. To reduce the risk, people need to be able to know when and how algorithms are being deployed to shape their online environment, what kind of personal data is being used to decide what content they are being exposed to – and what information is kept hidden. 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. This is why we recommend **supporting IMCO AM 1481, 1518, 1694 and 1699** and **opposing IMCO AM 1702**.

At the same time, the DSA should not put the burden of default protections on individual users. We should be able to do nothing and still be protected, just as we can all trust that the medication we buy in a pharmacy is safe, without having to verify the chemical formula ourselves. That is why the default option of recommender systems should 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. We therefore recommend **supporting IMCO AM 130, 1518 and 1690.**

Real user empowerment requires meaningful choice and the development of competing products to be available to users. That's why the EU should require the biggest platforms, that have the most power over our digital public sphere, to allow users to choose the recommender systems they prefer, including those provided by trusted third parties. This new freedom of choice enables a whole new market in the EU for recommender systems that could be designed to prioritise valuable information and facilitate constructive political debate instead of amplifying sensationalist content designed to maximise screen time and ad clicks. This solution, technically based on interoperability, paves the way for the development of European alternatives to Big Tech. To achieve this, we recommend **supporting IMCO AM 1700, 1703, 1707 and 1806**.

The DSA can create a digital public sphere as a safe, non-intrusive space, where people's fundamental rights are protected and where those wishing to shape their own experience have the tools to do so. Without better regulation of recommender systems, however, we will experience a further exacerbation of existing problems: mass violations of privacy, discrimination, the further erosion of public debate, and the use of platforms' surveillance advertising machinery for political manipulation.

Fair and transparent terms of service

924 Obliges online platforms to provide a readable summary of their ToS

925 Information about redress options for users is mandatory in ToS

926 Content restrictions must be in compliance with human rights law

929, 931, 935, 936, 938, 940 Useful clarifications on what kind of information needs to be included in ToS

957 Promotes appropriate training and working conditions for content moderators

945+ 946 Removes fundamental rights considerations from instances of allegedly illegal content

947+ 948 Introduces a general exemption of all 'press publications' from ToS compliance

949 Promotes non-transparent algorithms for unproven risks of 'gaming the system'

950 Falsely assumes that IP rights and trade secrets are necessary for the security of computers

953 Gives almost unlimited power to EU member states to dictate ToS

Human rights must be respected online as much as offline. The activities, functioning and business models of online platforms can have significant implications on individuals' capacity to exercise their fundamental freedoms, such as the right to privacy, freedom of expression, and freedom of assembly and association.

Most content moderation decisions taken by online platforms that restrict freedom of expression today are taken on the basis of commercial Terms of Service (ToS) rather than the law. Since private companies are not legally obliged to respect the EU Charter of Fundamental Rights, they often do not take it into consideration when applying these ToS and as a result, decisions are often arbitrary, non-transparent and exclude means of redress for concerned users. So-called "community guidelines" therefore often ban or restrict online content that is lawful in unpredictable ways. In addition, on most commercial online platforms users have no power to influence the rules that are applied to police their online behaviour.

In order to ensure that online platforms' terms of service are fair and transparent, the Digital Services Act (DSA) should oblige commercial online platforms to:

- Be transparent about any content moderation rules that apply to their users;
- Apply those rules in a fair and non-discriminatory manner;
- Notify users when their content is removed or otherwise restricted on the platform;
- Be proportionate in their content moderation practice by minimising the impact of their

measures to the content only, or the user's account in case of recurrent breaches; and

- Establish clear, accessible, intelligible and unambiguous terms of service in all languages in which the service is offered.

The EU should also make sure that none of its legislation, including the DSA, non-binding initiatives like codes of conduct or other activities incentivise companies to over-remove content, but instead encourage them to respect the fundamental rights and freedoms of people in the EU.

The role of trusted flaggers

1,260	Prevents the execution of unreliable notices by TF
1,262+ 1,306	Prevents abusive behaviour by TF
1,271	Clarifies that notifications do not automatically establish illegality
1,273, 1,274, 1,275, 1,291	Law enforcement and commercial interests should not be TF
1,282, 1,285, 1,287	Increases transparency and accountability
1,284	Ensures independence of TF
1,295	Increases accountability by making renewal of TF status non-automatic

1,257+ 1,258	Prevents any meaningful regulation of TF
1,261	Uses vague terminology and is open to abuse
1,266	Increases platform power to nominate TF and reduces their accountability
1,276+ 1,278	Rightholders and other commercial interests should not be TF, to avoid conflicts of interest
1,288	Would enable law enforcement authorities to become TF, who should follow due process instead
1,289	Undermines DSC's prerogative to award TF status
1,316	Creates ample risk of abuse for political goals

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 be 'trusted' provided that they act independently from online platforms, commercial entities, and law enforcement agencies and have the collective interests of the public and the protection of fundamental rights as their mission. This is why we **recommend supporting IMCO AM 1273, 1275, and 1291**.

Unfortunately, the criteria set out by the DSA proposal for becoming a trusted flagger fall short of these safeguards. They would allow governmental and law enforcement agencies to circumvent due process rights guaranteed under the rule of law in criminal investigations by abusing fast-track removal powers as 'trusted' flaggers. Instead of going after criminals, they can simply wipe allegedly illegal content off a platform without redress or consequence. This is why we recommend **opposing IMCO AM 1276, 1278, and 1288**.

One type of proposal would make the situation for users even worse: it suggests that public authorities should be automatically treated as trustworthy sources and be ranked higher by platforms — no matter the content they produce (like political propaganda, disinformation, or simply accidentally wrongful posts). This faulty approach is mirrored by special, must-carry protections for so-called 'public interest accounts', such as those held by politicians, which would lead to a

two-class society online where powerful account holders receive special advantages not available to ordinary users. These kinds of special-treatment approaches, such as **IMCO AM 1316 should be rejected.** The latest Facebook scandal revealed by the Wall Street Journal has demonstrated what this kind of provision would lead to.

An ambitious scope is a limited scope

None

680+ 709 Bloats up the scope to include messaging apps such as Signal and WhatsApp

1,020, 1,021, 1,022, 1,025, 1,073, 1,074, 1,080
Suggests that private messages should be treated just as if they were public statements, breaching the most basic privacy protections

1,526, 1,527, 1,528, 1,531, 1,548, 1,599
Forces providers to scan all private messages as if they were public statements, effectively outlawing end-to-end encryption that people and businesses rely on today

Private messaging services and the comment sections of websites that are merely ancillary functions to a services must not fall under the scope of the DSA. In particular, if messaging apps like Signal or WhatsApp were covered by the DSA — as proposed by MEP Geoffrey Didier's DSA opinion in the JURI committee — there would be no legal distinction any more between something you post publicly, say, on Twitter, and something you say privately in a conversation with your partner or friends. In addition, regulators should not have the power to impose obligations on service providers that would entail an unjustifiable interference with users' privacy rights, such as a weakening of end-to-end encryption or mandatory filters.

Otherwise, every single word you say over WhatsApp or Signal would need to be scanned and analysed for potential illegality under any of the 27 national jurisdictions in the EU. **It would be like if the postman was legally required to open every single letter and package and read/check it before delivery to the intended recipient.** Furthermore, messaging apps are already covered by the ePrivacy Regulation, the adoption of which EU member states have been blocking for four years instead of enacting the necessary protections.

Similarly, the DSA's scope of application should exclude below the line comments on news websites or blogs. The DSA was meant to protect users against the most systemic harms that the online platform economy creates today, especially the largest social media platforms with billions of users worldwide. It should not make it impossible for news publishers to run a modern website or put every single personal blog under the risk of legal liability.