DSA – Analysis

Article by Article

On 14 December 2021, the Internal Market and Consumer Protection (IMCO) Committee of the European Parliament adopted its report on the Digital Services Act. It is a crucial piece of legislation for the digital world which could set a gold standard for content regulation globally. The following provides an overview of the provisions successfully pushed through by the Greens/EFA, as a result of our Amendments (AM). It also outlines elements which we were opposed to but which were nevertheless adopted due to centre-right majority during the negotiations.

Greens/EFA's successes | Greens/EFA's mixed success | Greens/EFA oppose

General Provisions (Articles 1-2)

The issue: These articles include the scope of the Regulation and the definitions. The IMCO report broadly maintains the scope broadly as proposed by the Commission.

What we wanted: We proposed a distinction between allegedly illegal content (which is not obviously recognisable as being illegal) and manifestly illegal content (such as child abuse material), with a view to establishing a nuanced approach to handling different types of content.

What we got:

- 👍 The crucial definition of "illegal content" has been improved.
- 👍 We successful prevented several negative amendments, such as an over-broad exclusion of "cloud computing" from being added to the text.

- 👎 We were not successful in our efforts to introduce a definition of "manifestly illegal content" to improve the clarity of the Regulation.

Liability Regime - Articles 3-5

The issue: Rules governing intermediaries' liability form the core of the DSA are rules on the liability of intermediaries. The DSA is essentially an update of the 20-year old E-Commerce Directive and stipulates rules defining when online intermediaries, such as YouTube, Facebook

and Twitter, but also discussion forums and other small services, can become liable for content uploaded by their users.

Articles 3-5 as proposed by the Commission define when services can benefit from liability exemptions, for instance if they become aware of or obtain knowledge of the presence of illegal content on their networks and expeditiously remove such content. The EP Rapporteur suggested the introduction of a different set of liability rules for online marketplaces (new Article 5a), which were however very vague and could have opened a veritable Pandora's box for further changes to the regime.

What we got:

- 👍 The ECD rules on liability exemptions have been maintained.

Voluntary Measures (Good Samaritan) - Article 6

The issue: There is increasing criticism of online companies' power over what people can read, watch and communicate online, with the help of a business model that is based on the massive collection of personal data. A few tech giants' services have become inevitable for people's daily lives, but they are also the main spreaders of hate, disinformation and other types of harmful and illegal content. At the same time, governments have too often expected that those private companies would "do more" to fix the internet. Unfortunately, tech giants are not only make mistake after mistake after mistake – they are also the prime contributors to the problem because extremist and divisive content generates higher profits for them.

Article 6 of the DSA as proposed by the Commission states that intermediaries should not be held liable for "own-initiative voluntary investigations". It thereby confirms platforms' current practices of voluntary privatised and unaccountable content moderation practices, with no regard for the potential dangers of counter-productive effects, accountability, or review mechanisms.

What we got:

- 👎 The Renew Europe group together with the EPP maintained the Article to allow voluntary measures. Greens/EFA requested deletion of the Article.

- 👍 However, we successfully pushed for the inclusion of safeguards. These safeguards require the voluntary measures taken by platforms to entail ***"human oversight, documentation, or any additional measure to ensure and demonstrate that those investigations and measures are accurate, non-discriminatory, proportionate, transparent and do not lead to over-removal of content***".
- 👍 Online services and platforms must ensure that their technology limits the removal of legitimate content to the greatest extent possible when using automated tools.

Prohibition of general monitoring – Article 7

The issue: Online intermediaries should not be required to scan and monitor every single social media post, image or video for potential infringements across the Member States in the EU.

Article 7 as proposed by the Commission maintains that any obligation to generally monitor all user content is prohibited.

What we got:

- Services will not be obliged to use automated tools for content moderation or to monitor the behaviour of natural persons.
- The DSA ensures that providers can continue to provide end-to-end encrypted services
- EU countries cannot oblige providers to introduce a "real name policy" or to prohibit the anonymous use of services.
- EU countries cannot oblige providers to retain data in a generalised and indiscriminate manner. This is an important victory as it confirms what the CJEU has repeatedly ruled in the past 8 years, namely that indiscriminate data retention is illegal and violates the fundamental rights in the EU Charter.

Order for removal and request for user data - Articles 8 and 9

The issue: Articles 8 and 9 as proposed by the Commission impose an obligation on providers of intermediary services in respect of orders from national judicial or administrative authorities to act against illegal content (Article 8) and to provide information on their users (Article 9). Regarding the territorial effect of the order, the Commission proposal states that the order must fulfil "general principles of international law, [and] does not exceed what is strictly necessary to achieve its objective".

What we got:

- To safeguard victims' rights, people can now seek an injunction from authorities in their home country.
- The criteria and elements of authorities' orders which must be included have been clarified and incorporated. We were also successful in ensuring that individuals concerned are informed of the order and that information is provided regarding how and by when an appeal can be lodged.
- Providers can also refuse to implement an order if it is clearly erroneous.

- Restriction to the territory of a Member States has been broadened insofar as any administrative authority in another country can request the removal of content in any other country if "***the rights at stake require a wider territorial scope"*** (8). This means

that content which is legal in one country could be requested to be taken down by another European country.

- We did not succeed in ensuring that judicial authorities only can ask for a removal of content, or for access user data (our amendment proposed the distinction "national judicial ***authority, or against an offer of illegal goods or services issued by the relevant national*** administrative authority")
- Any administrative authority in another Member State can request access to your personal details such as your name, contact details and, where available, your address (9) from online services that you are using.

Effective remedies for individuals – Article 9a (new)

The issue: This article was initially not in the Commission proposal, but it was added to provide additional safeguards for people when governments issue orders to have content removed or to access their personal data.

What we got:

- This Article is based entirely on a Greens/EFA amendment (AM 889).
- People may exercise their right to an effective remedy before a court/judicial authority.
- People may challenge the legality of the measure, including its necessity and proportionality.
- The Digital Services Coordinators must develop tools and guidance for people to make information and access to complaint and redress mechanisms as easy as possible.

Points of contact and legal representatives (Articles 10-11)

The issue: The European Parliament largely maintained these articles as proposed by the Commission. A new Article concerning points of contact for users was added the well-known problems users face when communicating with online services.

- An additional Article was added to allow users to directly and efficiently get in touch with online services and platforms. Furthermore, they may request that the interaction involves a human interlocutor and is not solely based on automated tools (such as chat bots) (Greens/EFA AM 900).

Terms and Conditions (Article 12)

The issue: Big tech companies do not enforce their terms and conditions for everyone alike. Rather, proof provided by leaked Facebook documents shows that certain platforms give special treatment to VIP and celebrity users (a very prominent example being the very late expulsion of Donald Trump from various social media networks). Moreover, a number of recent reports have unveiled the bad working conditions, and lack of psychological support for platform staff tasked with reviewing material uploaded by users.

What we got:

- 👍 Terms and conditions need to be enforced for every user in the same way – notably, in a coherent, non-discriminatory and non-arbitrary manner.

- 👎 There is sadly no obligation requiring training, psychological support and legal assistance for content moderation staff.

Transparency reports (Article 13)

The issue: Some online platforms already issue annual content moderation reports. However, these reports are not harmonized, making it difficult for researchers to analyse and compare practices.

What we got:

- 👍 Stronger transparency reporting obligations for content moderation, including an obligation for reports to be standardised and machine-readable to allow for more efficient data analysis.
- 👍 We also prevented language which would have rendered transparency reports meaningless (RE and EPP tried to include a provision to allow for data to be withheld on the basis of "trade secrets", and to exclude violations of terms and conditions from transparency obligations).

Online interface design (dark patterns) (Article 13a)

The issue: The use of "dark patterns" is unfortunately a widespread practice across the internet, on websites and apps. These practices have emerged because services generate the majority of their turnover with the collection, use and analysis of users' personal data. Default settings, interface design techniques and features are therefore are often used to manipulate users and make them do things that they did not intend to do, such as buying additional things that were sneaked into their shopping basket, not cancelling a service or giving away their personal data. Online services and apps do this mostly do this by using privacy-intrusive default settings, misleading wording or privacy privacy-friendly choices deep in a service's interface.

What we got:

- 👍 The addition of this new standalone article (based on Greens IMCO AM 1014) on online interface design to prevent so-called "dark patterns" that manipulate and nudge users significant Green success is the inclusion of. In particular, this means that online services are not allowed to:
    - give more visual prominence to any of the consent options.
    - repeatedly ask a user for consent.
    - to urge a user to change a setting or configuration.
    - to make cancelling a service difficult.
    - to ask for consent even though the user has objected via automated means (such as a "Do Not Track" signal in the browser).
- 👍 We successfully insisted that the Commission should be empowered to update the list of banned practices, to ensure that this Article is future proof.

- 👎 One sentence that was added last minute by the EPP to the corresponding recital (so with no direct legal impact) might weaken the interpretation of this Article on dark patterns by courts in the future. It adds that this Article ***"should not be understood as preventing providers to interact directly with users and to offer new or additional services to them. In particular it should be possible to approach a user again in a reasonable time, even if the user had denied consent"***

Notice and Action (Article 14)

The issue: There is no harmonised system which allows users to easily report illegal content, when they find such content on providers' networks. Consequently, the mechanisms are very fragmented across the EU – and often fail to include any information to the user or the uploader, once the content has been reported.

What we got:

- 👍 The rules on notice and action have been made significantly more stringent than the Commission proposal, by clarifying the elements that a notice must be included for a notice to be valid.
- 👍 A notice no longer automatically implies "actual knowledge" on the part of the provider. This is crucial for avoiding over-removal of legitimate content (Article 14.3).
- 👍 Content shall be left online in cases of doubt and while an assessment is pending (Greens IMCO AM 1086).

- Services are dutybound to deal with notices in a "***timely, diligent, non-discriminatory and non-arbitrary manner***".

- Unfortunately, anonymous reporting is prohibited, which can have a discourage victims of hate speech and other users more generally from reporting more serious crimes. (However, the recital says that anonymous reporting "should always be possible".)
- Our proposal to permit individuals to defend their content before it is removed, through a "counter-notice" procedure, was not included.

Information to the uploader (Article 15)

The issue: Platforms very often do not inform users or uploaders, when their content has been taken down, blocked or otherwise restricted in terms of visibility.

- To ensure that the DSA remains futureproof and encapsulates all possible actions by providers when moderating content, justifications also need to be provided when measures to demote content (such as Facebook's or Instagram's "shadow banning" practices) or when "other measures" against content are implemented.
- Services must also provide an explanation to the user by the service also needs to be issued when an action is taken based on voluntary measures or in response to an order from a governmental authority.
- A machine-readable database listing the actions taken by services and the explanations to the users will be established.

Notification of suspicions of criminal offences (Article 15a, previously Art 21)

The issue: In past years, we have criticised the approach to illegal content online for tending to rely on the removal of content, while the underlying criminal activity was not prosecuted. This has led to an environment where perpetrators feel comfortable to repeatedly upload such content – while the victims are left without help or hope of relief.

- Providers are now obliged to notify law enforcement or a judicial authority when they suspect that "***a serious criminal offence involving an imminent threat to the life or safety of persons has taken place, is taking place or planned to take place***"
- An additional data protection safeguard has been added for data processed in relation to the obligatory reporting of suspicions of criminal offences, stating that the data cannot be used by law enforcement for any other purposes other than the prosecution of the offence in question.

Exclusion for micro and small enterprises and waiver (Article 16)

The issue: The Commission proposed an exclusion for micro or small enterprises in Article 16, which would apply to every Article in this Section 3 (i.e an exclusion from the obligation to introduce a complaint handling system, to engage in out of court dispute settlement, to cooperate with trusted flaggers, to have measures against misuse, to keep records of their traders on their platform and for additional transparency reporting).

What we wanted: We tabled an amendment to only exclude micro companies and non-profit services below 100k users. However, we suggested excluding them from the entire Chapter III, to avoid disproportionate burdens such as the establishment of a Notice and Action mechanism or annual reporting obligations for very small non-commercial forums that are, for example, run by just one person.

What we got:

- Renew Europe, supported by EPP, successfully introduced a hugely bureaucratic "waiver" system to permit medium-sized or not-for-profit organisations to first apply to national regulators and, subsequently, the Commission to be excluded from the obligations of this Section 3 of the Regulation. This Renew Amendment was agreed, despite Green opposition. This will lead to broadly similar medium-sized businesses having different obligations, to a lack of predictability for consumers, and to decisions on the regulatory regime being based, ultimately, on who has the best lobbyists. It effectively spells the end of the digital single market for the relevant provisions of the DSA. Individuals will be pushed towards big platforms for which rules are in place, while companies that are unable to handle the administrative burden entailed by the waiver process, will suffer a competitive disadvantage compared to those who can.
- There is no exemption for small non-profit providers, nor for non-commercial archives and scientific repositories, despite our repeated campaigning in this regard.

User complaints to providers (Article 17)

The issue: When online services take down, block or demote content because it is illegal or in violation of their terms and conditions, there is usually no obvious or easy way to allow uploaders to complain and defend their content. The DSA introduces an obligation for platforms to set up a complaint handling mechanism, and thereby creating a balance between the different actors in the online environment.

What we got:

- Users can can now not only lodge complaints regarding content removals but also if their content has been "***demoted***" or when "***other measures restrict visibility,***

availability or accessibility" of their content (in order to include "shadow bans", and to ensure that the DSA is future proof)

- Specific deadlines for stages of the complaints system (complaints must be handled within 10 days).
- The right to contact a human interlocutor to complain.
- The right to legal remedy.

Out of court dispute settlement (Article 18)

The issue: In cases where users feel that a platform has not handled a complaint correctly, users now have the right to contact an external, independent out-of-court dispute resolution body. Online platforms are obliged to engage with these bodies in order to resolve any dispute with users of their services.

What we got:

- We improved the rules for the accessibility and financial independence of dispute-settlement bodies.
- We successfully included rules that the staff of such bodies are not allowed to have worked for online platforms within the two years prior to taking up their position, and commit to not to work at an online platform for a period of three years after their position at the body has ended.
- Our proposals for improved oversight of and transparency reporting by dispute resolution bodies was added.

Trusted Flaggers (Article 19)

The issue: "Trusted flaggers" are organisations with a particular expertise in a specific field of illegal content or activities, such as hate speech or child abuse, and who can therefore report illegal content directly to platforms via dedicated channels. Their reports must be treated with priority.

What we got:

- Key improvements include the addition of transparency reporting obligations for trusted flaggers, better oversight, and stricter rules on independence.
- A major Green success was the introduction of what we refer to as "de-flagging" – meaning that organisations can also report mistakenly removed or demoted content, and that such reports are given priority, an achievement of particular value to media organisations and NGOs.

- We regret however, that S&D and EPP opposed ensuring independence of trusted flaggers from law enforcement authorities. We defended the position that law enforcement must not be given such direct privileged channels as the DSA should not lead to circumventing current legal frameworks for issuing orders.

Accessibility requirements (Article 19a)

- A new article on accessibility requirements for online platforms was introduced and broadly welcomed by the European Disabilities Forum.

Measures against misuse (Article 20)

The issue: Whenever a user frequently uploads illegal content or when platforms receive more than two orders to act, platforms are allowed to suspend those users' accounts, following a prior warning.

What we got:

- Since the "de-platforming" of users is a drastic measure and should be the last resort, platforms are not obliged but entitled to decide on such account suspensions.

- Our proposal for a clarification that users should be given a reasonable amount of time to defend themselves before action is taken, was not taken on board.

Traceability of Traders (Article 22)

The issue: Consumer associations repeatedly uncover unsafe and illegal activities online, notably concerning the sale of dangerous products on online marketplaces. Article 22 of the DSA introduces a 'know your business customer' obligation for marketplaces which will help to identify traders, while preserving the anonymity of private users.

- Online platforms will not be required to verify all relevant trader data but will be required to check relevant databases and generally make "best efforts" to ensure that traders are traceable.

- We were unsuccessful in including mention of short-term rentals (AirBnB) in the article and in the recitals.

Transparency of Online Advertising (Article 24)

The issue: Online platforms collect and connect the huge volumes of personal data, in particular their behaviour and interests, to create detailed profiles and target users with advertising. Such surveillance advertising spies on everything that users do without them noticing that this is happening. There is increasing awareness of the dramatic negative effects this has on our fundamental rights, our democracy and SMEs. This Article 24 DSA therefore generates greater transparency in online advertising. The Greens/EFA campaigned for a clear prohibition of surveillance advertising that goes beyond transparency.

What we got:

- 👎 Sadly, it became clear during negotiations that there was not only no majority for banning surveillance advertising, but also that the centre-right majority was pushing hard to lower the current data protection and privacy standard of the GDPR and the ePrivacy Directive. As a result, this was the best outcome available in the circumstances.

But:

- 👍 Very positive additions include more transparency on the financing of advertising.
- 👍 We successfully broadened the transparency rules to oblige platforms to inform users about all parameters used to target them with advertising (and not just select a few meaningless "main" parameters) and how to change those parameters.
- 👍 We achieved clearer rules on consent for advertising, for instance that **"refusing consent should be no more difficult or time consuming than giving consent".**
- 👍 The **targeting of minors is prohibited**, while no additional data should be collected to identify minors for the sole purpose of respecting this obligation.

Transparency of Recommender Systems (Article 24a/29)

The issue: Much of the damage done by online content such as hate speech, defamation and disinformation relates to its viral spread and amplification on and by big social media platforms whose business models are based on maximising attention while lacking transparency and accountability. Today, most of the big social media networks use automated systems to recommend content or products (like YouTube's "Next Up" or Facebook's "Groups you should join"), and to rank, curate and moderate posts. Article 24a addresses the use of such recommender systems and creates more transparency in how they are used to target users.

What we got:

- 👍 The Commission suggested transparency only for those recommender systems that are used by the very large platforms - we successfully suggested a change in scope to apply those obligations to all platforms' recommender systems, irrespective of platform size.

- 👍 Platforms must transparently explain how they recommend content.
- 👍 We successfully demanded for additional details to generate more transparency about the criteria that recommender systems use to target or to exclude users.
- 👍 Article 24a also allows users to modify the recommender systems to have information presented in a different order.
- 👍 Article 29 obliges very large online platforms to provide at least one option that is not based on profiling.

- 👎 The transparency requirements are weakened by qualifiers like "main" parameters that are "most significant" and without "***prejudice to trade secrets and intellectual property rights*****"**, which essentially void the Article of meaning. We fiercely opposed the addition of **trade secrets**, and regret that the centre-right majority included this item, especially in light of the Frances Haugen's testimony to the European Parliament.
- 👎 Our proposals for the interoperability of recommender systems were rejected by RE and EPP. This would have ensured that users can choose third-party systems for the organisation of content in their timelines.

Additional obligations for platforms primarily used for the dissemination of user-generated pornographic content (Article 24b)

The issue: Police authorities, women's rights activists and digital experts have been observing a worrying development for years: more and more women and members of the LGBTQ+ community are being sexually harassed, threatened and demeaned. The Council of Europe estimates that 9 - 10 million women in Europe are affected. More recent studies by the World Wide Web Foundation, the World Association of Girl Guides and Girl Scouts, and Plan International show that over 50% of all girls and young women (15 - 25 years of age) have already experienced sexual violence on the internet. A widespread form of sexualised violence on the internet is image-based sexualised violence, where intimate images and videos are shared on the internet without the consent of the person depicted - generally almost unhindered via social media and porn sites.

What we got:

- 👍 This new Article introduces additional obligations for porn platforms and is entirely based on an amendment tabled by the Greens/EFA (AM 1521)
- 👍 Porn platforms are now obliged to take technical and organizational measures to:
    - that users who disseminate content have verified themselves through a double opt-in e-mail and cell phone registration

- professional human content moderation, trained to identify image-based sexual abuse
- suspend content without undue delay when receiving a notification via a notification procedure additional to the mechanism described in Article 14, which would allow individuals to notify the platform that the content is depicting them and is being disseminated without their consent.

VLOPs definition (Article 25)

The issue: The DSA introduces different layers of obligations in order to avoid disproportionate burdens for small services. It includes a section for "very large online platforms" (VLOPs) who will have to comply with additional rules because they have a particular impact on the economy and society and pose particular risks in the dissemination of illegal content and societal damages. Article 25 defines that a VLOP is a platform with at least 45 million monthly active users. The methodology for counting users of has however been amended by the European Parliament by including a methodology to define "monthly active users".

What we got:

- The change narrows down the range of services that could potentially be defined as a "VLOP" and risks excluding platforms from obligations to which they, following the logic of the Regulation, should be subjected.
- Users connected on multiple devices should only be counted once, implying the collection of much more data to identify such people.
- The provision might also imply that only logged-in users should be counted, significantly modifying the 45 million threshold for those platforms where users usually do not log in.
- The exclusion of automated bots could also lead to further encourage fraudulent practices in online advertising.
- This methodology is highly problematic for data protection reasons.

Risk assessment and mitigation (Articles 26 and 27)

The issue: With the DSA, the European Commission recognised the negative impacts and risks that very large online platforms pose not only for our rights and freedoms, but also more broadly for our society and democracy. Much of the damage done by online content such as hate speech, defamation and disinformation relates to its viral spread and amplification on big social media platforms whose business models are based on maximising attention while lacking transparency and accountability. The documents leaked by whistleblower Frances Haugen have given us proof that Facebook knows exactly what harm it does but chooses profit over people.

Articles 26 and 27 introduce an obligation for platforms to assess the risks posed by their services and allow for greater transparency and oversight. The risk assessments lead to

obligations on risk mitigation measures, which must be transparent and involve adequate consultation. These will be evaluated by the Commission, which may issue recommendations. Furthermore, the Digital Services Board and Commission will report on the risk assessment measures taken by VLOPs.

What we got:

- Mandatory risk assessments for big platforms are significantly strengthened to also include algorithmic systems, and to assess risks before the launch of a new service.
- They must now also assess what risk could arise not only from malicious uses but also from how the "**service was designed and how the operation was intended to be used"**.
- They must now cover "***actual or foreseeable negative"*** effects for a range of additional potential damages including to civic discourse, democratic values and media freedom.
- The risk assessments must assess the ***"amplification of content".***
- They must also address the influence of, inter alia, underlying data collection, processing and profiling.
- The supporting documentation of risk assessments must be sent to the regulators (the Digital Services Coordinator).

- Unfortunately, Greens amendments to also include environmental risks in the risk assessment and mitigation were rejected.

Audits (Article 28)

The issue: There are currently no harmonised rules which allow us to hold big tech platforms to account, and to really "look under the hood". Article 28 stipulates that VLOPs will be required to pay for independent compliance audits in accordance with their obligations under Chapter 3 of the Regulation (Art. 10 – 37), which encompasses a range of provisions such as the notice and action system and redress mechanisms, obligations on transparency reporting, and risk mitigating measures including the use of codes of conduct.

What we got:

- We have strengthened the independence of audits, specifically by prohibiting "revolving doors" between auditors and VLOPs.
- Auditors must be given access to all relevant platform data.
- There is now a clear list of elements that must be audited in the corresponding recital (60).

Online advertising repositories (Article 30)

The issue: The underlying business model of many online platforms is the targeting of advertising to specific individuals, or to specific groups of individuals, with little transparency and accountability as to how this targeting and microtargeting is done. Reports in recent years have revealed that advertising discriminates, especially in the areas of housing, employment, and credit. Moreover, advertising tools have increasingly been used to disseminate targeted disinformation to vulnerable groups. In response to growing concern, Facebook and Google have voluntarily set up ad libraries, but have been criticised for the inaccurate and incomplete data in their repositories. The game changer of Article 30 DSA: advertisements that were previously only delivered to their target audience now become a matter of public record.

What we got:

- The big online platforms are now obliged to publish a registry detailing the advertisements sold on their service, along with certain metadata including the ad buyer's identity, the identity of person who paid for it, the period the ad was displayed for, audience demographics, and information about how the ad was targeted.
- We successfully included transparency requirements for hidden marketing and advertising by influencers.
- We successfully included an obligation to report which parameters the platform used "***to exclude particular groups***" which is important for analysing whether there is bias or discrimination.

- Unfortunately, our proposal to extend the period during which the ads must be made publicly available in their repository from one to seven years (which is already current practice at Facebook) was not adopted.

Access to platform data (Article 31)

The issue: Very large online platforms play an increasingly important role in society, with a huge power to influence opinions and the public discourse. Access for researchers, civil society and investigative journalists is therefore paramount for holding platforms to account, allowing independent oversight and enabling us to understand how these platforms work. However, very large online platforms, and Facebook in particular, have repeatedly interfered with independent research projects: Facebook tried to shut down an independent audit of their political ads by NYU, and then suspended researchers' Facebook accounts, stripping them of access to the Ad Library API and Crowdtangle research tools. Very recently, Facebook retaliated against data collection by the AlgorithmWatch NGO which was monitoring Instragram's newsfeed algorithm, by threatening it with legal action on the grounds that the NGO violated

the platform's Terms of Service. The issue of ensuring research access has therefore become urgent in platform regulation.

What we got:

- There were some significant victories regarding the access to VLOP data for Digital Services Coordinators and the Commission, such as that the platform must explain ***"the design, logic and the functioning of the algorithms if requested by the Digital Service Coordinator"***
- As it is important to understand how content is amplified and how it spreads, we successfully included that vetted researchers and organisations must have access to ***"aggregate numbers for the total views and view rate of content prior to a removal"***
- We were successful in **ensuring access for vetted not-for profit organizations** who can play a crucial role in contributing to further knowledge on harmful practices of the VLOPs.
- A big Green success was the removal of a loophole that could have allowed big tech to use "trade secrets" as a justification for blocking access to data.

- No fixed deadlines by when access should be given.
- No possibilities to request access to data via three Digital Services Coordinators of destination.

Standards, Codes of Conduct (Articles 34 and 35)

The issue: In the past years, the European Commission has launched a series of intransparent initiatives, inviting big tech platforms to abide by non-binding guidelines in an aim to establish procedures to fight against terrorism, hate speech or disinformation online. However, such voluntary codes raise a number of concerns, not only because they entrust private companies with the regulation of online communications - but also regarding their efficiency, the lack of key indicators (other than the quantity of removals), the lack of transparency over the measures taken and oversight. The proposal for Article 35 is a big step in the right direction. It will ensure that future voluntary codes will be regularly reviewed, in particular for potential negative effects, that they will clearly specify their goals, and that they include key performance indicators to measure their efficiency. Article 34 proposes the establishment of industry standards to assist compliance with the Regulation.

What we got:

- We ensured better oversight, more clarity on the public policy objectives of individual codes, clarity on the role, if any, of public authorities and, in the recital, mechanisms for independent evaluation.

- Elements added to the Commission's initial proposal include standards on terms and conditions, traceability of traders, advertising practices, recommender systems and protection of minors.
- A further element grants new power to the Commission to implement delegated acts on any of the points listed, if an appropriate standard has not been adopted.

- Unfortunately, Greens amendments to introduce standards for sustainability connection with energy, heat and water consumption by data traffic and data centres were rejected.
- Our amendment to democratise such self-regulatory measures through citizens' assemblies was not successful.

Enforcement (Chapter IV)

The issue: With the DSA, the European Commission has tried to avoid past mistakes, especially when it comes to the enforcement of the EU's data protection rules (GDPR). The DSA's enforcement involves various actors alongside the Commission in a maze of responsibilities. Each Member State shall appoint a Digital Services Coordinator (DSC) who is responsible for supervising the intermediary services established in their Member State. Unlike in the GDPR, the DSA provides strict deadlines for the DSC of establishment to answer a request of investigation and enforcement from another DSC or the Board of Digital Services Coordinators (Board) that can also advise the Commission. However, where very large online platforms (i.e., those with 45 million monthly users) are concerned, national regulators are required to coordinate with the Commission in a long, multi-step process.

What we got:

- The European Parliament's text on enforcement makes only minimal improvements to the Commission proposal, such as in Article 43a on redress or by adding deadlines in Article 41.

- The Greens/EFA have proposed comprehensive changes to the VLOPs enforcement mechanism by introducing a new independent EU Agency – this proposal was not adopted. We oppose the proposal to put the Commission in charge of VLOPs supervision, as the Commission is an executive body under political leadership and not an independent expert regulator as is needed to oversee platforms. While we understand the logic behind the DSA's centralised enforcement of VLOPs' obligations, this mechanism creates a potential democratic deficit within the EU institutional

framework. Decisions by the Commission will be subject to heavy lobbying by the big tech platforms.

- We proposed increasing the fines for a VLOP to 10% of its total worldwide turnover - however the final report of the European Parliament maintained the 6% as suggested by the Commission.