AMNESTY INTERNATIONAL

What the EU's Digital Services Act means for human rights and harmful Big Tech business models

7 July 2022

The EU's Digital Services Act (DSA) has crossed the finish line, with the European Parliament adopting the proposal in a vote on 5 July 2022.[1] This landmark digital regulation has gone through the legislative process in record speed and is expected to be of similarly transformative force as the EU's General Data Protection Regulation (GDPR). The following analysis provides an overview of what the legislation means for our rights in the digital age, and for holding powerful tech companies to account.

The DSA contains horizontal rules defining responsibilities and obligations for **providers of intermediary services** offering services in the European Union (EU). Examples of intermediary services are messaging services, web-based email services, web-hosting services and online platforms, such as social media and online marketplaces. Among the stated aims of the DSA is the creation of harmonised rules for a safe, predictable and trusted online environment where **fundamental rights** are effectively protected. The consolidated text of the DSA has been released and is expected to be subject only to minor changes after legal review and translation.[2]

The DSA was negotiated alongside its sister law, the Digital Markets Act (DMA).[3] The DMA seeks to curb the dominance of Big Tech by preventing "gatekeeper" platforms from anti-competitive practices and by forcing them to open up their services. From a human rights perspective, this is a great step to ensure the protection of people's rights and enable open and fair digital spaces that give people a real choice, including by ensuring that people can freely move between platforms and choose more rights-respecting alternatives.

Since 2019, Amnesty International has been calling out the harms of the surveillance-based business model of Facebook and Google, setting out how it is inherently incompatible with the right to privacy and poses a systemic threat to a range of other rights including freedom of opinion and expression, freedom of thought, and the right to equality and non-discrimination.[4] The present analysis focuses on specific parts of the DSA related to this business model, in particular the provisions on systemic risks, including online advertising, and algorithmic recommender systems.[5]

---

[1] European Commission, *Commission welcomes European Parliament´s adoption of Digital Services Package*, 5 July 2022 ec.europa.eu/commission/presscorner/detail/en/ip_22_4313

[2] Regulation (EU) 2022/... of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act), 2020/0361(COD), www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2022/06-15/DSA_2020_0361COD_EN.pdf

[3] Regulation (EU) 2022/... of The European Parliament and of The Council on contestable and fair markets in the digital sector (Digital Markets Act), 2020/0374 (COD), www.consilium.europa.eu/media/56086/st08722-xx22.pdf

[4] Amnesty International, *Surveillance Giants: How the business model of Google and Facebook threatens human rights*, November 2019, www.amnesty.org/en/documents/pol30/1404/2019/en/

[5] Given that the numbering of the Articles of the DSA is still subject to change, this analysis will not cite specific Articles.

RISK ASSESSMENT AND MITIGATION

The DSA introduces, as a first of its kind, novel obligations on very large online platforms (VLOPs) and very large online search engines (VLOSEs) to **assess and mitigate systemic risks** that arise from the "**design, including algorithmic systems, functioning and use** made of their services".

Very large online platforms and very large online search engines are those that reach an average of **45 million monthly active users within the EU** and that are designated by the European Commission as such. Among the platforms that are highly likely to be designated as VLOPs/VLOSEs are Meta's Facebook and Instagram, Alphabet's Google Search and YouTube, TikTok, Amazon, and potentially Twitter.

VLOPs and VLOSEs will need to carry out **risk assessments** on a yearly basis with a wide-ranging list of systemic risks to be included in the assessment, which covers the following:

- the dissemination of illegal content;
- actual or foreseeable negative effects:
  - on any fundamental rights with a specific mention of a number of rights;
  - on civic discourse, electoral processes and public security;
  - in relation to gender-based violence, the protection of public health, minors and serious negative consequences to the person's physical and mental well-being.

This broad appreciation of risks is welcome given the reality of the wide range of adverse impacts that are stemming from these systems, from the spread of "hate speech" and disinformation, to the undermining of people's privacy and their right to non-discrimination, to the amplification of content impacting people's mental health.

Furthermore, VLOPs and VLOSEs are required under the DSA to consider how certain factors, including the design of their **recommender systems, their terms and conditions, advertising systems and data related practices** influence the systemic risks. The assessment also must analyse how the use of bots and fake accounts influence these risks and take into account specific regional or linguistic aspects.

As a next step, having assessed the risks, VLOPs and VLOSEs need to take **reasonable, proportionate and effective risk mitigation measures** with particular consideration to the **impacts** of such measures **on fundamental rights**.

The DSA lists a number of examples of **risk mitigation measures**, including the following:

- adapting the design, features or functioning of their services, including their online interfaces;
- testing and adapting their algorithmic systems, including their recommender systems;
- adapting their advertising system and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide;
- taking awareness-raising measures and adapting their online interface for increased user information.

Under the **UN Guiding Principles on Business and Human Rights (UNGPs)** and other international standards, companies are required to conduct **human rights due diligence** across all their business activities and relationships. This is understood as the process of identifying and assessing; ceasing, mitigating and preventing; tracking and monitoring; communicating and accounting for human rights risks and impacts.

As affirmed by OHCHR's B-Tech project, in the technology sector this implies that companies should: **i)** pro-actively identify when their **business model-driven practices**, and related **technology designs**, create or exacerbate human rights risks; and **ii) take action** to address these situations—whether by mitigating risks within existing business models or by innovating entirely new ones.[6]

As such, while regrettable that business model-driven practices are not given specific consideration in the text of the DSA, the legislation does specifically affirm that advertising-driven business models are a factor adding to the systemic risks of the VLOPs and VLOSEs. It is also welcome that related factors have been taken into account in the risk assessment and mitigation measures, such as **design, algorithmic systems including recommender systems, advertising systems, and data practices**. This means that tech giants will have to become more accountable for the use of toxic content-shaping algorithms that are amplifying hate speech, disinformation or gender-based harassment, and that they will have to **adapt the functioning and design of these recommender systems** to avoid the spread of such harmful content.

These new risk assessment and mitigation provisions are revolutionary and precedent-setting and have the potential to go a long way to **counter the harms stemming from Big Tech's business model and design choices**. Google, Meta and others will have to account for and likely make significant changes to their harmful **surveillance-based advertising model**. However, it still remains to be seen how the rules will be implemented in practice and how effective enforcement will be.

AUDITS

Providers of VLOPs and VLOSEs will be subject to **yearly independent audits** to assess compliance with their due diligence obligations, including the risk assessment and mitigation measures. The DSA specifies safeguards to ensure that organisations carrying out the audits are independent and free from conflicts of interest with the technology companies.

Audits will also assess compliance with commitments undertaken under codes of conduct, which can be drawn up under the DSA to tackle systemic risks. Such codes of conduct are monitored and evaluated by the European Commission, and VLOPs/VLOSEs that adhere to its commitments can thereby demonstrate compliance with risk mitigation measures. An example is the Code of Practice on Disinformation, signed by Facebook (now Meta), Google, TikTok and others.[7] that contains commitments, e.g. related to online advertising, tackling manipulative practices, transparency and access to data and will become part of the signatories' risk mitigation measures under the DSA.

---

[6] OHCHR, *Addressing Business Model Related Human Rights Risks: A B-Tech Foundational Paper*, July 2020, www.ohchr.org/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

[7] European Commission, *The 2022 Code of Practice on Disinformation*, June 2022, digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

TRANSPARENCY:

Transparency is a key component of human rights due diligence, as set out in the UN Guiding Principles and other international standards. Companies "need to know *and show* [emphasis added] that they respect human rights" and "[s]howing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."[8]

Under the DSA, VLOPs and VLOSEs will have to, in principle, **make publicly available information on the results of the risk assessment, the specific mitigation measures and the audit reports**. However, they may remove from the public reports confidential information or other information that may cause significant vulnerabilities for the security of the service, may undermine public security or may harm recipients. This creates a potential loophole and risks that such exceptions will be used in an overly broad manner, obscuring information and hindering meaningful oversight. To counter this risk, the companies will still have to give the full information to the European Commission and the relevant Digital Services Coordinator (the enforcement authority at national level), together with a statement of the reasons why they have removed certain information from the public reports.

DATA ACCESS:

Another novel and critically important obligation the DSA imposes on VLOPs and VLOSEs is to provide the **authorities** in charge of supervising and enforcing the rules with **access to data** that are necessary to monitor and assess compliance. Access to meaningful information, including platforms' algorithmic systems, is crucial to enable oversight and to hold companies accountable for failures to comply with the rules.

Additionally, upon a reasoned request from the Digital Services Coordinator of establishment, **vetted researchers** can also get access to data to conduct research to **identify and understand systemic risks** as well as to assess the risk mitigation measures put in place. Civil society organisations advocated strongly for such provisions in the DSA as a crucial step to empower independent third parties to hold platforms to account and open up the "black box" of opaque algorithmic systems underpinning the platforms.[9]

In order to be vetted, researchers need to meet a number of conditions, including being affiliated to a research organization, being independent from commercial interests, disclosing their funding, protecting personal data and committing to making their research results publicly available free of charge. According to the recitals, research organisations may include **civil society organisations** that are conducting scientific research with the primary goal of supporting their public interest mission. In case civil society researchers do not meet this condition, they may still be able to get data access that is limited to **publicly available data** if they meet certain requirements, such as being independent from commercial interests, disclosing their funding and protecting personal data.

---

[8] United Nations Guiding Principles on Business and Human Rights, p. 15 and Guiding Principles 21, p.20.

[9] For example, see joint civil society statement, *Putting Meaningful Transparency at the Heart of the Digital Services Act*, October 2020 algorithmwatch.org/en/governing-platforms-final-recommendations ; Euractiv, *Access to platform data key to DSA, says Nobel Peace Prize winner*, February 2022, www.euractiv.com/section/digital/news/access-to-platform-data-key-to-dsa-says-nobel-peace-prize-winner/

Upon receiving a data access request, VLOPs and VLOSEs may request the Digital Services Coordinator to amend the request in case they do not have access to the data or in case giving access would lead to significant security vulnerabilities or if it would infringe on trade secrets. This clause **opens the door to overly broad interpretations** of what constitutes a trade secret and risks being used by tech companies to justify any refusal to give access to data, which will in turn strongly hamper oversight and researchers' ability to examine the data.[10]

DARK PATTERNS:

The DSA **prohibits** online platforms from designing, organising or operating their online **interfaces** in a way that **deceives, manipulates** or otherwise materially distorts or impairs the ability of users to make free and informed decisions (so called "dark patterns").

However, while such a prohibition is in principle welcome, it excludes practices which would fall under the Unfair Commercial Practices Directive or the GDPR, which makes the scope of application unclear and risks leading to a **very narrow scope of application**, leaving things like deceptive cookie banners behind.

TRACKING-BASED ADVERTISING:

SENSITIVE DATA:

The DSA **prohibits targeted advertising** practices on online platforms based on profiling using special categories of personal data aka **sensitive data** as defined under the GDPR. Sensitive data under this definition are: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

This means advertisers can no longer target people with ads based on things like their political opinion or their ethnic origin, and platforms' ad delivery algorithms may not use such data either to decide who will or will not be shown an ad. These protections are a positive step towards protecting people from intrusive data harvesting and ads that use personal information.

However, this provision **only applies to online platforms**, meaning that advertising based on sensitive data on most news websites, messaging or e-mail services would still be allowed. Additionally, the provision would have been clearer if the reference to profiling were left out, which is likely going to be a loophole used by online platforms as an attempt to further limit the scope of application.

Unfortunately, the **DSA did not go far enough** to **phase out all intrusive surveillance-based advertising** practices, as widely called for including by a coalition of political leaders, civil society organisations and companies, as well as the European Data Protection Board (EDPB).[11] Amnesty International will

[10] Claudia Prettner and Sarah Andrew, in Euractiv, *Trade secrets don't trump our rights*, November 2021 www.euractiv.com/section/digital/opinion/trade-secrets-dont-trump-our-rights/

[11] See for example, Joint civil society open letter, *EU member states urged to curb invasive internet practices*, March 2022 www.amnesty.eu/news/eu-member-states-urged-to-curb-invasive-internet-practices/ ; Tracking-Free Ads Coalition, https://trackingfreeads.eu; European Data Protection Board, *Statement on the Digital Services Package and Data Strategy*, November 2021, https://edpb.europa.eu/system/files/2021-

continue calling on legislators around the world to put an end to harmful surveillance advertising practices.

MINORS:
The DSA **prohibits targeted advertising** practices on online platforms based on profiling using **personal data of minors** if they are aware with reasonable certainty that the user is a minor. Platforms are not obliged to process additional data in order to assess whether the user is a minor.

This provision is far from being clear and raises questions as to how platforms will assess or be aware "with reasonable certainty" whether or not a user is a minor – without further intrusive data processing. Research has found that "the best way to keep children safe from the sale of their personal data on the internet is to ban all online advertising which targets users based on personal data".[12]

RECOMMENDER SYSTEMS

Algorithmic recommender systems facilitate access to information while ranking, prioritising and amplifying certain messages. They are responsible for what kind of content people see in their social media feeds, they stimulate public discourse and impact people's ability to retrieve and interact with information online.

TRANSPARENCY:
Online platforms will have to **disclose** in their terms and conditions the **main parameters used in their recommender systems** in order to explain why certain information is suggested to the users. This information has to include at a minimum, according to the DSA, the most significant criteria in determining the information suggested and the reasons for the relative importance of these parameters.

This is a **very weak protection** and means that people will not have the right to individual information but merely general information, which they will have to search for in lengthy terms and conditions. Furthermore, the criteria to be disclosed should be much more detailed than the ones the DSA stipulates, allowing people on an individual level to understand why they are shown certain content.

PROFILING:
Providers of VLOPs and VLOSEs that use recommender systems will have to provide **at least one option** for each of their recommender systems which is **not based on profiling** within the meaning of the GDPR. However, the DSA does not include a requirement for this option that is not based on profiling to be the default option. This is a missed opportunity, given that changing the default settings is often cumbersome and the majority of people will keep whatever option is the default.[13]

11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf

[12] New Economics Foundation, *Ban Surveillance Advertising To Protect Kids Online*, May 2021 neweconomics.org/2021/05/ban-surveillance-advertising-to-protect-kids-online

[13] CNet, *Default settings for privacy -- we need to talk*, December 2019, https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/

Under Article 4(4) of the GDPR, profiling is understood as any form of automated processing of personal data to evaluate certain personal aspects, such as to analyse or predict aspects concerning a person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. It follows that profiling involves the **processing of large amounts of personal data**, which is therefore inherently predisposed to include sensitive personal data (such as data related to a person's health, sexual orientation or political opinion). In line with the GDPR, this would mean that the data subject's **explicit consent** would be needed for the processing of such data and a mere possibility to opt-out of a recommender system based on profiling would not be sufficient.

It remains to be seen how platforms will implement this obligation in practice but more clarity by the legislator would have been useful to avoid unnecessary loopholes and to ensure a high standard of protection.

ENFORCEMENT:

The DSA will be **enforced by national authorities** and it is up to the EU member states to designate the authority or authorities in charge at national level. Member states have to designate one of these authorities (in case there is more than one) as Digital Services Coordinator (DSC), which will be the main authority responsible for supervision, enforcement and cooperation with other authorities. The DSCs have to be independent and be equipped with sufficient technical, financial and human resources to carry out their tasks.

The competence for supervision and enforcement lies with the **member state of the main establishment of the provider**.

As an **exception** to this rule, the DSA gives the **European Commission exclusive competence** for supervision and enforcement of the specific obligations imposed on **VLOPs and VLOSEs**. This is a welcome provision that is expected to **prevent forum shopping** and the possibility for providers to escape enforcement by choosing a jurisdiction with lax enforcement. It should also ensure **more consistency** in the enforcement of the rules and potentially address the lack of resources or expertise within national supervisory authorities.

Even though the Commission is specifically tasked with developing expertise and capabilities for this oversight function and to act in mutual cooperation with the DSCs, it remains to be seen whether the Commission will have built up the necessary resources and expertise by the time the DSA becomes applicable. The Commission, with support of the European Parliament, must ensure necessary resources are in place in a timely manner to effectively enforce the DSA.

In the case of **non-compliance** with the DSA, companies can be **fined** with an amount of up to **6% of their global annual turnover**. The Commission can furthermore conduct **inspections** at the premises of the provider, which includes the right to require the provider to give **access** to and **explanations** in relations to its **algorithms, data-handling and business practices**. If the provider does not comply with the request, they can be fined up to 1% of their global annual turnover. As a result, after the DSA comes into force it is likely that we will start to see significant fines being levied on Big Tech companies.

RIGHT TO REDRESS AND REMEDY:

Access to effective remedy is a foundational component of international human rights law. In the context of corporate actors, under the UNGPs States are required to take "appropriate steps to prevent, investigate, punish and redress" business-related human rights abuses within their territory/jurisdiction.

In case of infringements of the DSA, users and any organisations mandated to exercise their rights on their behalf have the **right to complain to the DSC** in their country of residence against providers of intermediary services. They also have the right to receive **compensation** from providers of intermediary services against damage or loss suffered stemming from infringements.

The DSA also foresees the possibility for **collective redress** under Directive 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers. This would substantially improve people's right to redress as it relieves the high burden for them to seek redress individually.

APPLICATION OF THE RULES:

The rules of the DSA will apply **15 months after their entry into force or on 1 January 2024** – whichever date is later. However, the obligations on **VLOPs and VLOSEs** could apply at **an earlier date**, namely four months after the notification of their designation by the Commission. This means it will still be some time until we will see any enforcement action.

CONCLUSION:

In conclusion, the DSA is a landmark piece of legislation to strengthen our rights in the digital age and while its scope is limited to the European Union, it is expected to create ripple effects far beyond its territory.

As outlined in the analysis, there are some missed opportunities and areas where the DSA could have gone further to ensure appropriate protection of our rights, and the legislation fell short of truly overhauling the destructive business model of surveillance advertising. Overall, however, the DSA will certainly have a positive impact and move us towards an online world that puts better control over so far unaccountable Big Tech giants.

Going forward, it is crucial that the rules are effectively enforced from day one. We cannot waste more time and can no longer be left at the mercy of Big Tech and harmful surveillance-based business models. Our rights in the digital world need to be protected now.