

# EU'S DIGITAL SERVICES ACT AND ITS HUMAN RIGHTS IMPLICATIONS



BY RIKKE FRANK JØRGENSEN, SENIOR RESEARCHER AT THE DANISH INSTITUTE FOR HUMAN RIGHTS, PARTNER OF THE CPH TECH POLICY COMMITTEE

This CPH Tech Policy brief is based on the Danish Institute for Human Rights' legal brief about the EU Digital Service Act (DSA) and its human rights implications<sup>1</sup>. The brief provides an overview of areas within the DSA that continue to present human rights challenges concerning digital platforms.

## OVERVIEW

The DSA has several positive implications for citizens' human rights protection on digital platforms as it ensures stronger protection against illegal content. Furthermore, it increases regulation of the online platforms' decisions to remove content and includes both internal and external complaint mechanisms for affected citizens. In addition, very large online platforms are subject to specific due diligence obligations to identify, analyse and mitigate systematic human rights risks regarding the use of their platforms. In certain cases, the DSA also requires platforms to state how their content-selecting algorithms work and how users can disable the use of these algorithms. Finally, the DSA sets out a range of requirements regarding oversight and enforcement.

Despite these positive implications, human rights challenges remain as the DSA's requirement to quickly remove illegal content may lead platforms to remove more legal content than necessary as a precautionary measure. This risk is well-documented and can have a negative impact on citizens' freedom of expression and information.

## BACKGROUND

In 2022, the EU adopted the Digital Service Act, which regulates, among others, social media platforms. This is the first time the EU explicitly regulates tech giants. In the DSA, tech giants are referred to as very large online platforms,

whereas in the Digital Markets Act (DMA) they are referred to as gatekeepers. Tech giant is not a legal term but refers to technological companies with a major impact on the human rights of citizens due to these companies' control of platforms where communication, research, public debate, etc. take place. Furthermore, these platforms have access to extensive data collection of their users. Tech giants thus have an unprecedented opportunity to influence the human rights and democratic processes of millions of citizens.

The DSA works in correspondence with other existing and forthcoming EU regulations (see figure 1). To ensure the protection of human rights, it is necessary that these EU regulations are seen as a combined package of supplementing regulations that are effectively enforced. In addition, it is crucial for the effective protection of human rights under the DSA that the national authorities responsible for monitoring the DSA have the necessary human rights expertise and that there is a focus on the rights of the citizen in the established redress mechanisms.

## TAKE-DOWN OF ILLEGAL CONTENT

The DSA defines illegal content as all products, services, and activities that are illegal under national law, such as illegal hate speech, terrorist-related content, or sharing private images without consent. The DSA states that digital platforms are generally not liable for illegal content shared or stored on their platforms. However, they have a responsibility to respond without undue de-

lay to orders from national authorities to remove illegal content or prevent access to it. National authorities can also issue injunctions to disclose information about one or more users that, for example, share illegal content. Under the DSA, failure to comply with an injunction can lead to fines. Depending on the circumstances, it may also lead to co-liability for illegal content under the general rules of criminal law. Clarification is needed as to when digital platforms incur such co-liability for illegal content.

## DUTY TO ACT ON USERS FLAGGING

The DSA obliges digital platforms to establish mechanisms to ensure that users can report content that they consider illegal. The platforms have a duty to act, which means that they are obliged to respond to the user notification without undue delay. If the content is removed or if the user is deactivated or blocked, specific reasons behind the decision must be provided.

Platforms must take human rights into account when making the decision - not least the right to freedom of expression and information, respect for private and family life, the right to protection of personal data, the right to non-discrimination and, where appropriate, the right to human dignity and rights of the child. In some cases, the assessments of whether the content is illegal require quite complex legal assessments that the platforms, as private actors, must make. Due to the volume of content, especially on very large platforms, the review and assessment of content will often be done in whole or in part by algorithms. It can be almost impossible to understand why specific content has been removed by the algorithm, which is problematic from a human rights perspective.

## TRANSPARENT TAKE-DOWN OF CONTENT

The DSA acknowledges that the platforms are entitled to set terms and conditions for the use of their services following contract law. However, the DSA imposes certain requirements on the platforms' terms and conditions, including that they inform the user about their use of algorithms to make decisions concerning content accessibility on their platform.

If the platforms decide to remove or restrict access to content from a user or otherwise limit its visibility, the platform must inform the user of its decision in an easily understandable manner. This applies regardless of whether the content is removed or restricted because the platform considers that the content is illegal or in breach of the platform's terms and conditions. The notification and justification requirements also apply when the platform partly suspends the user or permanently excludes the user from the platform. The requirements apply regardless of whether the visibility of the content is restricted, whether it is restricted for one or more users, or whether the user is blocked without being aware of it ('shadow banning').

It is positive that the requirements of the DSA create some transparency regarding the platforms' removal of legal content, including whether and how freedom of expression and information is considered.

## TRANSPARENCY AND OPT-OUT OF PROFILING

The DSA also sets transparency requirements for how digital platforms select content for the individual user. Platforms' recommender systems are usually based on algorithms, that

**FIGURE 1** EU Regulations

ABBR.	REGULATION	SHORT DESCRIPTION
DSA	Digital Services Act	Aim to protect users from harmful or illegal content by providing better information about why specific content is recommended and make users able to choose an option that does not include profiling.
DMA	Digital Market Act	Aims to ensure fair practices among different digital market actors aiming to ensure a level playing field for all digital companies, regardless of their size.
AI ACT	Artificial Intelligence Act	Aims to assign applications of AI to three risk categories. AI within the unacceptable risk category is banned, high-risk applications are subject to specific legal requirements and the remaining are left unregulated.
GDPR	General Data Protection Regulation	A general data protection law that regulates how the personal data of individuals in the EU may be processed and transferred.
CSDDD	Corporate Sustainability Due Diligence Directive	Aims to foster sustainable and responsible corporate behavior by ensuring that businesses address adverse impacts of their actions, including in their value chains inside and outside Europe.

Sources: [The Digital Services Act Package](#) - [The Artificial Intelligence Act](#) - [The General Data Protection Regulation](#) - [Corporate Sustainability Due Diligence](#)

recommend content to specific users based on user information stored on the platform. The DSA requires that users are informed of these criteria and their relative importance. In addition, for very large online platforms it is required that each of their recommender-systems provide the user with at least one option to opt-out from recommender-systems that are based on user profiling.

It is positive that the DSA requires increased transparency on the use of algorithms for content selection. It is also positive that users on very large platforms can opt out of user profiling. In this regard, it is crucial that the user can easily opt out of user profiling.

### INTERNAL COMPLAINT HANDLING SYSTEM

The DSA sets out rules requiring citizens to have access to a so-called out-of-court dispute settlement body. The body which cannot take binding decisions must be impartial and independent, have the necessary expertise and be able to settle disputes quickly and efficiently. The body is certified by a national authority in each Member State. The Danish Institute for Human Rights has previously recommended that an independent Danish board chaired by a judge should be able to review selected cases of principle where citizens have had their content removed. The complex legal assessments made by the platforms should be subject to an independent legal review on, for example, whether and how freedom of expression and information has been safeguarded. The recommendation for an independent legal review is also based on the need to document how the platforms in practice balance considerations concerning freedom of expression and information.

It is positive that the DSA establishes an independent complaint body. However, to ensure an effective protection of citizens' rights, it is essential that the body in practice base its decisions on a human rights assessment of all the rights implicated in the decision. It is also important that platforms comply with the body's decisions, even if they are not legally binding.

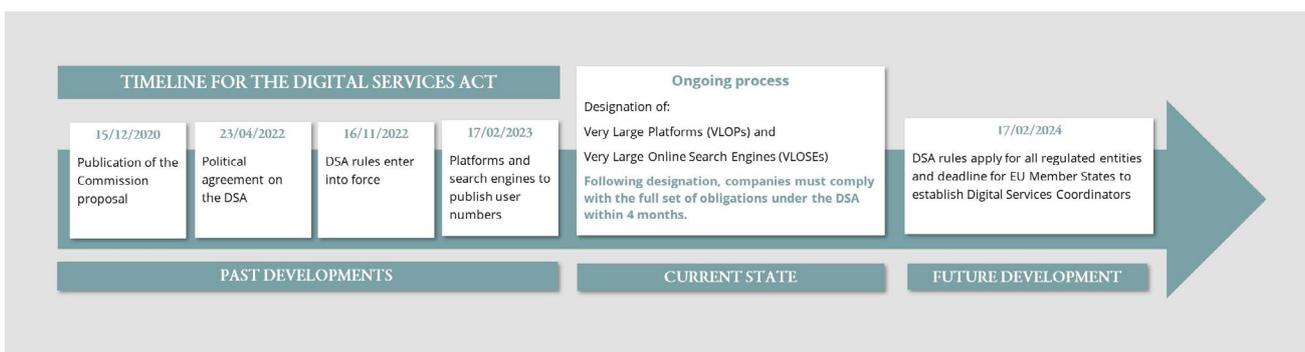
### OVERSIGHT OF THE DSA

Generally, the DSA will be enforced by supervisory authorities designated by the Member States. The national authority must have a set of investigation and enforcement competencies in relation to the digital platforms, including the ability to issue an injunction. The injunction could, for example, act against illegal content. The authorities may also impose fines in case of non-compliance with the DSA. Fines for breaching an obligation in the DSA can amount to up to 6% of the platform's annual global turnover. As a specific enforcement measure, the Commission has a so-called exclusive competence to monitor several of the requirements targeting major digital platforms. For example, the Commission can conduct on-site inspections of the platforms and require access to and descriptions of the platform's algorithms, data management, and business practices. As national authorities will be responsible for a large part of the oversight and enforcement of the DSA, it is essential that the national supervisory authorities have the necessary human rights expertise.

### DUE DILIGENCE AND HUMAN RIGHTS

The DSA lays down several due diligence requirements for very large online platforms. The platforms are subject to requirements for, among other things, risk analysis focusing on the human rights risks that arise or increase due to the size of the platforms. This includes risks of their services being used to distribute illegal content quickly and widely. It concerns risks to freedom of expression and information and furthermore it includes the risk of negative impacts on democratic processes, public debate, and electoral processes, as well as public security. Finally, it includes specific considerations for minors, including negative impacts on their physical and mental well-being, as well as impacts on gender-based violence.

The DSA's due diligence requirements thus address selected systematic human rights risks that are well-known and characteristic of very large digital platforms. However, the DSA does not specify in detail how platforms should carry out their risk analysis and -management in practice. The EU is currently negotiating a Corporate Sustainability Due Diligence Directive (CSDDD). This Directive will establish a set of binding human rights due diligence requirements covering all human rights. Like the DSA, this directive is aimed at large



companies, whereas the UN Guiding Principles on Business and Human Rights cover all companies regardless of size. The Danish Institute for Human Rights has recommended that the due diligence requirements should include companies of all sizes, as in practice the requirements will vary depending on the risk that companies pose in relation to citizens' rights. Similarly, it is important that the DSA's due diligence requirements are supplemented with criteria and guidelines that ensure uniform and thorough human rights risk analysis etc. from the platforms.

## GDPR: EFFECTIVE ENFORCEMENT

The Danish Institute for Human Rights has previously emphasized the human rights challenges that arise from the fact that major platforms base their business models on the collection of large amounts of personal data. The DSA requires increased transparency concerning what content the user is exposed to on the platform and why content is either removed or present on the platform.

However, it is not the DSA that regulates the data collection, but the DMA and the GDPR. The DMA prohibits tech giants (gatekeepers) from using personal data for third-party advertising, combining personal data across the platforms' different services, or combining it with personal data obtained from other platforms. The purpose of the prohibition is to limit the platforms use of personal data. The prohibition can be waived if the user voluntarily gives a specific and informed consent under the GDPR. However, in practice, it has proven difficult to enforce the GDPR against very large online platforms. This applies both in relation to the requirements for consent, the requirement for a clear and limited purpose for the data collection, and for the principle of data minimization. The principle of data minimization means that the data processor (such as a digital platform) must not collect more personal data than what is strictly necessary for the stated purpose.

The difficulties of enforcing the GDPR has a negative impact on the protection provided by the DMA. There may be a risk of similar challenges for the DSA, for example in relation to the user's ability to effectively opt-out of algorithmic profiling. The fact that there are challenges in enforcing the GDPR against the large platforms reduce the overall human rights protection on digital platforms, including the protection under the DSA and the DMA. If a DSA 2.0 is considered, these as well as other human rights challenges should be addressed in the revised regulation.

## SUMMARY

### The DSA's positive impacts on human rights

- ➔ Increased protection against illegal content on digital platforms.
- ➔ Insight into content moderation by digital platforms, including the use of algorithms.
- ➔ Access to internal and external complaint mechanisms.
- ➔ Certain due diligence requirements for tech giants.
- ➔ Insight into content selection algorithms and, in some cases, the possibility to opt out.

### Challenges/dilemmas

- ➔ Uncertainty about situations in which platforms have coliability for illegal content.
- ➔ Risk of unjustified removal of legal content.
- ➔ Uncertainty about whether supervisory- and complaints handling bodies will have sufficient focus on human rights.
- ➔ Need for human rights due diligence requirements for all digital platforms regardless of size.
- ➔ Challenges in enforcing EU regulation on tech giants.

## POLICY RECOMMENDATIONS

- ➔ The Public Prosecutor's Office tries cases against digital platforms in the courts to determine the limits of the platforms' co-liability.
- ➔ The complaints body bases its decisions on a human rights assessment and platforms comply with the body's decisions, even if they are not legally binding.
- ➔ The Commission sets criteria and guidelines for the DSA's due diligence requirements.
- ➔ The user has easy access to opt-out of user profiling.
- ➔ The national supervisory authority is provided with the necessary human rights expertise.

## REFERENCES

- 1 INSTITUT FOR Menneskerettigheder. "RETSAKTEN OM DIGITALE TJENESTER I ET Menneskeretligt perspektiv." (2023)