Policy briefing: Digital Services Act and Digital Responsibility in Europe

Background:

- A year ago, the European Commission presented its proposal for a Digital Services Act (DSA), to provide updated rules for how large and small organisations manage online content.
- Recognising the systemic risks in digital services, the DSA proposes rules on accountability and auditing that will increase understanding of their social impact.
- It aims to tackle child sexual abuse material, terrorist content and dangerous products, but also force platforms to reveal how their technologies work, including in relation to content moderation, age verification and other trust and safety processes.
- Requirements of the DSA include external risk auditing requirements, a field in which the Internet Commission is a first mover, having now twice implemented an independent accountability reporting process with a group of pioneering digital organisations.

- Through its first two reporting cycles, the Internet Commission has identified and evaluated 46 trust and safety practices, a unique body of evidence that provides insights about best practices in content moderation, and is ideally positioned to support the development of Codes of Conduct in the technology sector.
- European Commission aims for agreement with the Parliament by summer 2022, with legislation likely to come into force in 2023. Member states recently added an 18-month transition period so the rules will come into force in 2024 at the earliest.
- This briefing draws on discussion at the Internet Commission's EU Policy Roundtable in October 2021, which brought together leading Brussels policymakers to explore these new regulatory obligations and review the opportunities and challenges for corporate accountability[1].

(1) Objectives of the DSA

Tackling illegal content

Opacity and information asymmetry have made it difficult to fight illegal content online, including hate speech, CSAM and fraud. Regulators and law enforcement struggle to identify people, lack understanding of content moderation systems, and have incomplete evidence about the scale of illegal content. By obliging companies to undertake risk assessments and demonstrate the steps they are taking, the DSA aims to increase transparency and accountability in the field of content moderation.

Human rights in digital environments

At the same time as making sure illegal content is removed, a parallel objective is to ensure that legal content remains online. Overzealous notices and automatic takedowns of content has led to over blocking of content. In some cases, this has created a chilling effect on freedom of expression and access to information. It is important to ensure removals can be challenged and that complaints and redress mechanisms are fair. It may be necessary to incorporate a human rights impact assessment, including children's right to participate in an age-appropriate online environment[2].

Democratic oversight

The DSA aims to increase oversight of algorithms, including recommendation systems and malicious advertising practices that push extreme content and amplify misinformation. Auditing will play a key role in this, as will the continued evolution of co-regulatory mechanisms such as the EU Code of Practice on Disinformation, which was strengthened in 2021[3]. Such mechanisms may require greater scrutiny, with a wider range of actors from academia, civil society and media being invited to engage with them.

(2) Key challenges

Implementation and enforceability

Implementation issues have plagued GDPR enforcement where EU privacy complaints have stockpiled with the Irish Data Protection Commissioner in Dublin. Members States have therefore moved to agree oversight by the European Commission rather than the authorities in Ireland[4]. Even so, securing the right resources and access to expertise will be crucial for both regulators and in-house compliance teams. An independent enforcement authority might be necessary and it is not clear whether there is an existing body with the diverse range of competencies necessary to tackle the features of the DSA.

---

[1] See http://inetco.org/eurt21
[2] See Digital Futures Commission: https://bit.ly/3rIUWV7
[3] Code of Practice on Disinformation: https://bit.ly/3lLff0v

[4] Politico: https://politi.co/3D4g76h

Soft measures, hard law

To effectively change behaviour, and to ensure regulation is future proof, softer measures may need to be empowered. The DSA obliges very large platforms to develop codes of conduct, which would turn self-regulatory instruments into co-regulatory ones, but will this be enough? An open and inclusive multi-stakeholder approach may be needed to prevent the development of such codes and norms side-lining the democratic process. Alignment of codes of practice and evaluation frameworks across jurisdictions should enable platforms to comply with multiple regulatory requirements more easily. Voluntary schemes, initiatives, and reporting may be the most effective way to prevent companies starting an antisocial trajectory in the first place. Even so, fines could be necessary to encourage companies to uphold standards that they themselves have established.

Getting the risk-based approach right

The DSA requires very large online platforms to conduct risk assessments and demonstrate mitigation measures. Further debate is needed about how this assessment works and who decides which risks are to be assessed. Who sets the audit questions? Presumably not the organisations that are themselves being audited. Framed well, the DSA audits can be consistent with a risk-based approach, allowing regulators to focus on less developed platforms and amplifying successful and innovative practices in a "risk plus benefits" approach. But to assemble an auditor community that can hold the largest Internet companies to account, will require significant capacity building.

Our view

Authoritative and independent benchmarks needed

The identification and independent evaluation of trust and safety practices benefits from and supports the development of best practice benchmarks. Such benchmarks can also support the development of standards and provide direction to organisations that are seeking to improve.

Not only can such benchmarks inform practice, but they can evidence and support the development of the ethical business cultures that differentiate the world's best organisations. As part of a multi-stakeholder collaboration, the Internet Commission is developing a taxonomy of technical, AI and human practices that are used by digital organisations to achieve ethical outcomes and counter online harms.

Working with the Internet Commission enables organisations to better understand their existing culture and practices, compare notes with other organisations, and present innovations and challenges as part of an independent annual report.

The Internet Commission is a non-profit, independent from business and governments. It looks at digital organisations from the inside and seeks to inspire ethical business practice and enable smart regulation across jurisdictions.

As the Internet Commission plans a third reporting cycle, it invites collaboration with organisations that are preparing for Europe's new digital regulations.

For more information:		
Jonny Shipp	jonny.shipp@inetco.org	+32 488 67 48 78
Dr Ioanna Noula	ioanna.noula@inetco.org	+44 7847 095559
Juraj Kosturik	juraj.kosturik@inetco.org	+55 11 95080 6814
Baran Osmanoglu	baran.osmanoglu@inetco.org	+33 637 17 21 13
Patrick Grady	patrick.grady@inetco.org	+44 7879 880717

As a trusted broker within the new regulatory system, the Internet Commission aims to ask the right questions, provide reliable evidence, and help organisations to navigate different national and international requirements. It offers independent health checks, knowledge sharing and review services to organisations that lead in digital responsibility, and authoritative insight to regulators and other stakeholders. Its evaluation framework and process enable organisations to demonstrate progress in tackling problems such as illegal content, hate speech, cyberbullying and misinformation.

The Internet Commission is supported by visionary private and public institutions including Arm, Bates Wells, LSE, Sony and Wayra. Since 2018 it has engaged widely with Internet companies, content moderation practitioners, academic experts, NGOs and regulators.