GLOBAL PARTNERS DIGITAL

Data Access for Researchers within Digital Platforms

Unpacking the human rights implications, practical opportunities, and challenges for the Global Majority.

February 2026

Written by
Agustina Del Campo

Acknowledgements

This report was authored by Agustina Del Campo on behalf of Global Partners Digital, with input from Maria Paz Canales (Head of Policy and Advocacy, Global Partners Digital).

Agustina Del Campo is a law professor and directs the Center for Studies on Freedom of Expression (CELE), affiliated with Universidad de Palermo. This article summarizes the work she directed at CELE during the past three years on access to data for research.
The author would like to thank Nicolas Zara and Paulina Gutierrez for their feedback and contributions.

Content

01 Overview

This policy brief examines the regulation established by **Article 40 of the European Union's Digital Services Act (DSA)**, providing researchers with access to platform data, and on the **2025 Delegated Act** that sets out the practical modalities. It analyses how this new regime is being developed and implemented, the challenges it presents, and its **broader implications particularly for researchers and civil society organisations in the Global Majority.**

The DSA represents the most ambitious attempt to date to address long-standing information asymmetries between large online platforms, regulators, and society. By granting vetted researchers access to platform data, the DSA seeks to enable independent scrutiny of systemic risks, such as disinformation, content moderation practices, and impacts on fundamental rights and to strengthen regulatory oversight and enforcement. The Delegated Act is central to this effort, as it defines who qualifies as a researcher, how data requests are made, and how platforms must respond.

The **policy brief identifies practical, legal, and conceptual challenges that may limit Article 40's effectiveness.** These include:

- Complex and slow vetting and request mechanisms
- Restrictive interpretations of who qualifies as a researcher
- High specificity requirements for data requests, despite researchers' limited visibility into platform systems
- Over-reliance on quantitative data, which can produce decontextualized or biased analyses
- Potential unintended impacts of mandated transparency on freedom of expression.
- Conflation of different content categories (illegal versus harmful-but-legal), which risks misleading conclusions

Looking beyond Europe

A central contribution of the policy brief is to bring a Global Majority perspective. Debates and implementation processes around Article 40 have been overwhelmingly shaped by European and US actors, with limited engagement from researchers and civil society in the Global Majority. **The absence of Global Majority perspectives risks reinforcing biased understandings of platform harms and overlooking issues such as state-led censorship, propaganda, and surveillance.**

The policy brief explores how Article 40 may influence future regulatory models beyond Europe, both positively and negatively. While the DSA offers a unique and potentially powerful template for data access and platform accountability, it also carries risks of misuse, political capture, and over-implementation if transplanted without adequate safeguards.

Drawing particularly on Latin American experiences, the paper outlines the need for more inclusive research networks, clearer substantive standards, stronger access to state-held information, and greater attention to global and comparative contexts.

02 Introduction

In July 2025, the European Commission (EC) adopted the Delegated Act on data access for researchers under the Digital Services Act (DSA). The Act was adopted after at least two years of preliminary discussions over the role of research in the implementation of the DSA, Europe's cutting-edge regulation for online platforms and search engines. In the announcement, the EC explains that "This Delegated Act complements the DSA rules that oblige VLOPs [Very Large Online Platforms] and VLOSE [Very Large Online Search Engines] to grant access to researchers to publicly available data on their platforms. This will allow research on the systemic risks and on the mitigation measures in the European Union, overall contributing to the monitoring of the online environment and, therefore, to a safer online world."[1]

The Delegated Act was expected to clarify certain aspects of Article 40 (4) of the DSA, which grants access to data for vetted researchers, as opposed to publicly available data that companies are expected to provide regularly under Article 40 (12) of the DSA.[2]

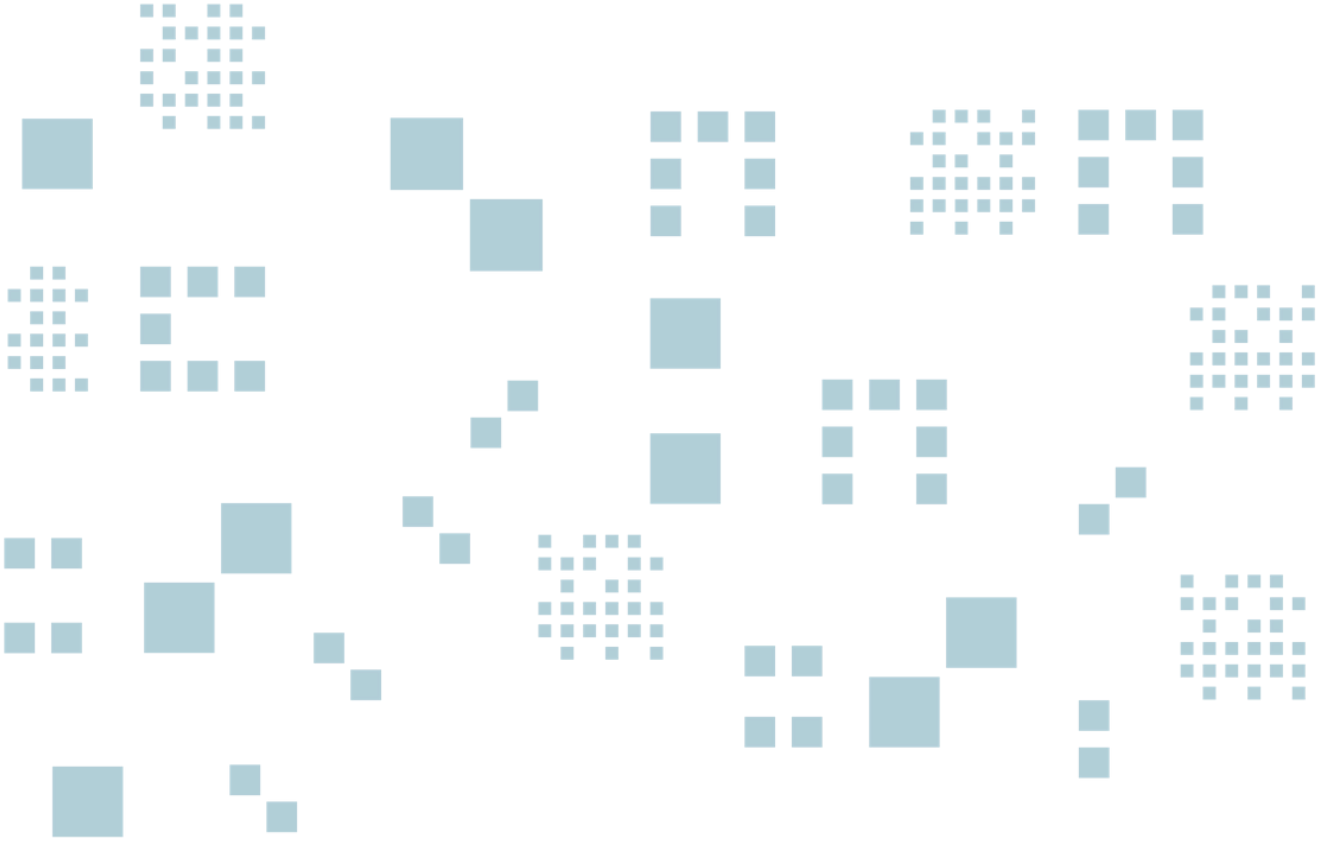
> *"Access to data for researchers has been a heated topic within academia and civil society organisations (CSOs) in Europe and the United States since the drafting of the DSA. The issue has, however, been understudied, underestimated and mostly ignored within academia and CSOs in the Global South. This is due to a number of factors including:*

In the US and Europe there is poor understanding of the distinct needs and contexts in the Global South leading to generalisations and partial, biased views of the impacts of technology on society, as well as a poor predisposition to hear best practices and lessons learned from Global South or Majority World countries. Furthermore, debates in this area show limited openness to non-European and external perspectives.

These factors undermine an otherwise interesting and one-of-a-kind legislation like the DSA and limit the possibility of making good use of it elsewhere. Moreover, they impact the ability of Europe itself to foresee and guard against unintended consequences of the implementation and development of this regulation, even within their own region.

This paper describes the current state of affairs in the development, understanding, and application of Article 40 of the DSA about access to data for researchers and its role within platform regulation more broadly with a Global South lens.

It provides a brief recount of the history and the context in which this provision was developed and is now being implemented; summarises some of the most salient challenges and opportunities for this regulation to be effective; and identifies a few, non-exhaustive, potential recommendations for Global South communities to engage with the topic going forward, drawing mainly from Latin American experience.

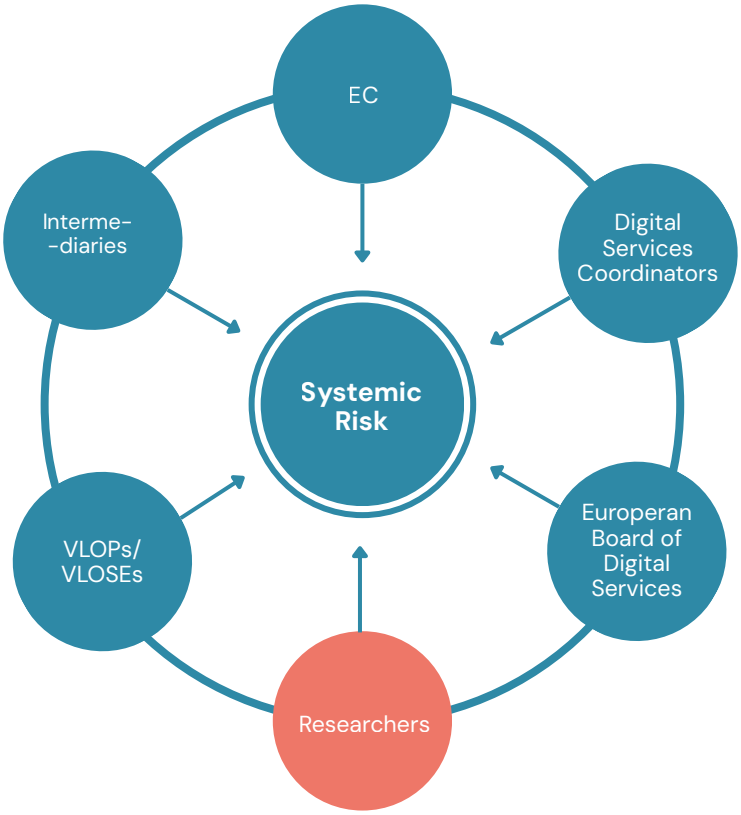


03 The DSA and the co-regulatory approach

The DSA is a complex system of rules and obligations ranging from primary norms for digital intermediaries to a multi-layered structure of oversight and enforcement of such norms. The overall goal of the DSA is to hold social media and search engines (mainly, though not exclusively) accountable for their actions and to protect the rights of end-users.

The DSA's starting point is an information asymmetry between society and the regulator and companies, which can only be salvaged through a complex mix and match of policies and regulations[3]: transparency reports, requests for information, meaningful engagement with civil society, independent audits, investigative powers, and data access for regulators and researchers.[4]

Within such a structure, researchers are called upon to collaborate with the EC, the Digital Services Coordinators (local authorities designed by the DSA and intended to be created by each national state), the European Board of Digital Services, VLOPs/VLOSEs, the rest of the intermediaries, and society at large to identify and understand evolving systemic risks created or enlarged by platforms and mitigation measures adopted by companies in response.[5]



> *Of all the stakeholders that partake in the DSA ecosystem, only researchers are entrusted with the responsibility of carrying out extensive research on this still obscure concept of systemic risks. Therefore, the DSA cannot function as intended if researchers and CSOs cannot effectively engage with data.*

The more thorough the research on systemic risks and mitigation measures, the greater the tools that the DSA enforcement mechanisms will have to understand and hold platforms accountable. The Delegated Act on data access for researchers is key as it provides researchers, platforms, and regulators alike with detailed procedural rules on how data must be requested and accessed for research purposes under Article 40 (4) of the DSA. The EC argues: "The impact of this provision is twofold: researchers who fulfil the conditions set out in the provision will benefit from access to previously undisclosed or under-disclosed data, opening up new avenues for research and increasing the potential of generating knowledge for the benefit of all. At the same time, these insights will contribute to the work of competent authorities in carrying out their supervision and enforcement tasks, including the assessment of the steps taken by providers of very large online platforms and of very large online search engines to fulfil their obligations under Regulation (EU) 2022/2065." [6]

Access to data for research is only a part of the transparency obligations that the DSA creates as it also seeks to actively contribute to the effective enforcement of the law.

"Researchers' access to data under Article 40 of the DSA will be part of a broader toolbox of transparency introduced by the DSA[7] which includes the DSA Transparency Database[8] and the DSA transparency reports,[9] among others."[10]

The DSA creates obligations for platforms to assess and identify systemic risks and report back to the EC on them, including mitigation measures regarding the points explicitly developed under Article 34.

Access to data for researchers is expected to fulfil three distinct roles:

01

Independently identify and assess other risks potentially not included by companies in their reports or developing over time;

02

Further refine the identification, advance mechanisms, and evaluate mitigation measures;

03

Contribute to verifying the information submitted by the companies in their reports.

Crucially, the DSA brought about different transparency and access to data obligations for companies in Article 40, although the scope of such obligations is narrowed and excludes any obligations to report state conduct or state-led company action.

Kinds of Reasearch under DSA Article 40

There are mainly two types of access to data established in Article 40:

- Article 40 (4) mandates access to private information held by companies by vetted researchers;
- Article 40 (12) grants access to publicly available data.

Professor Daphne Keller offers a clear explanation.[11] She distinguishes three kinds of research that may be conducted by three different kinds of researchers under the DSA Article 40 model.

ARTICLE 40 (4)

Vetted researchers under Article 40 (4), which was the most debated rule on transparency for research purposes so far. These researchers may apply to access non-publicly available data. They need to be vetted by the Digital Services Coordinators. We will refer to vetting mechanisms later.

ARTICLE 40 (12)

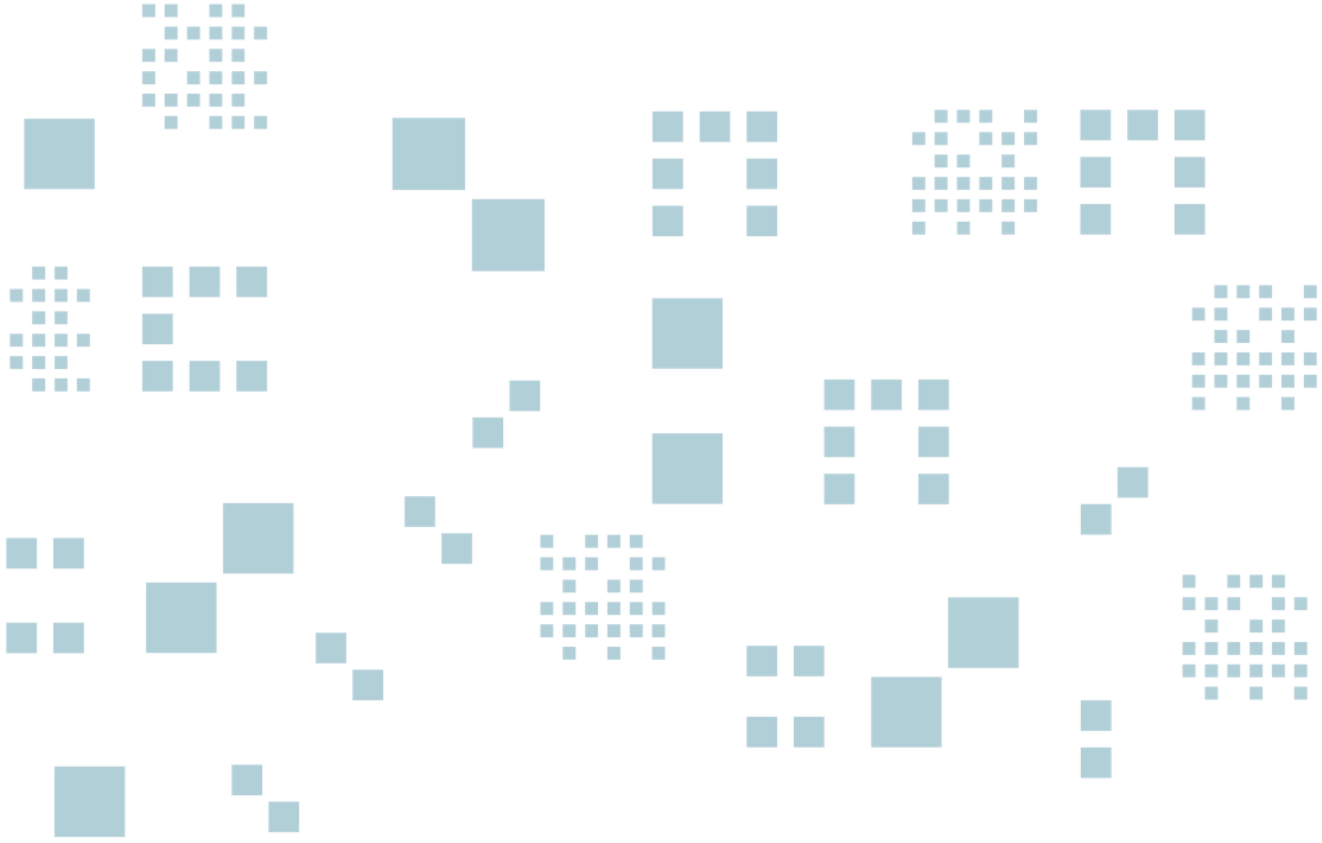
The second type of research is using publicly available information, under DSA Article 40 (12). No specific requirements apply to these researchers to request or retrieve such data.

NON-DSA RESEARCH

The third kind is non-DSA-related research that may complement or be affected by the rules developed for DSA research. For example, there is great expectation as to how the EC and tribunals across Europe interpret the meaning of "publicly accessible information" under Article 40 (12). The wording has been understood to promote scraping, data mining, and the development and deployment of APIs by some. These have been questioned by companies in the past, and they lack a legal framework.

The EU could be the first region to adopt standards regarding these common practices that so far have created legal risks for scholars who have, in many cases, been threatened or even sued by companies.[12]

> *Overall, the landscape for researchers has broadened significantly, and that includes both European and non-European researchers, particularly through the open, public data that the DSA gathers and mandates companies to disclose and organise. Whether that access is wider or narrower depends on the interpretation that the EC and courts make of the rather complex and vague terms that the law and the Delegated Act adopted.*



04 How did we get here? A little history and context

Although the DSA is the first regulation of its kind to adopt a collaborative implementation framework and explicitly grant researchers access to company held data, the imbalance between privately held and publicly available information about the functioning and potential impacts of ICTs is not a new concern.

Pre-2010
Intermediaries

Intermediaries and Liability

Unlike those in other industries, internet companies have been defined early on as "intermediaries" and regulated in the United States[13] and Europe.[14] The result of which was to shield their liability for third-party-posted content and for content curation and moderation practices. Although these were simple and somewhat limited originally, developments in the tech sector have allowed companies to curate, summarise, recommend, highlight, and make content invisible in ways that were not imagined when immunity from liability was established as the rule. Partly as a result of this existing regulation, the development and impacts of these curation technologies were, for the most part, not audited or supervised by those ordinarily in charge of holding legal and physical persons accountable to the common good (judiciary/congress).

2008
GNI

Global Network Initiative (GNI)

The Global Network Initiative (GNI)[15] had been created to foster responsibility among internet companies to protect users' rights from state abuses and from abusive states. As part of the initiative, member companies conduct assessments of their practices and policies in place to respond to state requests while maintaining their human rights commitments. Those assessment reports focused exclusively on requests for access to data and requests for filtering and takedowns. Efforts to sustain the GNI are still worthy, as recent policy and regulation do little to provide transparency or access to data regarding the state's conduct vis-à-vis internet companies. Maintaining and supporting self-reporting mechanisms and initiatives like the GNI are, therefore, key to comprehensively analysing and understanding the online information ecosystem.

2010
Transparency Reports

First Transparency Reports

Companies started publishing transparency reports in 2010. Until 2010, the workings of internet companies and their treatment of third-party-posted content went unpublished and remained outside of public or government scrutiny.

Still, the reports published in 2010 were the product of concrete concerns about the practices and pressures that some states were trying to exert on internet companies to access individual users' data and filter individual users' content.

2011
UN Guiding Principles

UN Guiding Principles

In 2011, the United Nations adopted the UN Guiding Principles on Business and Human Rights (UNGPs),[16] drafted by John Ruggie and endorsed by the UN Human Rights Council. The Principles are not binding for companies, but give strong recommendations for them to identify, assess, and mitigate human rights risks related to their operations. One major human rights risk at the time was the pressure from states to utilise global internet companies as a major surveillance and persecution tool, as was demonstrated by the case of Yahoo in 2005.[17] Yahoo provided data to the Chinese government that led to the imprisonment of journalist Shi Tao in China, among other human rights defenders.

Yahoo's admission to providing the data to the government led to a lawsuit and a congressional hearing in the United States in the late 2000s, and the case served as early proof of the need to hold companies to human rights standards to avoid their services being weaponised by different governments to suppress freedom of expression, privacy, or other political freedoms. The reports, which started being published in 2010, contained information disclosed by companies about state requests for individual users' data and requests for filtering and blocking content.

2015
Manila Principles

Manila Principles and the Push for Transparency

After the Snowden revelations (2013),[18] the Manila Principles (2015),[19] led by civil society organisations, pushed the agenda for transparency further to include companies' decisions over the treatment of data and content. They included the following recommendations for companies (besides others that were directed strictly to states):

1C. Intermediaries should publish their content restriction policies online, in clear language and accessible formats and updated as they evolve, and notify users of changes when applicable.

6E. Intermediaries should publish transparency reports that provide specific information about all content restrictions taken by the intermediary, including actions taken on government requests, court orders, private complaint requests and enforcement of content restriction policies.

6F. Where content has been restricted on a product or service of the intermediary that allows it to display a notice when an attempt to access that content is made, the intermediary must display a clear notice that explains what content has been restricted and the reason for doing it.

6H. Intermediary liability frameworks and legislation should require regular, systemic review of rules and guidelines to ensure that they are up to date, effective and not overly burdensome. Such periodic review should incorporate mechanisms for collection of evidence about their implementation and impact, and also make provisions for an independent review of their costs, demonstrable benefits and impact on human rights.

2016
Cambridge Analytica

The Catalyst for Regulation

The Cambridge Analytica scandal,[20] Brexit,[21] the election of Donald Trump[22] as President of the United States, and the Colombian Plebiscite for Peace in 2016 drew attention to content curation, content targeting, profiling, advertising, and the use of data in conjunction with propaganda.

Companies then limited access to their APIs[23] to prevent new "Cambridge Analytica-like" scandals and, with them, arguably, the only avenue to access data in real time from them. The scandals raised awareness and concerns about content policies and practices within companies.

2020
Covid - 19

The Evolution of Transparency

The rise of the disinformation scare and particularly the 2020 COVID-19 pandemic generated new demands for greater accountability as companies were placed under increasing pressure to disclose more information about their conduct, their practices, and their impact. Some companies started to include some of their content moderation practices and statistics as part of their transparency reports. However, the effort wasn't sustained or consistent across the industry until the adoption of the DSA and the first rounds of mandated transparency reports. Still, efforts remain inconsistent with regard to regions other than Europe.

Historically, these reports have varied significantly in both the type and scope of information provided across regions, making them hard to compare and, significantly, more complete in some jurisdictions than in others. Most reporting efforts have also remained globally aggregated, with Europe now standing as a notable exception, highlighting the critical role that a binding legal framework can play.

05 Challenges under the DSA Article 40

> *The DSA is the most comprehensive legislative framework to date for granting access to data held by internet companies, with the aim of improving understanding of the societal impacts of online platforms.*

With the caveats and limitations described above (namely, that it only addresses some intermediaries but not all, and that the transparency obligations are meant vis-à-vis company conduct but exclude state-led company conduct), Article 40 provides some light in an otherwise very dark tunnel that has been the private management of online content. Still, broadly speaking, there are pervasive technical and substantive challenges to the enforcement of data access for researchers that require attention for the successful implementation of the law. Furthermore, the global perspective of inter-jurisdictional companies is still missing.

In addition, there are issues that impact the whole global information ecosystem and its governance that may also be affected by the provisions of the DSA in Article 40 and how those are interpreted and implemented. Challenges with curation and moderation reports in the past – and pervasive within the DSA framework – lack uniform usage of terms, clarity in definitions, and abound in decontextualised information and much quantitative data that cannot be qualitatively analysed or understood to mean much.

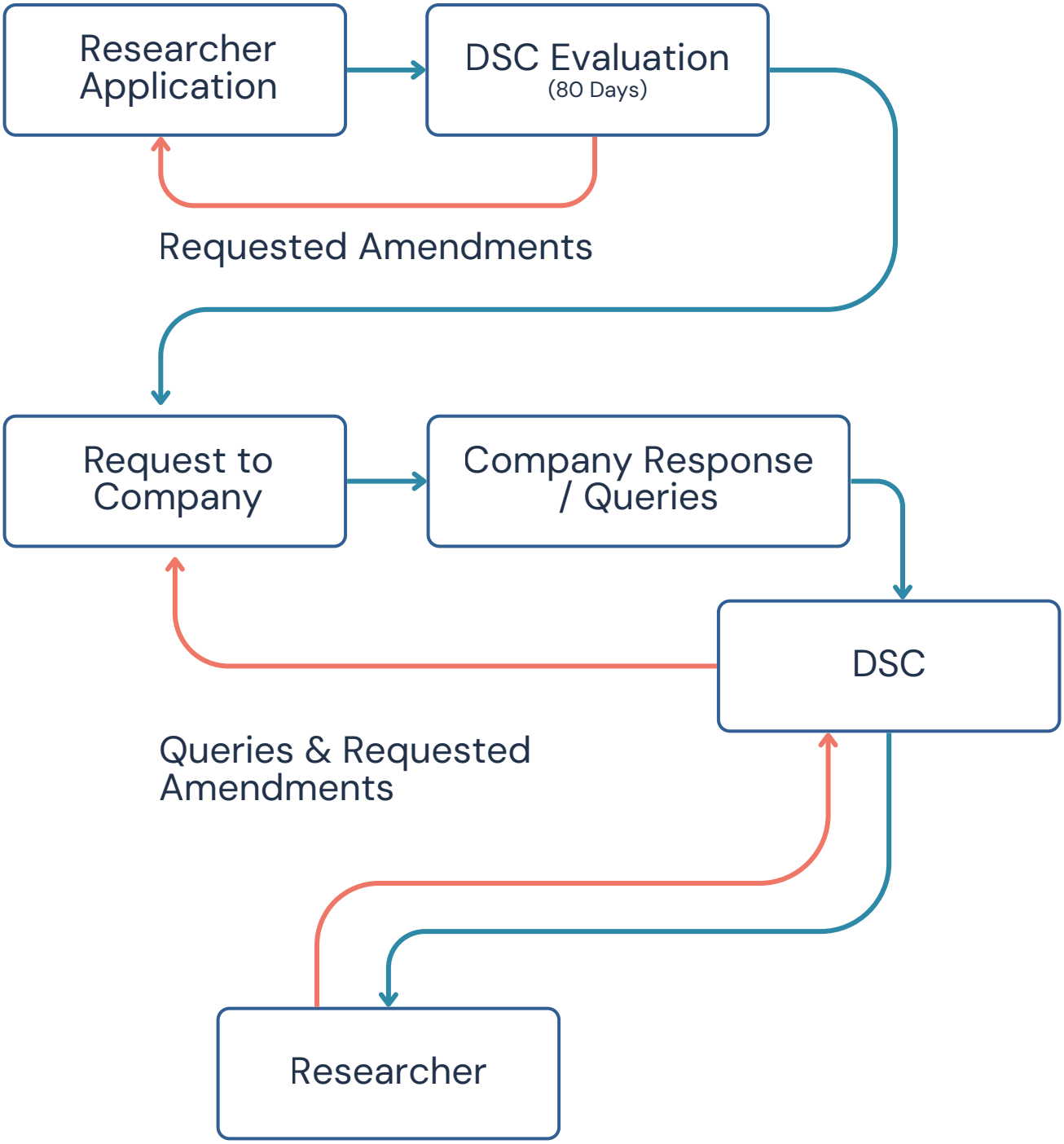
Data access for researchers will, hopefully, eventually help strengthen our understanding of these ecosystems globally.

Complex request mechanisms

Article 40 of the DSA puts Digital Services Coordinators, appointed by member states, front and centre of this mechanism. These bodies will be particularly important for data access for researchers, as they will be vetting researchers and receiving research applications. The system is complex: researchers file an application to the Digital Services Coordinator indicating the compliance of some formal requirements – affiliation with a research institution or CSO dedicated to research, commitment to publish free of charge, independence, and disclosure of funding – and detailing the data that they are seeking, the purpose for which they are seeking it (which needs to fit Articles 34 and 35 of the DSA), the inability to access such data through other means, the way they will handle and protect the data per other European laws such as GDPR, the format in which they seek the data and the timeframe for their research, among others.

Upon an evaluation from the DSC of the application, which may take up to 80 business days, the DSC will decide and notify the researcher if they will pursue a formal request for access to data with the company or whether they need additional information in the form of an amendment.

The company will receive the request from the DSC and respond to the DSC stating whether the information exists, whether it is available, whether the request is specific enough, and whether the means for accessing the data are agreeable to them – the DSA and the Delegated Act leave a wide space for discussion over the means to provide access to data. If the company has queries about the request, they will notify the DSC, and the DSC will then notify the researcher. Overall, the procedure is resource-intensive and procedurally complex, reflecting an approach intended to limit data access to narrowly defined and exceptional cases.



Specificity and exceptionality of access to data for researchers under Article 40(4)

At the stage of developing concrete and proportionate requests for data access, states and civil society organisations face a number of barriers, most notably significant asymmetries in technical knowledge between platforms and public or civil society actors. The risks of overreaching need to be balanced against the need to facilitate access in good faith. So far, experiences already cited suggest that some companies have been strict and literal in their understandings of data requests, making it hard and cumbersome for researchers to access the data they need to produce the research they intend.

The Delegated Act mandates that companies keep repositories of data available for researchers, which are intended to be kept updated and renewed. This may contribute to solving some of the issues. Under the DSA, researchers seeking access to data under Article 40(4) must also demonstrate that the requested information cannot be obtained from other sources. For example, the EC has encouraged civil society organisations and researchers to first make use of open-access and other "otherwise accessible" information before submitting data access requests. This approach places the burden - and associated costs - of demonstrating necessity primarily on the applicant.

Who is a researcher?

As per active legitimacy to request information in accordance with the Delegated Act, researchers applying for access to data need to be affiliated with a research institution or organisation. The organisation itself cannot request access to data, but individual researchers can. In the logic of NGO's and thinktanks, this creates hurdles that may be hard to overcome. For one, the ongoing research project is not always necessarily academic or attached to a single research team, but rather to the goals of an entire organisation.

How specific should the application be?

The level of specificity required for applications also poses challenges. The Delegated Act requires that requests under Article 40 (4) be specific and confined. In different interactions between academics and representatives from the EC, the EC indicated that the scope of the requests needs to be proportional and adequate for the research objectives.

Data requests must go through the DSC of the member state of the applicant or directly through the DSC of the establishment of the data provider (the one in the jurisdiction where the company is registered). Existing asymmetries in understanding and knowledge of private tools, systems, and data availability limit researchers' ability to formulate specific requests and may ultimately undermine research efforts, particularly where researchers or institutions are required to submit multiple, increasingly complex data access requests to pursue the same research objective. This is equivalent to going to the library to research a topic and requiring the researcher to identify, a priori, exactly all the books by title and author that they will need to develop their research. Furthermore, the timeframes that companies manage in providing access to data are indefinite, and the endeavour becomes a significant investment of time and resources in an otherwise poorly funded, multitasking pool of organisations.

Data sets available and the purpose of data collection

On the substance, key among the recommendations CELE made in the consultation processes that the EC launched in 2023 and 2024 regarding data access for researchers, was the importance of highlighting qualitative data besides quantitative data. The provisions around transparency within Article 40 included transparency reports, and the transparency focus mostly on quantitative data.[24] While during the consultations this was a mere theoretical assumption of what would happen, the publication of the first round of the VLOPSEs' risk assessment and mitigation reports in late 2024 and early 2025 proved the need for qualitative and contextualised data from companies in order to make sense of what companies have reported. CELE, for example, highlighted the need for the commission to define key concepts, like "cases". A "case" for the purposes of counting and reporting should mean the same thing within every platform. As academics and civil society organisations have pointed out in the past, a "case" or a piece of content can be defined differently by different companies (i.e. the same content reported across two platforms owned by the same company; or a single report including more than one individual piece of content). However, the Delegated Act does little to clarify the scope of qualitative data access for researchers. Moreover, many of the submissions cited (or highlighted) by the EC as informing its approach appear to reinforce a focus on expanding quantitative data, rather than addressing the need for clearer definitions and more contextualised, qualitative information.

Research topics allowed are narrow, vague, and in many ways mischaracterised

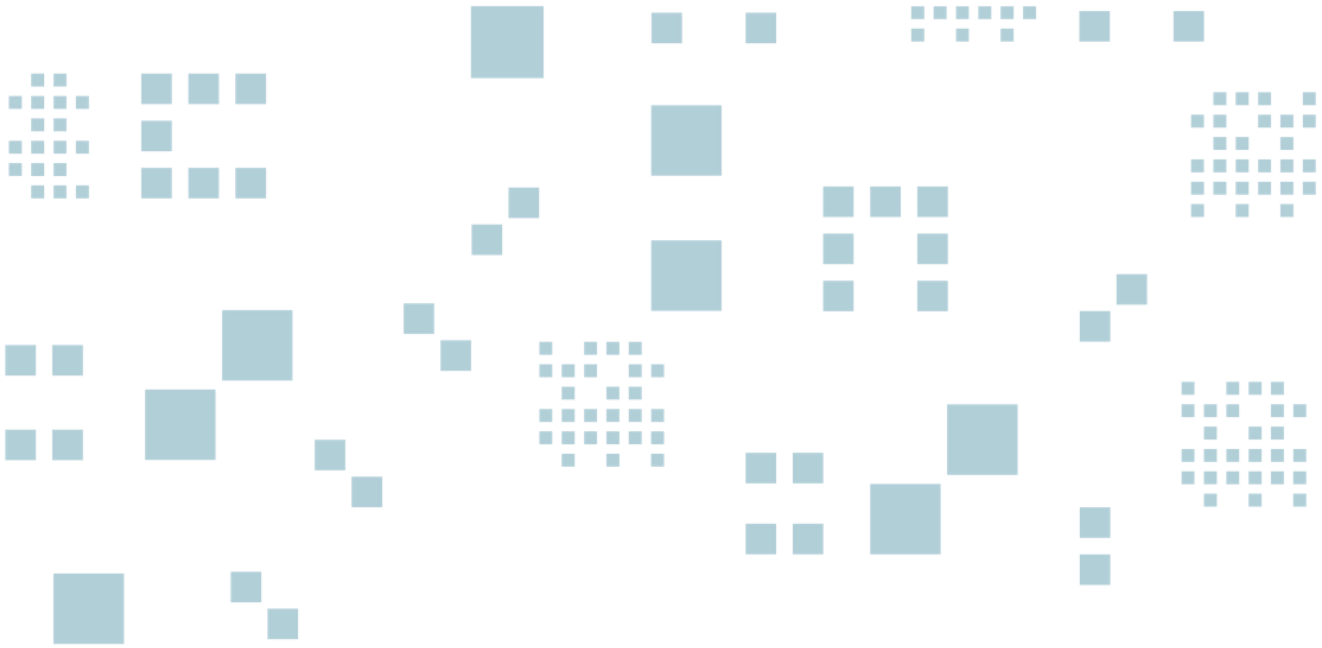
Finally, challenges arising from the DSA carry over to the data access for research debate. The conflation of illegal and (legal-but-) problematic speech in certain provisions of Article 34, and in the design of the EC's Transparency Database, raises concerns from a human rights and freedom of expression perspective. In order to assess risks or impacts, researchers require granular data and a clear understanding of how companies interpret these phenomena and the reasons for their actions. Content that is acted upon because it is illegal differs from content acted upon only because it is harmful. The underlying reasons for a company's actions may vary, and therefore, the associated responsibilities and implications should also differ. Companies should clearly distinguish between actions taken in compliance with state mandates and those undertaken as part of self-regulation.

The EC has not only failed to clarify this aspect vis-à-vis research or the data that companies should provide researchers to address these challenges, but has also added insult to injury, conflating categories that are incomparable and may promote biased research. The conflation of harmful-but-legal and illegal categories for reporting purposes, when addressed together in a quantitative analysis, may be misleading. For instance, the use of "disinformation" or – in proper DSA terms – "content that has negative effects on civic discourse"[25] can be misleading as it encompasses both legal and illegal content and overlooks the relevant differences between them. Considering that research is intended to inform the implementation of the DSA at different stages, and especially taking into account that the corpus of data to which researchers can access is intended to shed light on systemic risks under Articles 34 and 35, the use of confusing categories may foster wrong, illegitimate, or misguided mitigation measures and expectations for compliance.

Mandated transparency affects Freedom of Expression and may create new threats through bias and overimplementation

Transparency and access to information, like those fostered by the DSA, are key to protecting and promoting freedom of expression. International and regional freedom of expression standards[26] require that **mandated transparency** be necessary and proportionate, and when mandating information or transparency, the EC should ensure that the information is requested objectively towards the legitimate ends and purposes described in the enabling law.
When the EC publishes information or obliges platforms to make data available, it should provide clear guidance on the methodology used, the questions the data is meant to address, and the limitations of the information. Such clarity is essential to ensure transparency is useful for researchers and policymakers. To illustrate this further, an example may help.

Historically, the voluntary agreements made by companies regarding disinformation or hate speech in the EU have been evaluated against mostly quantitative data provided by the companies: i.e., the number of pieces of content flagged, the number of pieces of content detected by companies, and the number of pieces of content taken down. While quantitative data illustrate the volume of the problem and the solutions implemented, they provide limited insight into the proportionality or legality of these measures. Upon analysing these data sets, the EC, as well as other encumbered actors, should be made aware of the limitations of such data, the way those quantitative figures were calculated, the baselines, and so on. Further efforts should be made to evaluate the accuracy and effectiveness for the purposes the reports intend to serve. Otherwise, the data may be misleading, particularly if it relies on partial or unintentionally biased self-assessments, transparency reports, or incomplete data access for research. This could lead to interpretations and enforcement actions that unnecessarily or disproportionately restrict speech for all platform users, in ways that are incompatible with international standards on freedom of expression and access to information.

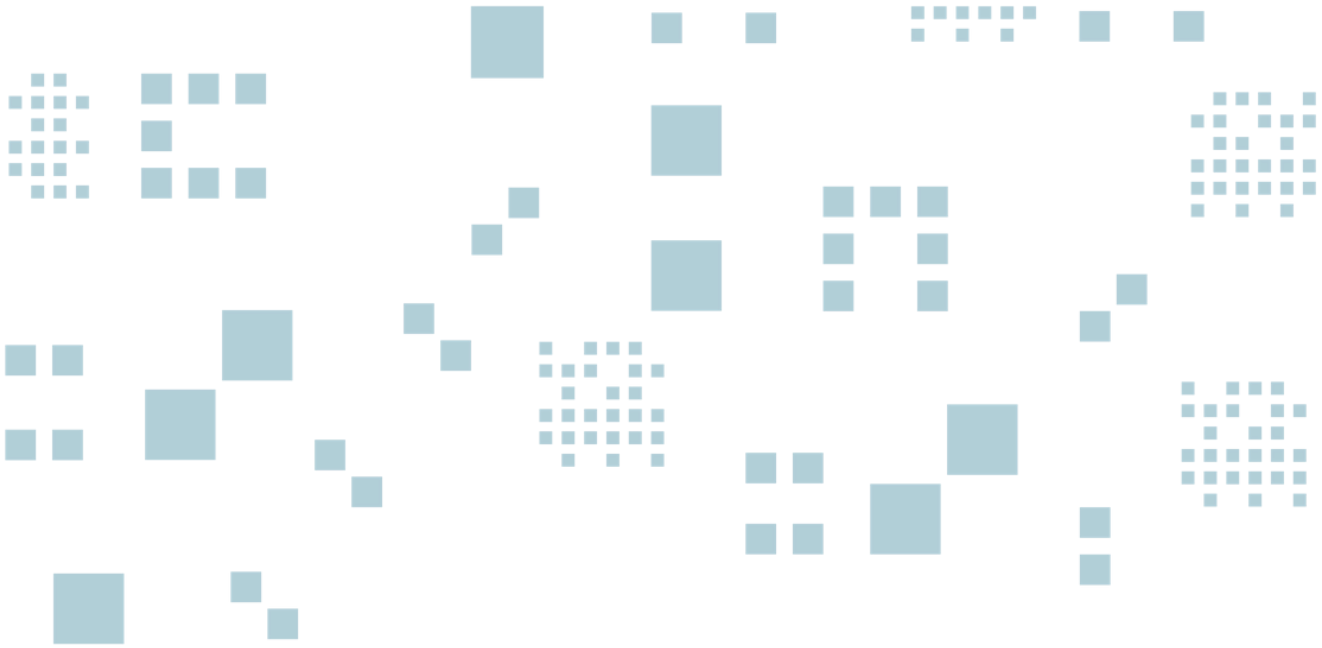


Access to state-held information as the missing link

Furthermore, any mandated transparency should be accompanied by strong access to publicly held information. ICT companies, like other private actors, are influenced and respond to incentives created by other stakeholders, the state being an important one. When access to data for research is intended to inform regulatory implementation in a law that is so broad that it can very well be compared to the US's "we'll know it when we see it" obscenity standard,[27] research needs to be carefully independent, narrowly tailored, and scientifically sound. Otherwise, we risk states promoting and financing research to arrive at foregone conclusions in the name of public interest regulation. An example may help clarify the point: research may yield different results depending on the question and the methodology we use to develop it.

One of the main critiques among academics and CSOs on the oversight mechanisms of the Codes of Conduct on Disinformation or Hate Speech, for example, was that the methodology for reporting allowed for decontextualised, quantitative information rather than qualitative information. Therefore, many reports emphasised the amount of content taken down without any context or any framing for the analysis conducted by the company to do so. These metrics allowed companies to say they were mitigating and taking active measures to fight disinformation, and states to say that the legislation was successful in fighting against fake news.

Neither of those is entirely proven by the information contained in the company reports under the Codes of Conduct or the evaluation that the EU commissioned on the performance of those instruments. States and governments must therefore be transparent about the financing, fostering and intended purpose of any data requested for research purposes, and for any mandated transparency expected from companies.



Limited Geographic Scope

With global tech, risks and impacts cross borders. This is true in two different ways. First, risks may originate in different jurisdictions and still impact Europe. Second, the understanding of risks in global tech requires global input and global data; otherwise, any conclusions drawn from it may be biased or partial, to the detriment of successfully addressing the challenges brought about by global platforms. The risks for democracy that social media creates may benefit from comparative experience in different jurisdictions. For example, if researchers were trying to identify risks before the Cambridge Analytica scandal, they would have had trouble foreseeing the case solely with European data.

The same goes for the 2016 series of scandals that brought about changes, for instance, to the GDPR. Phenomena across the internet have multijurisdictional interpretations, applications, and impacts. Understanding why a certain use or service may be a problem in Europe but not in South Africa can provide valuable input into identifying and assessing appropriate and effective mitigation measures. What makes a service prone to abuse in Myanmar but not in Venezuela can contribute more to our understanding of the responsibility of platforms and, therefore, help build our expectations with regard to companies' conduct.

Finally, global tech provides for global information ecosystems. Information ecosystems have been studied for decades, and those who study communication and history know that there are severe inequalities and asymmetries in the study of information ecosystems. Data access for researchers may contribute to bridging the existing gap in information ecosystems or may feed and strengthen the divide. Despite the potential initially envisioned by non-European researchers, the scope of the DSA Article 40 and the Delegated Act does little to enable the active engagement of non-European research institutions. They fail to acknowledge the existing gap or the existing asymmetry in the ability to conduct research in different areas and jurisdictions, which, given the global nature of the technologies in question, may negatively impact the implementation of the DSA in Europe.[28]

06 How does Article 40, or this debate, impact the Global South? Using the DSA and modelling laws after it

> “The DSA provides a unique and incomparable framework for data access for researchers. The only one so far, in fact. The uniqueness of this provision and access is, without a doubt, good news for Europeans and non-Europeans alike.

For Europeans, the advantages are clearer as they are the intended beneficiaries of this legislation. They will also have a first-mover advantage in testing and framing the interpretation of these provisions, and even if the tool is not as efficient, it will certainly provide a better understanding of platforms than the one they have now.

For Global South researchers and policy makers, there are direct and indirect opportunities that arise from the legislation and the Delegated Act itself.

For one, after much debate, the Delegated Act defines vetted research as a person affiliated with a research institution or a CSO dedicated to public interest research. The EC adopted a broad definition of researcher, thus facilitating more access by a wider variety of stakeholders to data access requests. Moreover, the Delegated Act does not expressly limit vetted researchers to European researchers. It has therefore been interpreted by academics as a carte blanche for foreign researchers to access data through this mechanism.[29]

Still, there are concrete challenges that may need additional framing and concerted efforts from researchers, both local and foreign, to contribute to a sustainable, comprehensive, and efficient regime capable of living up to the expectations that the DSA creates for it.

General challenges have already been discussed in the previous section. However, there are additional challenges that apply to Global South communities specifically that merit attention.

Lack of, or poor, meaningful engagement with the drafting, implementation and interpretation process in Europe

The discussions and negotiations over the implementation of Article 40 (4) were mainly driven by European and US researchers, research institutions, and civil society organisations. CELE and InternetLab were among the few organisations beyond European and US organisations that produced feedback[30] towards it. Reasons behind the lack of engagement may be varied and are absolutely valid. They include different regional priorities, lack of human resources, lack of funding or expertise in European law, geographical distance, and the reluctance of European civil society, academics, and institutions to take foreign feedback into account. During the process of drafting the Data Access for Researchers Delegated Act, the EC conducted meetings with US institutions in Palo Alto, California; they consulted with researchers, mostly by invitation, and put the resources of their tech embassy in California towards engaging US academics, scholars, and advocates in the conversation.

There are multiple reasons why this may have been prioritised, including a well-established and well-funded research system within the US, reputational value among their institutions, closeness with the main platforms that Europe was intending to regulate, expertise that, for the most part, is missing in other jurisdictions, and a track record of private agreements between reputable research institutions and companies to disclose data and commission research, among many others.

Still, the absence of Global South voices in the negotiations will impact the use that organisations in these regions can make of it and deprive the law of the benefits of enabling a global understanding of these technologies and businesses, to the detriment of its enforcement. It will also impact the ability of European civil society and researchers to foresee the consequences of this lack of participation, including a platform research landscape that addresses and projects solely European perceptions and values rather than broader concerns over platform governance that are viewed, understood, and treated differently in other regions. Both Latin American and African civil society organisations and academics[31] have, for example, highlighted the role of governments in both regions in producing and disseminating harmful content themselves.

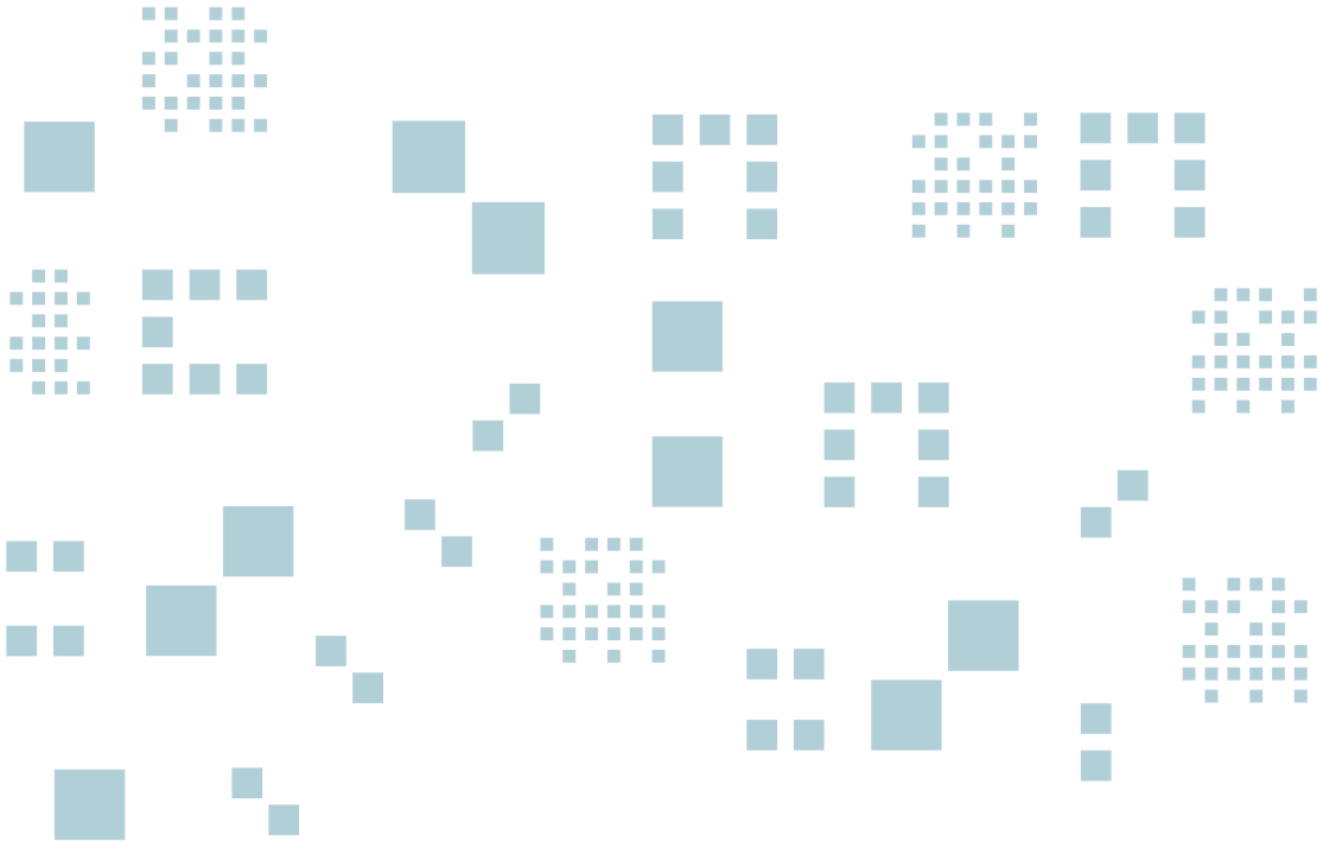
Complexity of the system for foreign use and replication

Although the DSA had sparked and engaged researchers in different countries and regions, current ongoing initiatives after the DSA Delegated Act have confirmed concerns regarding the difficulties that researchers outside Europe will probably face in accessing data. Among those, the complexities of the mechanisms to access data require extended expertise, shared knowledge, and an overall network of people and institutions working to implement it. Furthermore, the application process relies on DSCs, adding a new layer of bureaucracy. Concerns have already been raised about the lack of expertise and resources to put these structures to work in some countries in Europe, or the technical abilities that those bodies will need to evaluate research applications fairly. The EC is working on shared resources, and CSOs are getting organised across countries as well.

Research networks are so far mostly European

European research institutions and researchers are already developing networks to strengthen their requests to access data from companies, identifying and mapping the research landscape, providing networking opportunities among researchers, and sponsoring seminars and debates on how to monitor compliance with the DSA Article 40 provisions. For example, the DSA40 Data Access Collaboratory,[32] an initiative intended to create a network of researchers and provide support for them while monitoring the implementation of the law. This initiative seeks to strengthen the community of researchers, create opportunities for multidisciplinary research, foster co-authorship in access requests, and monitor the implementation of DSA Article 40. Although it acknowledges an intention to foster international and inter-regional collaboration, so far, the website only lists European researchers as part of the consortium.

The DSA Observatory at the University of Amsterdam[33] has also been an active and important actor in fostering a better understanding of the DSA for researchers and organisations in Europe and in shaping the provisions that the DSA is now implementing. Their annual training programme on the DSA[34] brings together public officials from European countries called to implement the DSA locally, junior academics entering the field, advocates, and practitioners. So has Martin Husovec's course at LSE[35]. However, currently, they have had limited space and provided limited accessibility for Global Majority researchers and CSOs.



Data access, handling, and storage standards

The DSA is part of the broader system of European law, which includes the European Union Treaty and other European treaties, statutes, and institutions that dialogue with each other and that need to be understood to enter debates over the implementation of this particular law. In fact, in our digital field, conservatively defined, the DSA is complemented by at least the GDPR, the AI Act, the Digital Markets Act, the Voluntary Codes of Conduct drafted by the EU for internet companies in relation to disinformation and hate speech, and more recently, the European Democracy Shield. Every one of these laws is intertwined with the DSA and its implementation and will impact the scope and definitions for valid research.

The technical and infrastructure requirements that the DSA and the Delegated Act propose, not only to access data, including GDPR compliance,[36] but also technical capabilities to host and analyse vast amounts of data safely, can be insurmountable barriers for non-European institutions. This is especially true for Latin America, where data protection laws are flawed at best, research institutions for the most part lack the infrastructure needed to comply with technical and legal requirements under European law, and funding is scarce.[37] Africa is similarly positioned,[38] and these challenges have been highlighted as particularly important for research and autonomy.

Article 40 limits its scope to research related to Articles 34 and 35 of the DSA

Besides procedural or expertise-driven challenges, the wording of the data access for research provisions limits the scope of permissible research questions to those that relate to Europe and the DSA-enacted priorities. The conception of valid research questions and the need for requests to expressly argue the relationship between the research and the systemic risks identified in Article 34, or the mitigation measures established in Article 35, are most likely to be understood restrictively to Europe's geography, priorities, and understandings. In practical terms, this means that under the DSA, research on topics such as Holocaust denial is likely to be considered valid in Europe due to historical and legal significance.

By contrast, the legal and social practices of other groups on issues such as, state-driven propaganda, and government-led censorship issues that are especially relevant in many Global Majority countries are less likely to fall within the DSA's scope. Similarly, while research on foreign information manipulation and interference (FIMI) may be encouraged, studies on partisan disinformation or "dirty campaigning" are unlikely to be supported, not because they are unimportant, but because the DSA prioritises distinctly European risks and separates company actions from state involvement. Not because these are not valid concerns, but because in the DSA context, company and state conduct are clearly separated and distinct, independent from one another, rather than two parts of a wider, more diverse and complex information ecosystem.[39] In the DSA context, state action, or state-company interactions, are not factored as risks capable of generating a negative impact on human rights. This has been particularly questioned by academics and CSOs, especially in Global Majority countries.

Risks of abuse

Every law creates a risk for abuse. This does not mean that the issue should not be regulated or legislated, but rather that in designing, interpreting, and implementing legislation, there should be control mechanisms built in to counter eventual abuse. These often vary depending on cultural and historical issues. Some states are more prone to corruption, others to despotism or authoritarianism, others to armed conflict or war, etc. These risks can be unpacked in the following way:

State capture of research for political purposes:

The DSA is built under the assumption that the state has built-in mechanisms to balance political forces and interests and keep them in place. This may be partially so because the EC is a regional body and reserved for itself the oversight of VLOPSEs. In the EC, there are many states and many political interests represented, preventing the capture of the mechanism for any one member state or any one political party. When the DSA is viewed or envisioned as a model, this particular balance of power needs to be accounted for. Particularly when the law is vague and its concrete contents can, and probably will, be derived from research.

Funding for education in the Global South is diverse and varies from one country to another. In Latin America, there are countries where the state holds most of the funding for research and where, in many cases, there is room for political capture. Even in a system like the European, the power vested in the DSCs is unprecedented and needs to be complemented with vigilant oversight mechanisms and full transparency and accountability.

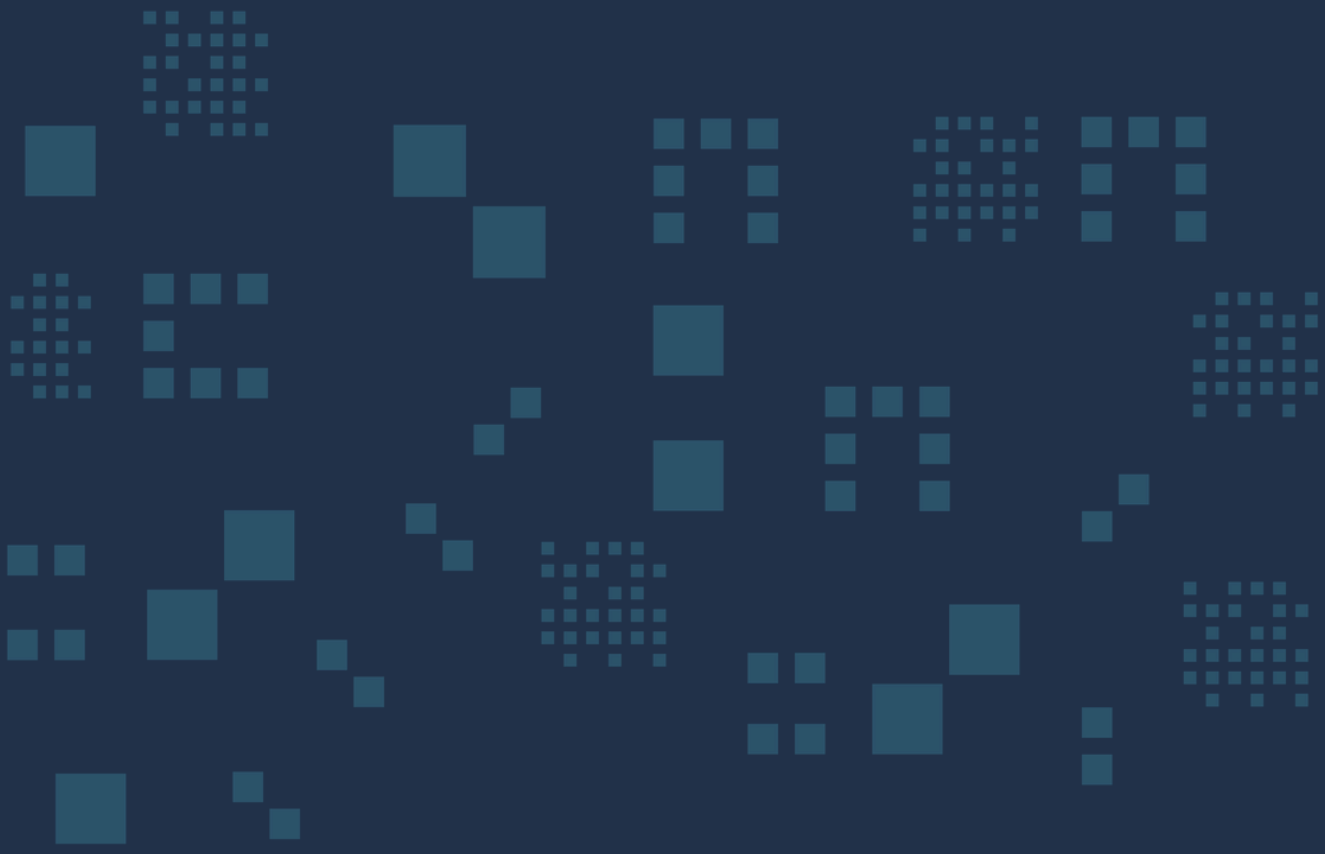
Weak access to information mechanisms:

Among the challenges that the DSA presents for foreign and domestic researchers alike is the scope of the provision. Access to data for researchers is limited to issues related to the research of systemic risks under Articles 34 and 35 of the DSA. And none of those articles identifies the state as a potential creator of risks within platforms. This paper has already highlighted the need for active transparency of the state and the EC in its enforcement and implementation of the DSA. This requirement for access to information and transparency cannot be underestimated in countries where there are weak traditions of transparency, a history of opacity, and a lack of efficient oversight and accountability.

Surveillance: Access to data and Open Source Intelligence (OSINT):

Access to data, particularly individual personal data from account holders, needs to be handled delicately. Security infrastructure needs to be in place, and guarantees that these mechanisms don't become a new form of surveillance in disguise need to be provided. State-controlled institutions should probably be held to different standards and rules than private entities or academically independent and autonomous entities. Data protection regimes, including the GDPR, should be amended to include restrictions on the transfer and use of data accessed for research purposes by other state entities or other public purposes. This is particularly important in countries where data protection laws apply rigorously to the private sector but are lightweight towards the public sector.

Furthermore, this paper has described the potential of Article 40 (12) to shape access to publicly available information and provide a legal framework for its development and deployment. Open-Source Intelligence is precisely dependent upon what can be considered open source or publicly available information and can foster and further state mass surveillance efforts to the detriment of its citizens and anyone else under its jurisdiction. The judicial and academic interpretation of these provisions could benefit from Global South experiences with the issue, particularly given the opacity that has characterised the acquisition of open-source surveillance technology from states.[40]



07 Other existing models and initiatives?

Besides the DSA, there are other initiatives that seek to access data from companies and conduct research into platform operations and their societal impact. Historically, these initiatives have been independent and isolated, and many times fostered duplication of efforts among many different actors. The use of APIs, for example, was widespread before 2016 and more limited afterwards.

IRIE

One interesting overarching initiative to address information and data access on a systemic level was the IRIE initiative[41] (Institute for Research of the Information Environment) proposed by professors Alicia Wanless (Carnegie Endowment) and Jakob Shapiro (Princeton University). This initiative stemmed from the concern that access to data within platforms would require infrastructure that would be expensive, difficult to replicate, and overall inaccessible to many. Professors Wanless and Shapiro envisioned a CERN-like institution, where the idea was to create centralised nodes that could host and process information per researcher requests and address the information environment as a whole, rather than solely digital or solely platform-related information. The IRIE model was intended to bring support from states and universities across different countries, but the effort was diluted as the DSA implementation got more complicated and delayed, and due to funding constraints in building the proposal.

Global North Initiatives

Concurrently, there have been a number of other initiatives that sought to facilitate bits and pieces of data for researchers to work with. Key among them were CrowdTangle, within META and in existence until 2024, for example, or the possibility offered by certain platforms to work their way through data using APIs. Another interesting initiative was NYU's Ad Observer,[42] which was closed at the behest of Facebook in 2021. Each company, additionally, negotiates private agreements and commissions research with different institutions and researchers, allowing them access to data that is otherwise unavailable to others. These initiatives, in general, depend on the consistent funding and support provided by philanthropy or universities and rely on companies' goodwill to survive. Overall, researchers across different regions and fields of study still complain that companies are reluctant to surrender data, that processes to apply for data access are hard to navigate, and that even when some data is shared, conditions and the quality of data surrendered are far from ideal.

Better Access Framework

In November 2025, the Knight-Georgetown Institute released a report[43] on data access for research that proposes an interesting paradigm shift. Entitled "Better Access: Data for the Common Good", it doesn't focus necessarily on legally mandated transparency obligations, but rather on the construction of a shared understanding of what information should be publicly held for research and what data companies should treat differently for data access purposes. The premise is not that this information should be accessible for research purposes, but rather that this information should be available for everyone to see and access, whether it's for research, journalism or even citizen curiosity. The grounds for the openness of these accounts and their data are not the right to research but rather the duties of transparency that should guide democratic societies and the universal right to access state information.

The report makes an interesting cut regarding the kinds of accounts or information that should be public by their own merits, and in doing so, it creates hurdles to an otherwise clean and elegant proposal for data access. The Better Access framework calls for the availability of data from:

- "Highly Disseminated Content: Posts or videos that achieve exceptional reach or engagement, shaping the public agenda.
- Government and Political Accounts: Posts from accounts belonging to elected officials, candidates, political parties, and institutions, which directly influence governance.
- Notable Public Accounts: Content from accounts belonging to celebrities, journalists, civic leaders, or other public figures whose reach gives them outsized influence.
- Business Accounts and Promoted Content: Advertising and commercial messaging, which can sway consumer behaviour, public health, or public trust."

The distinction between public officials and institutional, state-owned accounts and other accounts that impact the conversation needs further clarity, and the grounds to grant and demand these kinds of data need some sorting. Although the logic behind the grouping of these accounts and their distinction from other accounts can be understood, the legal grounds for these claims are radically different. For example, public officials' data and account activity may be easily requested under access to information obligations. Data from accounts that get "highly disseminated content" may be harder to explain under the access to information logic. It may be easier under the public interest logic if it is a public interest matter. And in that case, probably not all content will be of public interest. Should all the data from that account be open and available for anyone to see and search, or only the data related to the highly disseminated content? How should companies address this? What should be understood by highly disseminated content?

The report defines each category and provides guidelines, but still, the grouping of these diverse accounts raises issues from an implementation and translation into regional contexts. Regardless, the Better Access framework provides an interesting starting point for discussion. This is particularly true in Global Majority countries, where government opaqueness and lack of transparency regarding social media and technology use are widespread, often creating greater risks to public discourse than private actors. It may also provide some grounds for regional human rights bodies and instruments to help build a framework that can encompass state action, as well as private actors' action to frame these conversations from a freedom of expression point of view.

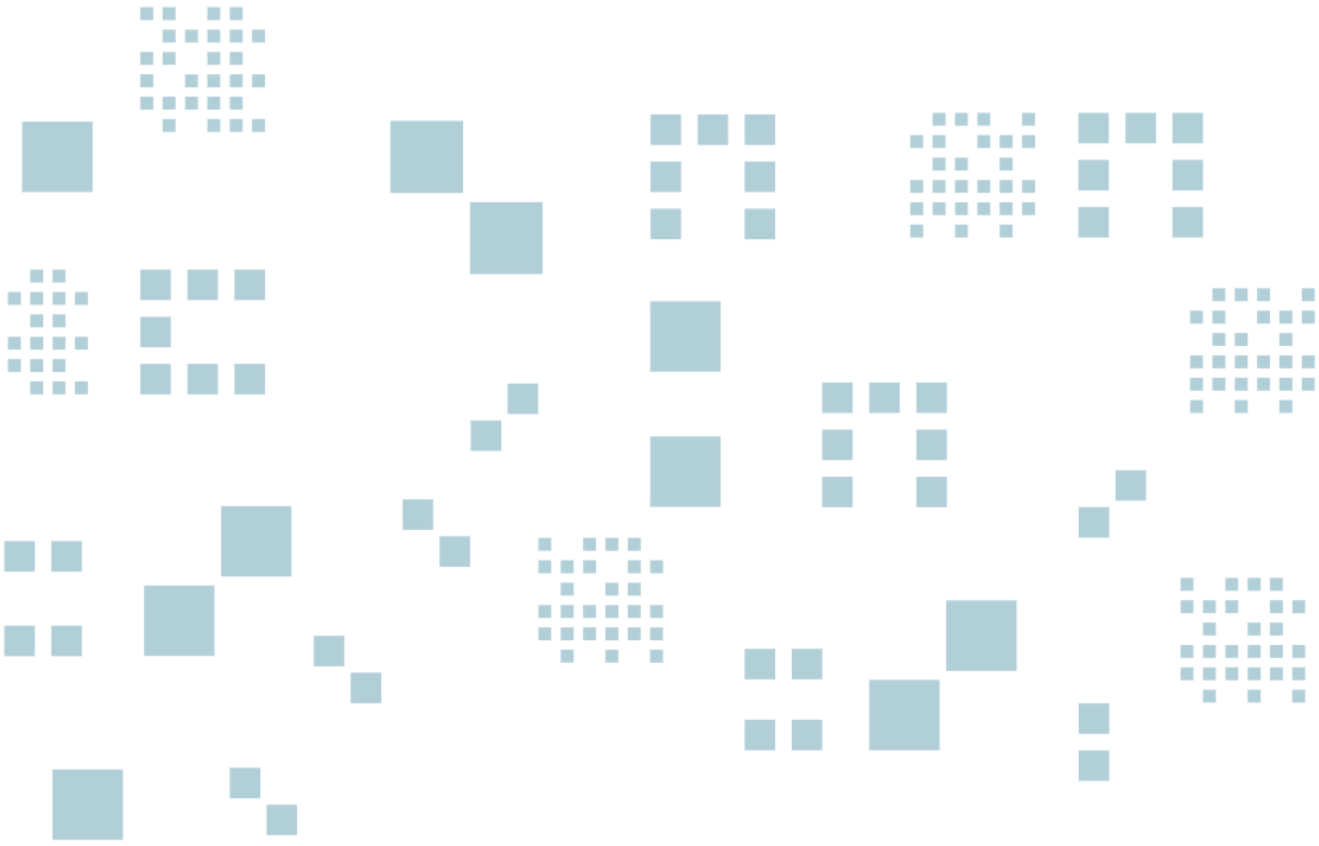
Global Majority Initiatives

In Global Majority countries, few initiatives are currently looking into access to data for researchers.[44] CELE published a couple of blog posts on the issue and followed the debate over data access to research in the negotiation and consultation phase in the EC. And it worked with InternetLab in Brazil to develop common positions that could gain some more traction among European counterparts.[45] CELE also worked with IRIE to raise issues affecting the Global South and to foster the inclusion of diverse voices in framing the need, scope, and understanding of the project. The Center also hosted a discussion as part of RightsCon 2023 in Costa Rica to hear from different organisations about their research needs, opinions, or positions on the potential implementation of data access for research projects. The Centre for Communications Governance at the National Law University Delhi has published a comprehensive report on platform transparency under the DSA that looks at them from a Global South perspective. It includes a whole chapter dedicated to data access for researchers.[46]

Linterna Verde, a Colombian organisation, also later had a project that intended to look at the issue, spark a dialogue, and build resources towards a common understanding of data access to research, in line with prior efforts. Even though the effort was more practical and less policy-oriented, the project did gather experiences that could feed regulatory or self-regulatory efforts towards more openness and data access for research purposes. The overall impression from the project leader, however, was that companies were reluctant to include new members in their data access for research initiatives. Linterna to access META's data library, and it took them at least two years to get approval and start getting some of the data they had originally requested.[47]

Need for an enhanced conception of data access for researchers in the Global Majority

The above initiatives and experiences are not exhaustive nor are they conclusive in their descriptions of Global Majority efforts. Still, there are commonalities to different regions in the Global South that call for further attention and development. The lack of content governance discussions in the Global Majority countries is among the most salient challenges for data access for research. Except for India and Brazil, most other Majority World countries' concerns seem to be focused on data protection, broader human rights protections and state-led discrimination and censorship rather than content governance. In this context, framing the conversation like the Better Access framework does, may contribute to developing an enhanced conception of data access for research and may foster a translation of regulatory obligations that better meets the needs of Global Majority countries.



References

[1] European Commission, Press release: "Delegated act on data access under the Digital Services Act (DSA)", July 02, 2025, available at https://digital-strategy.ec.europa.eu/en/library/delegated-act-data-access-under-digital-services-act-dsa.

[2] European Commission, Delegated Regulation (EU) 2025/2050 of 1 July 2025 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

[3] CELE & InternetLab, Submission in response to the Public Consultation on the draft delegated act on access to online platform data for vetted researchers under the Digital Services Act (DSA), Documento de posición No. 22, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024). Available at https://www.palermo.edu/Archivos_content/2024/cele/diciembre/2024_12_10_DP22_CELE%20(1).pdf

[4] Digital Services Act, Articles 15, 24 and 42; Article 10; Recital 90; Article 37; Article 40.1; Articles 40.4 and 40.12, respectively.

[5] Digital Services Act, Articles 40.4 and 40.12

[6] European Commission, Delegated Regulation (EU) 2025/2050 of 1 July 2025 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council by laying down the technical conditions and procedures under which providers of very large online platforms and of very large online search engines are to share data with vetted researchers

[7] European Commission, Consultation Results: Digital Services Act: Summary report on the call for evidence on the Delegated Regulation on data access, November 24, 2023, available at https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-call-evidence-delegated-regulation-data-access.

[8] DSA Transparency Database: https://transparency.dsa.ec.europa.eu/.

[9] European Commission, Press release: Very Large Online Platforms and Search Engines to publish first transparency reports under the DSA, October 26, 2023, available at https://digital-strategy.ec.europa.eu/en/news/very-large-online-platforms-and-search-engines-publish-first-transparency-reports-under-dsa.

[10] European Commission, Consultation Results: Digital Services Act: Summary report on the call for evidence on the Delegated Regulation on data access, November 24, 2023, available at https://digital-strategy.ec.europa.eu/en/library/digital-services-act-summary-report-call-evidence-delegated-regulation-data-access.

[11] Keller, Daphne, Using the DSA to study platforms, Verfassungsblog, October 27, 2025, available at https://verfassungsblog.de/dsa-platforms-digital-services-act/

[12] Id.

[13] See Wikipedia, Section 230, at https://en.wikipedia.org/wiki/Section_230.

[14] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

[15] See Global Network Initiative, About GNI, https://globalnetworkinitiative.org/about/.

[16] See Business and Human Rights Centre, UN Guiding Principles, https://www.business-humanrights.org/en/big-issues/governing-business-human-rights/un-guiding-principles/.

[17] Amnesty International, Yahoo's data contributes to arrests in China: free Shi Tao from prison in China!, July 2006, https://www.amnesty.org/es/wp-content/uploads/2021/08/asa170402006en.pdf.

[18] Wikipedia, Edward Snowden, https://en.wikipedia.org/wiki/Edward_Snowden

[19] Manila Principles, available at https://manilaprinciples.org/index.html

[20] Wikipedia, Cambridge Analytica Scandal, https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[21] Id

[22] Wikipedia, Social Media in the 2026 United States Presidential Election, https://en.wikipedia.org/wiki/Social_media_in_the_2016_United_States_presidentialS_election.

[23] Tromble, Rebekah. (2021). Where Have All the Data Gone? A Critical Reflection on Academic Digital Research in the Post-API Age. Social Media + Society, 7(1). https://doi.org/10.1177/2056305121988929 (Original work published 2021)

[24] CELE's Submission on the Draft Delegated Act on Transparency Reports (detailed rules and templates) under the DSA, June 24, 2024, available at https://www.palermo.edu/Archivos_content/2024/cele/paper-dsa/dsa.pdf

[25] DSA, Article 34.1. c

[26] Art 19 ICCPR, Art 10 ECHR, Art. 13 ACHR.

[27] Supreme Court of the United States, Jacobellis v. Ohio, 378 U.S. 184 (1964), concurring opinion of Justice Stewart

[28] CELE & Internetlab, Submission in response to the Public Consultation on the draft delegated act on access to online platform data for vetted researchers under the Digital Services Act (DSA), Documento de posición No. 22, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024). Available at https://www.palermo.edu/Archivos_content/2024/cele/diciembre/2024_12_10_DP22_CELE%20(1).pdf

[29] LK Seiling, Clara Iglesias Keller, Jakob Ohme, Ulrike Klinger, Claes de Vreese, Data Access for Researchers under the Digital Services Act: From Policy to Practice, Weizenbaum Policy Papers #14, September 2025, available at https://www.weizenbaum-library.de/server/api/core/bitstreams/377ca0de-f3cf-488f-bffc-9d8740d18cab/content.

[30] CELE & InternetLab, Submission in response to the Public Consultation on the draft delegated act on access to online platform data for vetted researchers under the Digital Services Act (DSA), Documento de posición No. 22, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024). Available at https://www.palermo.edu/Archivos_content/2024/cele/diciembre/2024_12_10_DP22_CELE%20(1).pdf

[31] Ilori, Tomiwa, Contextualisation over Replication: The Possible Impacts of the Digital Services Act on Content Regulation in African Countries, Verfassungsblog, November 3, 2022, available at https://verfassungsblog.de/dsa-contextualisation-replication/

[32] DSA 40 Data Access Collaboratory, About the Collaboratory, https://dsa40collaboratory.eu/about/

[33] DSA Observatory, https://dsa-observatory.eu/

[34] University of Amsterdam Law School's Institute for Information Law, Summer Course on European Platform Regulation 2026, https://www.ivir.nl/courses/epr/

[35] The London School of Economics, Specialist Course on the EU Digital Services Act, available at https://www.lse.ac.uk/law/study/short-course/eu-digital-services-act

[36] Complete guide to GDPR compliance, GDPR.eu

[37] Tavishi and Shobhit S., 'Platform Transparency under the EU's Digital Services Act: Opportunities and Challenges for the Global South' (Centre for Communication Governance, National Law University Delhi 2025), chapter 5: Researcher Access to Platform Data, available at https://ccgdelhi.org/research-reports/platform-transparency-under-the-eus-digital-services-act-opportunities-and-challenges-for-the-global-south

[38] Hendrix, Justin, Can An Alliance Get Access to Platform Data for African Researchers?, Tech Policy Press, January 5, 2024, available at https://www.techpolicy.press/can-an-alliance-get-access-to-platform-data-for-african-researchers/

[39] See, for instance, Agustina Del Campo, Nicolas Zara and Ramiro Álvarez Ugarte, Are Risks the New Rights? The Perils of Risk-based Approaches to Speech Regulation, 16 (2025) JIPITEC 23, available at https://www.jipitec.eu/jipitec/article/view/439. Also Agustina Del Campo, Nicolás Zara, Ramiro Alvarez-Ugarte Proceedings of Fourth European Workshop on Algorithmic Fairness, PMLR 294:265-280, 2025, available at https://proceedings.mlr.press/v294/del-campo25a.html.

[40] Zara, Nicolás, Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay, Centro de Estudios en Libertad de Expresión (CELE), September 2023, available at: https://www.palermo.edu/Archivos_content/2023/cele/papers/23300of8-reporte-regional-OSINT.pdf.

[41] See Carnegie Endowment for International Peace, Information Environment Project, https://carnegieendowment.org/projects/information-environment-project?lang=en

[42] See NYU Cybersecurity for Democracy, Ad Observer, https://adoserver.org/

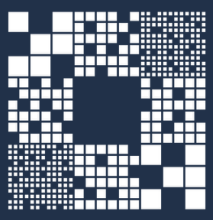
[43] Knight Georgetown Institute's Expert Working Group on Public Platform Data, Better Access: Data for the Common Good A Framework for Accessing High-Influence Public Platform Data, November 2025, available at https://kgi.georgetown.edu/research-and-commentary/better-access/

[44] See for example https://dataalliance.africa.

[45] CELE & InternetLab, Submission in response to the Public Consultation on the draft delegated act on access to online platform data for vetted researchers under the Digital Services Act (DSA), Documento de posición No. 22, Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2024). Available at https://www.palermo.edu/Archivos_content/2024/cele/diciembre/2024_12_10_DP22_CELE%20(1).pdf

[46] Tavishi and Shobhit S., 'Platform Transparency under the EU's Digital Services Act: Opportunities and Challenges for the Global South' (Centre for Communication Governance, National Law University Delhi 2025), chapter 5: Researcher Access to Platform Data, available at https://ccgdelhi.org/research-reports/platform-transparency-under-the-eus-digital-services-act-opportunities-and-challenges-for-the-global-south

[47] Juan Martín Marinangeli, Access to Data for Researchers: The Challenges of Civil Society in the Face of Digital Platforms. A Conversation with Carlos Cortés and Laura Palacio, CELE blog, November 7, 2024, https://observatoriolegislativocele.com/en/Access-to-data-for-researchers%3A-the-challenges-of-civil-society-in-the-face-of-digital-platforms%3A-a-conversation-with-Carlos-Cortes-and-Laura-Palacio/



GLOBAL
PARTNERS
DIGITAL