United Nations Office of the High Commissioner for Human Rights (OHCHR)

Response to the European Commission consultation on draft act on researcher access to data under the EU Digital Services Act

9 December 2024

Introduction

OHCHR is grateful for the opportunity to feed into the consultation on the draft delegated regulation on researcher access to data under the Digital Services Act (delegated regulation). OHCHR welcomes this delegated regulation, transparency, and access to data are key components for an evidence-based approach to human rights compliance of online platforms. At the same time, providing access to data does not come without human rights risks, nor is it easy to strike the balance between protecting privacy and ensuring meaningful access to researchers. OHCHR respectfully makes recommendations and analysis to help forward our common goal of ensuring stronger human rights protection online.

Digital Service Coordinators (DSCs)

The delegated regulation proposes that the DSCs manage requests and ultimately make decisions regarding researchers request for access to data, and that they *may decide* to consult experts in reaching those decisions. Given the enforcement role that the DSCs have under the DSA, a conflict of interest could arise when approving access for researchers, as over time, the research concerned could provide critical analysis of the very work and role of the DSCs themselves. OHCHR therefore echoes the calls of civil society, that an independent intermediary body could be more appropriate to carry out this role. Such a body should have a mandatory, not optional duty to consult with experts.

Vetted researchers

The delegated regulation, as per the DSA relies on the definition of a researcher as per Article 2, point (1), of Directive (EU) 2019/790 ('the copyright directive'). According to this definition, a research entity is said to mean a university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research: on a not-for-profit basis and or pursuant to a public interest mission recognised by a Member State.

Law Enforcement

OHCHR is concerned that a public interest mission recognised by a Member State could be interpreted to include interests relating to national security or law enforcement. The EU's general data protection regulation (GDPR) provides a legal framework concerning data access for law enforcement, however, neither GDPR Article 89 nor DSA Article 40 would entirely prevent a law enforcement agency from acting as a "vetted researcher" under this regulation. To ensure robust "use limitations" on law enforcement use of data, and given the existence of

other, more appropriate channels for law enforcement to access such data, OHCHR would echo the recommendations of the European Digital Media Observatory Working Group, in suggesting that the delegated regulation should explicitly preclude law enforcement agencies or those working for law enforcement from qualifying as vetted researchers for the purpose of the DSA. Rule of law safeguards regarding law enforcement access to data are crucial, nothing in this proposed regulation should allow for access which might otherwise merit a warrant or other form of judicial oversight.

The Need for Human Rights Expertise

The primary objective of research under the proposed regulation would be considering the systemic risks stemming from platform behaviour, as iterated in the DSA. As we have previously highlighted certain concepts listed in the DSA as systemic risks such as 'civic discourse' or 'democratic participation', require further clarification. At the same time, the international human rights framework is a logical reference point when breaking down these concepts i.e. the quality of civic discourse can be considered considering the respect of the right to freedom of opinion and expression Art. 19 ICCPR, as well as the rights to freedom of association etc.

Furthermore, to date, audits under the DSA are primarily being carried out by the largest private sector consultancy firms. Such private sector actors present a risk of corporate capture, and do not have the requisite expertise and experience on human rights as other mandated bodies such as national human rights institutions, equality bodies, the EU Fundamental Rights Agency, and human rights NGOs.

To offset the risk of corporate capture, and to close the gap in expertise, OHCHR would recommend that such human rights actors as listed above be mentioned as *prima facie* vetted researchers for the purpose of the delegated regulation. This explicit mention would be merited as the definition of research entity above is limited to where research is the 'primary goal', whereas many human rights actors including OHCHR have numerous roles including but not limited to human rights research. Their expertise and independence should make them logical candidates for this consideration.

Technical Access for Human Rights Researchers

Article 9. of the proposed regulation states that the "Digital Services Coordinator of establishment shall determine in the reasoned request the modalities according to which access to the data is to be granted by the data provider" ... the Article clearly points to "a secure processing environment" as an elaborated mode of access.

It will be important to ensure that human rights researcher actors, such as NGOs and OHCHR can use APIs to download data for further analysis in their own environments. This is important because currently some of those platforms who have content libraries use setups, with two modalities for interacting with the data, the first is through a user interface, the second an API, both of which sit on top of a secure processing environment, which means that the Platform provides the environment in which the data is accessed and processed by researchers. The lack of possibility to use the API to download data for further analysis in OHCHR's environment or for OHCHR-internal dissemination of research results via a dashboard or data product can undermine the scalability of our use of such content libraries and, for example, obstruct approaches to monitoring phenomena such as incitement and hate speech. Concretely, OHCHR

or NGOs may wish to download data on takedown requests from law enforcement and analyse it alongside our existing civic space data. Current experience to date suggests that such a use case would be inhibited by the secure processing environment modality.

While there are good reasons for this approach (Article 9 mentions the protection of confidential information and the security of the data provider's service), and while the current draft leaves open the possibility of more permissive access to data from the very large online platforms, at the discretion of the Digital Services Coordinator, it may be useful to balance the mention of data providers' secure processing environments by reference to other common access modalities and associated safeguards.

Protections Against Reprisals

Previously researchers and fact-finding mandate-holders have highlighted the importance of the anonymity of the applicant researchers. This would not be possible under Article 8(2)(a) of the proposed regulation. To on-board our researchers in the past and provide them access to content libraries OHCHR has requested derogations from standard terms, for instance permission to use generic un.org email addresses etc. OHCHR takes this precaution due to the sensitivity of the research and the potential for reprisals against those carrying it out. OHCHR would therefore recommend derogations from the requirement to submit a resume/CV for each researcher, in cases where the research entity itself has been vetted.

ENDS/