Address the Amplification of Dis- and Misinformation

EU DisinfoLab responds to the Digital Services Act Consultation

8 September 2020

Address the Amplification of Dis- and Misinformation: EU DisinfoLab Responds to the Digital Services Act Consultation

8 September 2020

Dis- and misinformation on digital platforms threaten the functioning of our digital public sphere, and the core institutions and values of European Member States. As the Covid-19 health crisis and 'infodemic' have shown, the health and safety of individuals is also at stake. The Digital Services Act legislative package has a crucial role to play in addressing the information disorders in our online environment.

The EU Code of Practice on Disinformation showed that self-regulatory initiatives compose part, but not all, of a comprehensive response to disinformation. While the Digital Services Act should maintain the essence of the current limited liability regime and avoid the trap of general monitoring, the new legislation presents an opportunity to address the mechanisms on digital platforms that amplify dis- and misinformation.

Distinguish between misinformation and disinformation

Though the two terms are often used interchangeably, the distinction is important in the context of the new legislation. Disinformation should be understood as deliberately fabricated or manipulated content that is spread for economic, personal, or political gain, or to intentionally deceive the public[1]. Camille François established a framework for analysing modern influence operations known as the disinformation "ABC", which accounts for "manipulative actors", their "deceptive behaviours" tactics and techniques, and the "harmful content" itself[2]. In our monitoring of digital disinformation activities at EU DisinfoLab, we have also found it is necessary to examine the distribution of this content, or the structural factors that assist its dissemination. As EU DisinfoLab Executive Director Alexandre Alaphilippe has explained, "How disinformation diffuses and spreads owes largely to the digital architectures of online platforms"[3].

Misinformation, unlike disinformation, does not need malign intention. Misinformation may simply be content that is reshared with insufficient care or

---

[1] https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

[2] https://science.house.gov/imo/media/doc/Francois%20Addendum%20to%20Testimony%20-%20ABC_Framework_2019_Sept_2019.pdf

[3] https://www.brookings.edu/techstream/adding-a-d-to-the-abc-disinformation-framework/

context; it can stem from an inaccurate translation, caption or date. For the purpose of the Digital Services Act, an important technical difference between dis- and misinformation relates to amplification. These challenges are intricately linked and even overlapping, but they imply different responsibilities for different stakeholders. Mechanisms like open content recommendation systems and targeted advertising further the reach of disinformation and create conditions for misinformation[4].

Focus on curation rather than content

Disinformation represents a particular challenge to the DSA's efforts to distinguish between illegal and harmful content. Disinformation can be harmful, but legal (misleading information, conspiracy theories, rumours) or illegal (voter suppression, foreign interference, defamation), depending on the situation. It can be extremely difficult to distinguish illegal versus harmful content, for instance, content in the so-called "grey zone", without a court ruling. Regarding dis/misinformation, we think the DSA should therefore focus on curation rather than content. For such complex moderation challenges as dis and misinformation, it is important to focus on the platform's methods of diffusing and amplifying content. This is preferable to an approach that risks encouraging general monitoring and overblocking of legal content.

Provide meaningful transparency for all stakeholders

Much digital disinformation remains under-investigated and its mechanisms poorly understood due to the asymmetry of the information available. At the moment, data provided by the platforms, mostly as a result of public or mediatic pressure, is often partial or unusable. Indeed, only a few global stakeholders have the ability to process very large amounts of data in order to research and investigate disinformation campaigns. Moreover, these processes are time-consuming and therefore not a match for the constant acceleration of online disinformation.

For this reason, the Digital Services Act should set requirements for meaningful transparency. Academics, journalists, open-source investigators, and other experts must be able to research and unfold the tactics, actors and behaviours behind disinformation, as well as their impact. Beyond data for data's sake, stakeholders need information that helps them understand the platforms' digital architectures, particularly algorithmic content curation and acceleration; the data shared by platforms is generally inadequate (and often unverifiable) in this regard. For researchers, computational transparency (real time access to APIs with data, auditable algorithms) should allow them to further investigate information

---

[4] https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/

disorders and disinformation activities. For users, clearly explained, understandable transparency around content recommendations and advertising should reduce the information gap between platforms and users and facilitate a trustworthy journey. Finally, the new legislative framework should set up transparency requirements enabling independent public oversight, and provide adequate support for this oversight. The DSA should establish a new regulatory mechanism with auditing competence over platforms that is capable of assessing platforms' commitments as well as risks related to manipulation and the amplification of dis- and misinformation.

Require accountability for amplification

Disinformation can be spread by actors who intentionally abuse digital services, for example, through coordinated behaviour, misleading synthetic or tweaked media, false or divisive messaging, and through monetised campaigns. But the architecture of digital platforms is also responsible for amplifying this content. Open recommendation systems are optimised for user engagement, which in practice means drawing on predictive metrics that infringe user privacy. It also means optimizing for divisive, sensationalist and unverified content, like hate speech, and disinformation.

In our own research, we discovered that Facebook's recommendation algorithm was promoting pages with disinformation from a French white supremacist group[5]. Facebook's algorithm extended the reach of this group, helping it achieve nearly a half million followers. In fact, Facebook's recommendation system actually helped the group generate revenue by guiding Facebook users to the group's payment and monetisation services. Similar mechanisms have been described for instance around QAnon Facebook groups[6] or YouTube conspiracy videos such as the Plandemic video[7].

Open content recommendation systems and targeted advertising are not the only mechanisms on digital platforms that amplify dis- and misinformation. Recent research suggests that exposure to social engagement metrics (followers, likes, shares) also increases the likelihood that users will further diffuse "low-credibility content"[8]. In parallel to the implementation of meaningful transparency we have described, content recommendation systems and targeted advertising represent sufficiently defined areas for the Digital Services Act to already intervene to impose accountability.

---

[5] https://www.disinfo.eu/publications/suavelos-white-supremacists-funded-through-facebook
[6] https://www.nytimes.com/2020/08/19/technology/facebook-qanon-groups-takedown.html
[7] https://www.nytimes.com/2020/05/20/technology/plandemic-movie-youtube-facebook-coronavirus.html
[8] https://misinforeview.hks.harvard.edu/article/exposure-to-social-engagement-metrics-increases-vulnerability-to-misinformation/

Account for networks and the porosity between services

While focusing on the gatekeepers of our information society, the DSA must acknowledge the larger landscape of digital services and especially the porosity between services. With regards to disinformation, digital platforms — even so-called "walled-gardens" — are not fully siloed spaces. Disinformation often relies on magnifying its reach as well as manipulating the legal restrictions and terms of services by traversing many digital services at once. For instance, research from Graphika on the disinformation campaign labelled "Secondary Infektion" has shown that more than 300 websites and online platforms have been used (and abused) to spread forged documents from the EU Commission or EU member states[9]. EU DisinfoLab's current research is focused on the role that crowdfunding platforms play in financing disinformation, in particular the way that actors use smaller platforms to sustain their activities on gatekeeping platforms. The mechanisms through which digital platforms allow malign actors to profit from disinformation and exploit the porosity between services is an area necessitating further research and regulatory attention. Moreover, the cross-posting and amplification of disinformation content on multiple platforms is also an element that is under-researched, where engagement numbers have been driving algorithmic recommendations.

Align with the European Democracy Action Plan

An effective and rights respecting approach to dis- and misinformation must be as multifaceted as disinformation itself. EU DisinfoLab recalls its position on the need to sustain a decentralised framework of civil society stakeholders in order to efficiently combat disinformation. Indeed, this issue requires the engagement of a high variety of stakeholders in a whole of society approach. EU DisinfoLab wishes that the new legislative package will align closely with the European Democracy Action Plan. These proposals must be harmonized to guarantee the development of meaningful transparency and accountability for disinformation beneficiaries and their intermediaries. Alignment between the proposals will also ensure that civil society is equipped, both financially and structurally, to research, investigate and democratically hold malicious actors responsible.

---

[9] https://secondaryinfektion.org/

For more information please contact:
Claire Pershan, Policy Coordinator, EU DisinfoLab, cp@disinfo.eu