mediagov@univie.ac.at
Währinger Str. 29, A-1090 Wien
mediagovernance.univie.ac.at

FREuDe
JEAN MONNET CENTRE OF EXCELLENCE
COMMUNICATION, FACTS & REGULATION FOR EUROPEAN DEMOCRACY

POLICY BRIEF

November 2022

REGULATORY RESPONSES TO DISINFORMATION AND CYBERSECURITY THREATS IN EUROPE

Jorge Abaurrea

DOI 10.5281/zenodo.7891968

Who is this aimed at

- EU digital media policy makers and planners in government and institutions

Key messages

- Information disorders have aggressive and emotional online and real-world responses from many individuals
- The character of the problem is hybrid, including bodies and individuals
- Final responses must find a balance between regulation and education

Introduction

Since 1995[1], some not-so-new (but wholly refurbished and transformed) “disorders” have reappeared linked to technology and, more specifically, to digital platforms. Propaganda, fake news, and similar are part of a vast catalogue of phenomena reshaping public opinion.

The disorders term has been neatly described by Wardle and Derakhshan[1], who makes the difference between mis-, dis-, and mal-information and creates an interesting proposal based on an element matrix. They use the harm and falseness dimensions to make the boundaries between these types of information.

Companies like Meta (formerly Facebook), Twitter, and TikTok are involved in the massive use and range of capability of their tools to target selected high-spreading hubs to get digested messages (mainly commercial but also some others related with the social and political space).

[1] Bran, R., Tiru, L., Grosseck, G., Holotescu, C., & Malita, L. (2021). Learning from Each Other—A Bibliometric Review of Research on Information Disorders. Sustainability, 13(18), 10094. https://doi.org/10.3390/su131810094

According to Eurostat data[2], social media are the primary medium of choice for reading news for young people (aged 16-29 years). Data state that is the preferred option for 69% of them. That seems entirely organic when 95% use the internet daily.

Technology has always been in the eye of countries, especially concerning their security. We remember how the Internet was formerly known as Arpanet, a military project. Its evolution has grounded topics like the cyberthreat one, primarily regarding systemic risks. In them, disinformation has its place, as it can have several civil or military impacts.

Disinformation and Cybersecurity Threats: Context of the Problem

Since the general adoption of the Internet, we have seen several stages of its relationship with many affected shareholders (civil society, governments, and companies). If we think of the early years, it was seen as something for techies, as the access was by not-so-expensive machines (all you needed was a computer and a modem linked to a telephone line). The biggest connectivity problem was solved, as the www became a linked platform, breaking the lines of the international (and expensive) calls to connect to other computers, mainly in Europe, where have roaming was still not a mainstream policy. From that moment, national companies started building dedicated “internet” platforms, including offers to DSL lines.

From that internet early years, we have moved to one kind-of “internet adolescence”, where the Internet needs to find and suit the constitutional world and its protection limits. Next to these adolescent challenges, informational disorders emerge that comprise this policy brief’s core. And the time has come to reconsider everything. Old world war (and sales) tactics find a new propagation way without paying (at least in their first days) much attention to the impacts they may have.

It was like a “monkey with a gun”, where strategy companies could use digital platforms and their “playing tools” (who would be afraid of a quiz that finds the best place to live or the dog you match with). The underneath reality links with creating a database of interests. That could be used (and sold) to political parties and other organisations to build and test opinion hubs.

This late adolescence has changed its manners to work with other new models (still in their very early days) to create tailor-made messages. We are talking about algorithms, artificial intelligence, and many other patronage and analysis tool that can create the perfect message for the intended objective. In cases like the Cambridge Analytica one (related to Facebook's use of personal information, 87 million users could have been affected[3]. That means thousands, if not millions, of messages inside a structured journey acting in a predictive way modelled by their predecessors. To sum up, fake accounts and bots pique the collection.

Current Stage

Internet may be preparing to move into its stage of adulthood, albeit not meaning the age of the majority of its users, but the one where the brain completes and can leverage risks. It should behave with honour and courage, leaving evilness aside. That is the point where regulatory responses come in. States and institutions have had a privileged point where they have seen the effects of limitless growth, defeating the early thoughts of a connection network that would improve the world and the relationship among towns or even create world peace [4].

---

[2] https://ec.europa.eu/eurostat/databrowser/view/isoc_sk_dskl_i21/default/table?lang=EN

[3] Confessore, N. (2018). Cambridge Analytica and Facebook: The scandal and the fallout so far. New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analyticascandal-fallout.html

[4] Meinel, C., Broß, J., Berger, P., Hennig, P. (2015). Continent of Docu-Blogs Use Case: The IT-Gipfelblog. In: Blogosphere and its Exploration. Springer, Berlin, Heidelberg. https://doi-org.bucm.idm.oclc.org/10.1007/978-3-662-44409-2_5

The privileged (and most worrying) point of view, with regards the impact of disinformation on democratic processes to check this stage are elections. It is essential to consider these as suffrage, a hard-earned right of people, especially women. In it, we see how some technology-incipient politicians were called by the mermaids' songs of some consultants and data-model agencies to deliver the finest "global election management." They had found that there is no need to shout to a crowd if you can whisper to every voter. Thanks to them, polarisation has overcome, and as chickens come home to roost, others go to Capitols on riot or try to push countries out of boundaries. If we look at citizens as individuals, we have seen some aggressive and emotional online and real-world responses. Those answers may be linked to orchestrated and interested manoeuvres from these factual powers encapsulated in a kind of post-cold war enlargement. Again, old problems with refurbished tactics.

These points collide with the right of free choice, an essential point in elections, as they are finally trying to create new currents of public opinion. That is where regulation comes in handy, and the legislature must understand the problem and their opaque involvements and try to find a balance between freedom and equality.

Policy Implications

The European Union has framed the answer to these information disorders and their relationship with disinformation and its cybersecurity side within The Digital Services Act package[5], mainly split into the services and market ones. In them, we can find a rapprochement to the many issues in play.

One of them is anonymity and individuals' private data (previously isolated in the GDPR and with a new approach in this matter). Data is the new gold, as it can be used to build profiles and use them to make the tailored messages we have already described. Therefore, users must know how and with what intentions they will be used.

Linked with it, we find content and new channels (with serious attention to the so-called very large online platforms). We are no longer talking about isolated social networks but interconnected platforms sharing data among them. It is pretty difficult to make policies for the future; that’s why ground must be settled beforehand.

Being specific, an overall approach to the electoral campaign timeframe must also be defined. As election campaign period is narrow, and response time is also limited, all actors must share and accept rules.

One of the points the policy must deal with is the kind of content the user is exposed to every time. Clearly is not the same when deciding a future government than the first days after the elections. We know that information and opinion are wrapped into the freedom of speech model. Something not so clear is the advertisement one (philosopher's stone of the platform's business model). In it, the act pinpoints when talking about appealing to the vulnerabilities of the recipients. Manipulative techniques are also reflected, especially the profiling one previously defined in the EU Regulation[6]. Data such as ethnicity, political views, or sexual orientation get banned on targeted advertising on online platforms.

Another way to promote a disorder on online platforms is the ways in which information is prioritised and presented. If we were talking about the traditional press, the impact is different if something is on the front page of a newspaper or hidden in between. That clearly can amplify the dissemination of information (or, on the other side, conceal interested information).

---

[5] https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
[6] Article 4, point (4), of Regulation (EU) 2016/679

Providers' Position

This point collides with to what extent providers act as 'mere conduit'. Their design of the system (and, therefore, how their algorithms act) and their role as traders in a bidding model may seem apart general wisdom from this point. To add transparency to this matter, the DSA acts some provisions for these providers:

- **Traders 'information.** By getting this information, users and regulators could have accurate information about the publisher of the information. Companies like Meta already show this data in special moments, like those related to official elections.
- **Additional obligations to manage systemic risks.** To put the focus on the most urgent and essential matters around this matter, the DSA points out in its article 34. c. "(c) any actual or foreseeable negative effects on civic discourse, electoral processes, and public security."

The actions pinpointed to the providers include adapting, reinforcing, and taking targeted measures in several areas to finally protect "any actual or foreseeable negative effects for the exercise of fundamental rights."

Conclusion

May we live in interesting times[7]. The European Union has taken a big step in a massive stock of its Internet live. Not only many of the threats are listed, but also a clever way to handle them with a balance of relationships within the public interest, the private sector, and how law and terms and conditions interrelate.

The limits and cautions could be more precise, especially in a quicksand environment where technology and the way they are created and adopted changes in close steps of time.

Only time will say, once the judiciary and the companies apply this new law if the parliament was proper or new amends must be made. The expectations are enormous.

---

[7] 1936 March 21, The Yorkshire Post, Lesson of the Crisis: Sir A. Chamberlain's Review of Events, Quote Page 11, Column 7, Leeds, West Yorkshire, England. (British Newspaper Archive)

The Policy Brief is published in the framework of the FREuDe project. The project aims to intervene for positive future social change that derives from the commitment and intellectual input across disciplines, such as Sociology, Law, Education, Childhood and Youth studies, European studies and Politics, as well as Communication scholarship and Security studies. Moreover, the Centre addresses the question from the perspective of future autonomous citizens, today's children, and explore closely the ways in which information and Europe feature in their lives.

Jean Monnet Communication, Facts and Regulation for European Democracy (FREuDe) Centre of Excellence

– stimulates new forward thinking with regards the role of facts and place of regulation for securing a future democratic Europe
- generates new research and policy-oriented thinking about integration on the basis of informational rights and enabling informational environments across disciplines not traditionally involved in studying Europe:
- develops new agendas for research, policy and teaching across disciplines and across stakeholder communities
- provides an impetus for future oriented thinking, by researching the needs and perceptions of Europe's future autonomous citizens, young people and in particular children for factual information in and about Europe
- mobilises knowledges and competencies of a range of experts and especially aiming to "hear from" stakeholders which have historically been permitted least input to questions of right to accurate and comprehensive information as a civil and human right.

Jorge Abaurrea is an associate professor in Constitutional Law at the Complutense University (Spain). Author and translator of over twenty books on the Internet, Photography, Twitter, and other digital related topics. He has over 20 years of experience in corporate marketing and communication.

MEDIA GOVERNANCE lab
With the support of the Erasmus+ Programme of the European Union
universität wien