European Parliament
2019-2024

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

12.5.2021

WORKING DOCUMENT

on foreign interference using online platforms – threats, risks and remedies

Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation

Rapporteur: Sandra Kalniete

Without a doubt, online platforms have revolutionised democracy and our daily lives. Whether in personal or professional contacts, access to information, free speech rooms for dissidents or whistle-blowers, or having accessible spaces for discussions about life and society, online platforms have led to immense improvements in almost every area. In addition, many of these services are available to citizens for free or at very low cost. If we consider how they have developed over the last few decades, clearly the women and men who have contributed to this progress deserve admiration.

However, despite all these outstanding achievements, more and more people are losing trust in these platforms or even abandoning them. And they are doing so for excellent reasons. Since the very first meeting of the Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation (INGE), we have heard reports from researchers, whistle-blowers, journalists and human rights activists about how platforms have become useful tools for those engaging in election interference, the creation of disinformation, spreading hate, harassment, the silencing of opponents, espionage and other criminal or deeply wrong and harmful activities.

Very few of those who abuse platforms are ever caught. The sanctions for abusers who do get caught are not severe enough to deter them from trying again. It is clear that current systems, such as the EU Code of Practice, leaves too much room for platforms to do nothing or very little to combat interference in their systems.

The purpose of this working document is to analyse why online platforms make us so vulnerable to foreign interference. I will also suggest a series of measures that could reduce the risks, protect individuals from abuse, increase the costs for perpetrators, and reinstate the trust needed to allow us to confidently use all the aspects of platforms that are beneficial and promote a better society.

We know who the most active foreign actors are and which platforms they prefer to use. However, most of my recommendations would work for any actor and on any platform. Whereas it is clear that the self-regulation approach in the current version of the Code of Practice has not been enough, the upcoming update will hopefully improve it. Legislative work is also ongoing on the Digital Services Act (DSA) and other measures related to the European Democracy Action Plan (EDAP). The aim is to achieve a transparent, detailed and structured accountability system for online platforms. The DSA has great potential, and Parliament's report should be ambitious. However, we should keep in mind that this legislative proposal does not cover harmful content or malicious intent, and many of the measures proposed only cover large platforms. Although the reasons for this are entirely valid, we should look into how to address their potential loopholes.

In this working document, I will not yet specify which measures should voluntary, which are better co-regulated, and which need full-blown legislation. I will closely follow the work in our sister committees and their expected proposals during the following months, and will develop my thoughts further between now and the submission of the INGE report.

I see this working document as an initial risk assessment of our democratic processes. Once we have identified the vulnerable spots of democracy, the next step is to remedy these loopholes, gaps and overlaps. The security dimension should be significantly strengthened in general. This is a responsibility shared by legislators, societies and online platforms. This

cannot be a one-off investigation, but something we need to repeat regularly as society develops. Furthermore, we need to do this together with our democratic partners worldwide. Failure to perform such preventive checks and to fix what is broken will leave platforms wide open for those wanting to hurt our democracies. Moreover, it could lead to us having to stop using many online platforms altogether, which would be a considerable loss for us as society and individuals.

To be clear, this Working Document does not aim to demonise platforms, but to improve their functioning, transparency and accountability, and to strengthen them against malicious interference.

Scope and statistics

Online platforms share certain key characteristics, such as using information and communication technologies to facilitate interactions between users, the collection and use of data about such interactions, and network effects. These network effects make the use of the platforms with the most relevant users most valuable to other users.

Most examples in this working document come from the most prominent platforms such as Facebook, Google and Twitter (including Instagram, YouTube, WhatsApp, Android, etc., that belong to them). This does not mean that links to foreign interference are limited to the most used platforms. Many other platforms have been or could be used for foreign influence operations. Malicious foreign actors pick the platform most suitable for their target audience and disinformation laundering.

Many age groups, nationalities, political communities, socioeconomic, religions, or ethnic groups have their preferred platforms. White-collar workers, especially managers, use LinkedIn and Twitter more than manual workers. Snapchat, TikTok, Twitch and Discord are generally more common among teenagers or young adults than among other age groups. Estonians and Lithuanians are more than twice as likely as Germans to use Facebook on a regular basis. Twitter usage is ten times more widespread in Ireland than Romania, while WeChat is common among the Chinese diaspora. In the US, Parler is popular among Trump supporters.

New platforms constantly appear and grow big, like Clubhouse this spring, while others lose importance, like Myspace.

These different preferences often have natural explanations linked to needs of users, and are not problematic at all in most cases. However, if foreign actors manage to exploit weak points in a specific platform, it could develop into filter bubbles or echo chambers for harmful content, and would affect some segments of the population harder than others.

How the platforms increase our vulnerabilities to foreign interference

During all our meetings, we have seen that there is the will among malicious foreign actors to interfere in European democratic life. Many of our experts have described how foreign actors use online platforms as a tool for this. They have good reasons to do so. The way platforms are designed today includes many features that could be used for interference purposes.

Social platforms collect and store an immense amount of data about each user. Before the age of the internet, few secret services would have dreamed about the collections of detailed, sensitive and private information which platforms have access to for almost any individual. We have seen how this information is used for strategic mapping, micro-targeting and controlling what people say.

The way platforms let malicious actors use personal data to facilitate political targeting or recommend contents and groups, to mention only two examples, would in itself be sufficient grounds for concern. But some characteristics of the online world makes the situation much more worrying. One circumstance is that so much power is concentrated in so few hands. This is due to the small number of popular platforms, and the interconnections between some of the main ones. Therefore, robust and proper implementation of the DMA (Digital Markets Act) could be a possible remedy for this situation. In addition, the lack of safe and user-friendly ways to log in online makes many of us use account details from one platform to log in on unrelated online services. This means unimaginably large amounts of personal data are collected in very few places.

The never-ending succession of leaks, even from large and resourceful platforms like Facebook[1], make the issue of large collections of private data even more alarming. A malicious actor wanting to target, threaten, put pressure on or recruit an individual knows that collections of the most intimate data[2] about them are available and just a few hacks or leaks away. There is a huge illegal data market, which is also shockingly cheap and accessible in the global network[3].

The use of platforms for campaigns has huge advantages compared to offline campaigns. Traditional campaigns involve buying expensive advertisements in newspapers, billboards, TV or radio. They often need to be planned a long time in advance and without knowing how the people targeted react when the message reaches them. In contrast, online campaigns are fast and more affordable. They let you target the people most likely to listen, and allow authors to check whether the campaign is successful, and adjust it if it is not. Some of these features are very useful for society, for instance for dialogue between citizens and their elected representatives. However, malicious actors also take advantage of these features. A common tool for targeting and reaching people is the use ‘sock puppets’, which means fake personas or outlets created to attract the target audience. Like real sock puppets, the audience engages with the sock puppet’s personality, unaware that it is being controlled by somebody else[4].

Many foreign interference activities have the strategic goal of undermining Western democracy. Two standard tactics are promoting polarisation, which makes democratic debates and decision-making more difficult, and undermining trust in institutions. Platforms have a

[1] ‘533 million Facebook users’ phone numbers and personal data have been leaked online’, *Business insider*. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=US&IR=T
[2] ‘I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets’, *The Guardian.* https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold
[3] *Data Brokers and Security*, Nato Stratcom CoE report: https://stratcomcoe.org/publications/data-brokers-and-security/17
[4] ‘The disconcerting potential of online disinformation: Persuasive effects of astroturfing comments and three strategies for inoculation against them’, *The Sage Journal.* https://journals.sagepub.com/doi/full/10.1177/1461444820908530

legitimate business interest in making users want to use their services more and for longer. However, the efforts to make services more attractive to users can also lead to radicalisation and polarisation. We have seen how algorithms promote polarising or strong emotional content at the expense of constructive dialogue, factual content and quality media. For instance, most of the people who join extremist Facebook groups do so after receiving automatic recommendations[5].

Inauthentic actors and activities

Phenomena like trolls and bots make it possible for foreign actors to boost their impact on social media. Anyone interested can easily buy fake accounts or engagements, i.e. views, likes, comments, shares, etc. They can, for instance, use them to twist the debate in a particular direction, which, if successful, can manipulate the reporting of quality media if they perceive this twist as authentic. In parallel, there is also a technique called information laundering[6], which is very often used by malicious actors. In this process, false or deceitful information is legitimised through a network of intermediaries that gradually apply a set of techniques to distort it and obscure the original source.

There is extensive evidence of how foreign actors use trolls to harass or threaten individuals spreading 'unwanted' messages. Many of our guests in INGE are victims of such harassment. The overall goal is to silence critical voices. Too little is done to stop these illegal actions, and the sanctions for the people and organisations behind them are insufficient and rarely enforced. The problem is exacerbated by the fact that currently under international law the right to adopt countermeasures is reserved for the injured state only, i.e. the EU cannot enact collective sanctions.

A further aggravating circumstance is that most legislation has not yet been updated to the digital age. Often, rules concerning offline behaviour are either not implemented online or not suitable for the online environment. This affects all issues - rules on harassment, privacy infringements, hate speech, advertisement regulation or hoax emergency reports.

Many of the experts invited to INGE have witnessed the very low risk of being caught for perpetrators – actors clearly breaching the platforms' own community standards, or even the law. The resources platforms dedicate to monitoring and acting upon external reports are far from enough. We heard about junior employees left with overwhelming monitoring tasks and very little support from their supervisors. NGO representatives bore witness to the difficulties they encounter even contacting and reporting suspected cases of content or actions that are either illegal or in conflict with the community rules the platforms themselves promise to uphold.

---

[5] 'Facebook Executives Shut Down Efforts to Make the Site Less Divisive – The social-media giant internally studied how it polarizes users, then largely shelved the research', *The Wall Street Journal.* https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499?mod=searchresults&page=1&pos=1

[6] *Information Laundering in Germany* https://stratcomcoe.org/publications/information-laundering-in-germany/23 and *Information Laundering in the Nordic-Baltic region*, NATO StratCom CoE reports. https://stratcomcoe.org/news/a-new-report-focuses-on-information-laundering-in-the-nordic-baltic-region/133

Unfortunately, most platforms are still failing to adequately counter inauthentic behaviour[7]. Furthermore, many protective features are available only or mainly in English. Platforms perform worse in detecting and sanctioning abuse in languages other than English, even when the facts are checked and reported. This is the case even for very widely spoken languages like Italian, French, Spanish and Portuguese[8]. The situation is worse for less widely spoken languages, especially those that are not Latin script based, such as Bulgarian[9].

An additional issue not studied in depth in INGE is dependence on foreign technology, both for hardware and software.

When the platforms do act, there is no real right to appeal for the individual or organisation concerned. In conclusion, as designed today, using platforms for foreign interference is easily affordable and effective, and perpetrators do not need to fear detection or deterring sanctions.

Current efforts to improve and strengthen the platforms

Many platforms have voluntarily introduced several measures against interference online. During the first year of the pandemic, platforms pushed authoritative content, downgraded clear dis- and misinformation, and promoted the work of fact-checkers. We regularly receive reports of how platforms close or suspend accounts or networks that break the law or community standards that the platforms themselves promise to uphold. Many platforms have installed specific protection mechanisms for elections and referendums. Again, mainly those consuming content in English and some other larger languages have benefited from most of these measures.

Legislators worldwide have also tried to improve and strengthen the platforms and their users' experience, safety and security. In the EU, the Code of Practice against Disinformation was a first milestone, and is due to be updated in the near future. The Action Plan against Disinformation, the EDAP, the DSA, and expected proposals on political advertising also worthy of mention. Several countries in the EU and beyond have adopted national legislation to protect online platforms and their users from election interference.

It is also essential to recognise the immense work done by the media, civil society organisations, think tanks and universities. We can thank brave and hard-working journalists, researchers and activists for the many insights we have collected during the first part of INGE's mandate. They do an admirable job mapping, preventing, alerting and countering all kinds of interference. Unfortunately, they are often attacked for their findings.

How to strengthen our protection against foreign interference – ensuring fair play in democratic processes

[7] *How Social Media Companies are Failing to Combat Inauthentic Behaviour Online,* NATO StratCom CoE report. https://stratcomcoe.org/publications/how-social-media-companies-are-failing-to-combat-inauthentic-behaviour-online/33

[8] 'Left Behind: How Facebook is neglecting Europe's infodemic', Avaaz. facebook_neglect_europe_infodemic_report.pdf (avaaz.org)

[9] *Bulgaria: The Wild, Wild East of Vaccine Disinformation*, EU DisinfoLab https://www.disinfo.eu/publications/bulgaria%3A-the-wild-wild-east-of-vaccine-disinformation/

Cooperation with democratic allies

When malicious actors try to interfere in democratic processes, it is a problem for everybody who believes in democracy as a system, no matter what our political views are. It is therefore crucial that democracies and democracy defenders work together on these issues. Cooperation across political affiliations inside the EU is essential. Close transatlantic cooperation and cooperation with allies in the rest of the world are also needed. Together, we need to develop common standards of democratic and fair play in the online world. We should also do this in cooperation with civil society and online platforms. The standards agreed should apply globally and on all platforms. The security dimension should also be significantly strengthened, which is shared responsibility of legislators, societies and online platforms.

Investment in research and protection of researchers

To draw the correct conclusions and decide on the most suitable measures, we need facts and knowledge. We need to ensure enough financing for research in this area. Democratic institutions also need proper capacities for in-house analysis and research. We also need to protect researchers better when they face threats and harassment for publishing their conclusions.

Proper sanctions needed to interrupt and deter interference

We need proper sanctions for those who use platforms to break the law, for instance, via threats and hate speech, and for deliberate disinformation campaigns. The platforms should ensure effective sanctions for users who violate the community standards, for example, by deploying large groups of fake accounts, information laundering or other forms of massive manipulation. This should go hand in hand with establishing robust mechanisms to tackle inauthentic activities. Platforms that fail to ensure this basic level of protection need to pay the price.

In terms of sanctions against foreign state actors engaging in interference, the EU could aim to strengthen every Member State and the Union collectively by looking into the possibility of establishing the right to collective countermeasures and solidarity mechanisms.

Using freedom of expression as an excuse to allow threats and harassments

Some people and even politicians state that freedom of expression is a core problem or an obstacle to combating interference via platforms. I disagree. Protecting the same freedom of expression as one of our fundamental rights and freedoms is among the most important reasons why we need to work against foreign interference. However, to preserve these freedoms and rights, we also need to clarify what freedom of expression means and what it does not mean.

Freedom of expression is not the right to get attention using manipulation of algorithms or targeted content. It is also not a right to flood the information environment and drown out all different views with the help of fake accounts and other coordinated unauthentic behaviour. Freedom of expression is something for real humans; fake personas do not have any freedoms or rights. It is not the right to hate or harass anonymously and without consequences – this right must not be used to threaten other people into silence. There is no duty for platforms to publish or amplify hate speech or dangerous disinformation. Platforms are free to give

prominence to quality journalism, authoritative content and verified organisations, and should do so in most cases.

With the quasi-monopolistic situation some leading platforms enjoy today, it is more questionable whether large platforms should be allowed to entirely suspend the authentic accounts of real individuals, even after repeated offences. The most famous and much criticised example is when Twitter suspended the account of the then sitting US president, Donald Trump[10], arguing that his tweets about the Capitol Hill attacks breached Twitter's rules on 'glorification of violence'.

Everybody should enjoy the same protection as users of English

To adequately protect our democracies, it is crucial for the level of protection against interference not to be linked to the language used. We cannot accept a situation where the protection against disinformation, arbitrary takedowns, hate speech and other kinds of interference depends on language. Platforms should ensure they employ enough staff competent in the languages used on them. A lighter regime could be considered for very small platforms or start-ups, while at the same time evaluating their impact and potential. However, as a general rule, online platforms should invest in linguistic competence everywhere they have a sizeable number of users.

The number of measures currently taken by platforms on preventing spreading disinformation depends on commercial data and the number of users. However, since platforms today are much more than simple business entities, they should consider the level of threat and geopolitical situation of each country.

Individuals, institutions and researchers, should be able to contact platform representatives easily and quickly, not just through standardised communication via online forms.

Reducing vulnerabilities linked to collections of personal data

Control and ownership of personal information should stay with individuals. Platforms have access to vast amounts of detail and sensitive data about individual users. There needs to be a balance between, on the one hand, enabling the platforms to run their businesses for profit, using, for instance, effective advertising and targeting or addictive algorithms, and protecting privacy on the other. Moreover, abundance and insufficient security of storage has already created larger scale security issues.

A specific vulnerability is linked to the data broker industry. Data brokers take advantage of all the traces we leave online when we use apps, media, GPS and other services. They collect, aggregate and trade this data for commercial gain in a relatively unregulated digital space with little transparency. The data brokers' customers use the data for targeting groups or individuals. This practice can create difficulties for the individuals targeted, and become national security threats when malicious actors, such as hostile states or terrorist groups, get their hands on the data. Data brokers have access to too much data, which they often store in an insecure way. There is little or no oversight or control of how data sold by brokers is used by their customers. We need to remedy all of this. Even though we sometimes have the option

[10] Permanent suspension of @realDonaldTrump Twitter account https://blog.twitter.com/en_us/topics/company/2020/suspension.html

not to share our data, the procedures for doing so are often annoyingly repetitive and time-consuming. For many of these critical decisions, platforms do not offer us a real choice to use their services without being profiled and targeted. The message we get is 'take it or leave it'. The quasi-monopolistic status of many platforms and the way they are designed makes the price we need to pay for the 'leave it' option very high.

For instance, I cannot join a group of Facebook-connected friends without myself being a full user of Facebook. Neither can I send a message via a messaging app to a person who is not connected to the same app. However, outside the internet, it is perfectly possible to make a phone call to someone who uses a different phone provider or to join a club without agreeing to surveillance and targeted advertising. There need to be ways to decouple the different functions of the platforms in order to reduce the amount of collected information available, which constitutes a vulnerability as it can be used for all kinds of malicious targeting.

There is also a need to limit the kind of data about us that platforms can collect and store and how long this data can be used. In 2014, the Court of Justice of the European Union declared the 2006 Data Retention Directive invalid[1], arguing that blanket data collection violated the EU Charter of Fundamental Rights, particularly the right to privacy. The data that platforms collect and store about any one of us, often without us understanding its scope, exceeds what was considered excessive in the Data Retention Directive by many orders of magnitude. We need to set some limits this.

Some sensitive information, such as sexual orientation and preferences, religious beliefs, political values, place of residence, health, private economy and habits, need more robust protection against targeting, transfer to third parties and leaks. The same goes for micro-targeting about sensitive issues, such as political decisions. This practice should be limited or banned.

More robust protection should also be the general rule for content targeting children and other vulnerable groups. Platforms and applications considered safe or trust spaces, like messaging, health, finance and dating apps and small discussion groups, need more robust protections against hacks and leaks. Platforms must ensure adequate protection of sensitive data. If they neglect this duty, they should be held responsible for leaks.

Platforms should regularly inform their users about how they collect and use user data, and do so in an easily understandable format. After reading this information, users should have real options to opt out.

Fixing the algorithms

Algorithms are essential parts of the platforms' business models. We need much more transparency about how they work. We need to shine a light into the black box of algorithms. Researchers should have meaningful access to information about algorithms while fully respecting the users' privacy.

It is also clear that platforms need to correct the balance between the business-motivated urge to make people stay longer on platforms by feeding them with engaging content, and a responsibility to promote quality content. Platforms need to ensure that their algorithms do not one-sidedly promote illegal or extremist content. Especially for political content, platforms need to make sure that their algorithmic choices do not lead to radicalisation but

that they offer users several different viewpoints. We heard examples about how nudges can be used: they are encouragements to rethink the wording before posting if violent or strong language is being used. This could be further developed.

Furthermore, platforms should be required to modify algorithms to demonetise and deprioritise content from inauthentic accounts and channels that are artificially boosting the spread of harmful disinformation. The current mechanisms for de-prioritisation and shadow-banning (blocking or partially blocking a user) can be easily circumvented. These mechanisms could be strengthened by capping engagement, i.e. disabling the option to favour/'see first' content from accounts, pages and channels that frequently spread disinformation.

There needs to be systematic scrutiny of the consequences of algorithms. This could be done by a supervisory authority (covering both EU and national levels), which would also involve representatives from the industry, civil society and others. Such a body should also look into whether platforms can uphold the guarantees promised in their respective community standards, and whether they allow large-scale coordinated inauthentic behaviour to manipulate the content on their platforms. To sum up, we must aim at a detailed, structured and transparent accountability system.

Advertising mechanisms should not fund disinformation or radicalise target audiences

Advertising policies and methods should be reviewed to address problems such as advertising revenue going to extremist and polarising content at the expense of quality content of benefit to citizens. In general there is a severe lack of transparency in online political advertising. We may want to consider introducing industry-wide minimum standards on the monetisation of disinformation content.

To avoid foreign interference in democratic elections, measures to limit foreign actors' possibilities to place political or issue-based advertisements could be considered, as long as they do not put obstacles in the way of genuine cross-border events such as the EU elections. Candidates standing for election to the European Parliament must, for instance, have the right to run a campaign in the country where they wish to be elected, even if they are not a resident of country during the campaign.

Special measures are needed to remedy the democratic consequences of differences in prices being used to politically target different socioeconomic groups[11]. Whereas segmenting in income groups can make sense for commercial advertising, it should not be cheaper to create political influence operations targeting more impoverished people.

Work harder against online threats and harassments

It is of the utmost importance to strengthen the measures against harassment, threats and hate speech online. These illegal practices threaten freedom of speech and democratic debate as a whole if they scare people into silence. Platforms need to step up their abilities to remove

[11] 'Facebook Charged Biden a Higher Price than Trump for Campaign Ads*', The Markup*. https://themarkup.org/election-2020/2020/10/29/facebook-political-ad-targeting-algorithm-prices-trump-biden

such content and protect the victims. Since threats and harassment are illegal offline, they should not be allowed online. Platforms failing to act on this should face sanctions.

Right to appeal

To avoid increased responsibility to remove illegal and dangerous content leading to arbitrary removals of legal content, users whose accounts or content are removed should have the right to appeal and the right to have their complaints dealt with promptly.

Transparency and anonymity

It is essential to be very transparent about the origin of online content and the real organisations behind accounts. Several initiatives already exist and could be developed further. For messaging apps, the most important priority is to respect the privacy of users. However, some initiatives could increase transparency, such as the 'forwarded' label in WhatsApp indicating that a message has been forwarded and not created by the person who sent it.

Platforms also need mechanisms to detect and suspend fake accounts linked to coordinated influencing operations. Whereas verification could be considered in many cases, demands for proof must protect anonymity for persons in vulnerable positions. Therefore, the question of closed messaging groups should be considered from different angles. On the one hand, they may themselves be sources for the spreading of disinformation and other harmful or manipulative content, but on the other they can also be one of the very few ecosystems for whistle-blowers and dissidents in authoritarian countries.

Media literacy and awareness-raising

To build up their general resilience, democratic countries need to invest in media and digital literacy for all age groups, starting at schools and other educational bodies. This should not be a one-off information campaign, but different parts of the government could raise awareness about the risks linked to foreign interference in their respective areas on a continuing basis. The first step is to increase awareness about threats among staff in strategically essential institutions and people in sensitive functions. Where relevant, this can be combined with training in strategically important languages.

To facilitate contacts with citizens, democratic institutions should be present on the major platforms and available for dialogue.

Update legislation and co-legislation to the digital age

Finally, and no less importantly, we need to review current legislation on a permanent and regular basis at all levels, and in areas such as advertising, hate speech and harassment, data protection, competition, and rules for funding to identify where an update to the digital environment is needed. This screening exercise needs to take into account the latest developments in foreign interference.