Disrupting Disinformation:

A Global Snapshot of Government Initiatives

www.disinformationindex.org

Authors: Craig Fagan and Aaron Sugarman

Design: www.designbythink.co.za

The Global Disinformation Index is a not-for-profit organisation that operates on the three principles of neutrality, independence and transparency. Our vision is a world free from disinformation and its harms. Our mission is to catalyse industry and government to defund disinformation. We provide disinformation risk ratings of the world's news media sites. For more information, visit www.disinformationindex.org.

GDI Global Disinformation Index

Table of contents

Section 1: Introduction

Disinformation is a global problem not contained by borders. The online ecosystem that encourages and financially rewards the creation of harmful content is a worldwide phenomenon.

Different countries have taken varied approaches to address the problem of disinformation, but few have taken an approach to cut the funding sources of peddlers of disinformation.

By briefly examining the current legislation of 12 countries, GDI has found that disinformation is gaining more policy attention. But there are significant gaps in the approaches of these governments that need to be addressed.

The 12 countries included in the scope of this study are: Argentina, Australia, Brazil, Canada, France, Germany, India, Italy, South Africa, Spain, the United Kingdom and the United States. GDI also provides an analysis of policy efforts by the European Union (EU), of which four countries in the study are members.

As GDI has argued,[1] regulating disinformation does not need to be a trade-off with ensuring freedom of expression or providing freedom of information. People have a right to say what they want as allowed under law, but not to profit from or amplify what they say. Unfortunately, GDI's findings from the policy mapping in this study show that current regulatory efforts in the 12 countries do not adequately address the financial incentives or amplification of disinformation.

This study notes that:

- Every country in the sample, except South Africa, has created an official policy that focuses on fighting election-related disinformation, although these are usually limited to the electoral cycle.
- Ten of the 12 countries have restrictions against hate speech, including some new proposed initiatives in Canada and the UK.
- Over half of the countries have set up an interagency disinformation task force, although the remits and focus of the respective task forces vary.
- Three-fourths of the countries in our sample have some type of penalty – monetary or otherwise – for infractions related to spreading disinformation.
- No country has adopted regulations to demonetise disinformation, although one country (Australia) has a voluntary code of practice that includes such regulations.

Disinformation will continue to be funded by profits from online advertising until governments join together to remove the financial incentives for peddling harmful content. The aim of this policy briefing is to call attention to this shortfall and the need for a regulatory response, as the European Union is currently proposing (see Box 1).

GDI firmly believes that, to combat disinformation, there should be a common "regulatory floor" that covers online advertising and monetisation platforms. These monetisation channels incentivise the spread of and engagement with content that disinforms. A common regulatory floor would set the minimum regulatory obligations for online advertising and monetisation platforms, including for reporting, impact metrics and penalties or sanctions. Such a comprehensive approach is the best policy solution to ensure a coordinated, inter-jurisdictional response to demonetise disinformation.

Section 2: Findings

Over the past six months, GDI has assessed 12 countries across all regions to determine the nature and extent of current initiatives being pursued by these governments to curb disinformation (see Table 1). These countries were selected based on their previous challenges with disinformation and GDI's past risk assessments of their media markets.[2] These countries also represent a good cross-regional sample of large, established and growing digital media environments. It is a sample of countries that represents nearly 1.7 billion internet users,[3] including three of the top five countries with the most internet users.[4]

To assess each country, GDI decided to focus on policy actions in five areas:

1. Electoral disinformation

2. Hate speech disinformation

3. Ad-funded disinformation

4. Interagency task force

5. Non-compliance sanctions

The findings from this assessment are found in Table 1 and also Annex 1 to the report (which provides a standardised overview of each country).

Table 1. Current government policies to combat disinformation: coverage areas

Country	Elections	Hate speech	Advertising	Interagency task force	Non-compliance sanctions
Argentina	✓	✗	✗	✗	✗
Australia	✓	✓	✓	✓	✓
Brazil	✓	✓	✗	✓	✗
Canada	✓	✓	✗	✓	✓
France	✓	✓	✗	✗*	✓
Germany	✓	✓	✗	✗*	✓
India	✓	✓	✗	✗	✓
Italy	✓	✓	✗	✗*	✓
South Africa	✗	✓	✗	✓	✓
Spain	✓	✓	✗	✓	✗
United Kingdom	✓	✓	✗	✓	✓
United States	✓	✗	✗	✓	✗

**Note: While Germany, France and Italy do not have an individual disinformation task force for their respective countries, there is an EU-wide disinformation task force.*[5]

The following findings were compiled from a review of these metrics across all the countries in the sample. For each country, the institutions, legislation and policy gaps were reviewed as part of assessing these five areas. All findings are based on a desk review of existing research and analysis of the regulatory and policy frameworks in place in each country. These are referenced where relevant under each country section (see the Annex). In addition, GDI engaged with local experts in each country to ensure that this overview correctly represents the current state of play of country-level policy actions.[6]

GDI considers this cross-country analysis a useful contribution to efforts to combat disinformation. While doing this analysis, GDI did not find any recently completed policy comparisons similar to what is provided here. GDI hopes that this succinct analysis helps to further more cross-comparison work in this area.

Electoral disinformation

Through this review, GDI noted the existence in nearly all 12 countries of policies to address disinformation in an electoral cycle, including prior to, during and after elections. We found that in all countries, except South Africa,

there is some form of voluntary or mandatory regulation, particularly as a set of ad hoc measures targeted at a specific election or only in operation during electoral cycles.

These measures are largely instituted to protect the integrity of electoral processes and democratic institutions. Italy, for example, proposed a new bill in 2017 that aimed to establish rules for digital platforms to combat "false news" aimed at electoral interference (the bill has not been passed). In Spain, prior to its 2019 general elections, a highly controversial Royal Decree-Law 14/2019 was published to expand government control of the internet and electronic communications, including during elections.

Overall, only three of the countries (France, India and Spain) have passed specific anti-disinformation legislation, which also covers elections. These initiatives are often called "fake news laws", which are intended to protect electoral processes from "false" information about the process, candidates and/or parties. Brazil is currently tabling such a measure. However, in cases where the rule of law and checks and balances may not be strong, there is a risk that these regulations could be misused to actually undermine democratic processes, limit freedom of expression and suppress opposition parties and voices challenging the current government during an election.

Hate speech disinformation

GDI assessed whether hate speech is regulated in a country in order to understand whether disinformation – which is increasingly being classified as "lawful but awful" – is addressed indirectly or directly by such legislation. Hate speech is relevant given its extensive overlap with disinformation narratives and the harm that both of these produce, both online and offline.

Different countries in our sample have taken different approaches to hate speech regulation, which in some cases does not include disinformation. In Germany, for example, hate speech is illegal and is regulated online. While these measures are not explicitly formulated to combat disinformation, it is indirectly covered. In the UK, the Online Safety Bill, which has been presented as a draft to Parliament, is intended to regulate illegal and harmful but lawful content online, including disinformation. Canada has just introduced measures to modify existing legislation to combat online hate speech, but not as part of tackling disinformation. In the US, there are current efforts in Congress to reform Section 230 of the Communications Decency Act (1996), which shields online platforms from civil liability for third-party content published on their service, such as hate speech or disinformation.[7] Yet in France, attempts to regulate online hate speech have been largely struck down in the courts.[8] In Italy, criticism and media coverage of a move to regulate online hate speech resulted in the legislation never being formally presented.

While hate speech regulation can help to address disinformation, there is a risk that this legislation is still too limited in scope to deal with the cross-platform nature of disinformation without having consequences for freedom of expression and free access to information.

Ad-funded disinformation

GDI examined whether existing government policies address the financial incentives of disinformation, including online advertising. Advertising on disinformation sites results in harmful content generating revenue. Content that triggers a strong emotional reaction tends to get the most clicks – and earns more advertising revenue. GDI conservatively estimates that a quarter billion dollars' worth of advertising globally goes to sites flagged as disseminating disinformation.

Despite this challenge, no country currently has specific regulations aimed at curtailing the funding streams that act as financial incentives for producing and publishing disinformation. The overall lack of this regulatory coverage across the sample of countries will continue to leave open a back door and provide a monetary incentive for disinformation actors to create, spread and monetise disinformation. No country has yet attempted to regulate online advertising (although there are some proposed bills in the US that, if approved, would do that).[9]

Only one of the countries in this study has some form of limited voluntary policy to tackle ad-funded disinformation: Australia. The Australian government worked with the local digital industry body to develop and adopt a Code of Practice on Disinformation and Misinformation. The code was launched in late February 2021.[10]

The general lack of policies to defund disinformation could change, however, with the updating of the EU Code of Practice. This code will require relevant signatories to improve their advertising and ad-placement systems to defund disinformation across the region (including four of the countries covered by this study).

Interagency task force

GDI looked into how governments were tackling the cross-sectoral nature of disinformation through ad hoc, interagency committees that work across government institutions and bodies. Task forces of this nature can help governments to leverage an array of inter-institutional expertise and approaches needed to effectively design, develop and deliver policies aimed at disrupting disinformation.

Many of the task forces that we studied had a specific focus on elections and combating foreign interference. The Canadian government, for example, created a task force composed of 12 government bodies to secure the integrity of the 2019 Canadian elections and which will be put into service for all future elections.[11] In the US, the Global Engagement Center (GEC), housed under the US State Department, was created in 2017 by the National Defense Authorization Act. The GEC is tasked with coordinating interagency efforts to counter foreign propaganda and disinformation (and more recently with investigating COVID-19 disinformation).

Still, the interagency task force model to combat disinformation is not in place in all countries in this study, including Argentina, France, Germany, India, and Italy. The German government, for example, has a cross-government task force on hybrid threats (including disinformation) but not a specific task force

to combat disinformation as a hybrid threat (which is how the GEC is set up in the US).[12] In Argentina and India, there are no institutions or task forces that are set up to work on disinformation across government institutions (outside of the regulators who look at the tech sector for compliance issues).

Non-compliance sanctions

GDI assessed whether and how sanctions were being used by the countries in the study as an accountability mechanism to enforce their anti-disinformation measures (whether voluntary or legally binding).

Voluntary frameworks, such as the codes of conduct adopted in Australia and South Africa (and the EU), are fairly new and have only recently been assessed by regulators. When it comes to enforcing legally binding regulations, the countries in this study tend to devolve enforcement to their ministries of justice, their telecommunications regulators and/or their competition regulators. In a few cases, the press bodies also have the ability to issue sanctions against members, such as in Germany and the UK.[13]

In terms of country examples, Germany has tasked the German Federal Office of Justice with levying fines for the violation of laws related to disinformation, including platform obligations under the Network Enforcement Act (NetzDG). Similar to Germany, many other countries in this study use their penal code to enforce sanctions. Argentina's Penal Code outlines crimes against the public order and of publicly inciting collective violence, which are punishable by imprisonment and/or fines if the actions are intentional. France's Penal Code has similar language and sanctions, in the form of fines, for defamation and "false news" (when it is done in bad faith). Brazil's Penal Code punishes people who falsely accuse others, whereas Italy's Penal Code also addresses defamation and imposes fines on those who publish or disseminate "false, exaggerated or tendentious news which is likely to disturb public order". South Africa has imposed temporary measures due to the COVID-19 pandemic. These measures criminalise fake news about COVID-19, and worryingly to some organisations, also forbid criticism of the government's response to the pandemic.

In terms of regulators, it is expected that once the Online Safety Bill in the UK is adopted, it will be enforced by the Office of Communications (OFCOM), the UK's regulatory body for the broadcasting, telecommunications and postal industries, to fine companies that fail in their new "duty of care".[14] In the US, the Federal Communications Commission (FCC) prohibits broadcasting false information that could cause significant public harm. It may act on complaints, through sanctions and fines, if broadcasters intentionally distort the news. In France, the country's main broadcasting regulatory agency, the Conseil supérieur de l'audiovisuel (CSA) is responsible for investigating French disinformation and enforcing platform transparency measures.

BOX 1. The European Union: efforts to combat disinformation

At present, three key regulatory initiatives have been proposed to combat disinformation across the European Union: the Digital Services Act (DSA), the Digital Markets Act (DMA) and the EU Code of Practice on Disinformation, a voluntary regulation.

- The goal of the Digital Services Act is to create a safer digital space in which the fundamental rights of all users of digital services are protected and to promote innovation within the EU and globally. When passed, this Act will issue a common set of regulations for intermediaries within a single market.
- The sister legislation to the DSA is the Digital Markets Act. The DMA will require new transparency obligations and a regulatory framework for ad tech and other online monetisation companies operating within the EU. If approved, online advertising platforms and services, for example, will be required to provide information related to their advertisers and publishers, including pricing.
- The EU Code of Practice is a "soft" law mechanism that encourages[15] signatories to include requirements to address the monetary incentives of disinformation. The EU code is similar in scope to the Australian one and has some common language when discussing issues related to disinformation. However, the EU code is administered by the European Commission and not by a trade body.

In addition to these three initiatives, the EU Democracy Action Plan (EDAP) is a non-regulatory framework that outlines areas where regulation is needed to address specific challenges to the democratic systems in the European Union and its member states. Among the areas it covers is the need to counter disinformation (and to disrupt the financial incentives supporting disinformation).

The European Union has taken the lead in proposing policy frameworks and regulations that combat disinformation through a whole-of-industry approach, which also targets removing the financial incentives of disseminating online disinformation.

There are still a few areas where the EU's current legislation could be strengthened. Both the Digital Services Act and the Digital Markets Act are currently under consultation at the European Parliament and with member states. Both Acts will undergo amendments that could strengthen how they address disinformation – or weaken these components of the legislation. The next 12 to 18 months will be critical for better understanding how this regulation will look compared to the current drafts proposed by the European Commission.

Section 3: Conclusion

Governments around the world have all taken different approaches to addressing the growing online and offline harm caused by disinformation.

This study is an attempt to compare these approaches in order to learn from other countries' experiences to disrupt and defund disinformation.

One of the key conclusions is that measures to counter disinformation often lack a focus on the financial incentives that promote and allow the peddling of disinformation. As GDI has argued, it is essential to remove these financial incentives if the disinformation ecosystem is to be disrupted. Current "soft" regulatory measures that address ad-funded disinformation, such as the voluntary code in Australia, are still too nascent to determine whether platform signatories will adequately adopt measures to address the funding of disinformation. If the list of current signatories to the Australian code is any indication, it would seem not to be the case. Key players like Amazon, Stripe, eBay, Etsy, and PayPal are visibly absent among its signatories.

Moreover, sanctions are currently a mixed bag – either too light or too harsh, creating concerns over their effectiveness. Eight of the countries in our sample have some type of penalty against creating disinformation and over half have instituted a disinformation task force.

The issue of how governments institute legal structures and sanctions to combat disinformation signals a broader challenge: the tenuous balance of creating policies that effectively combat disinformation while not infringing on one's right to freedom of expression and information. Policies that tackle the financial incentives encouraging disinformation are able to avoid some of these difficulties because they respect people's freedom of expression while taking aim at how disinformation is algorithmically amplified and/or monetised.

In the midst of the current infodemic it is more important now than ever that countries across the globe take common steps to demonetise and disrupt disinformation. This report shows the current lack of a "regulatory floor" and consistent gaps in and among many governments. The GDI hopes that these findings will lead to the establishment of minimum obligations for online advertising and monetisation platforms to defund disinformation – and make the internet a safer place for all.

Annex: Country profiles

This section provides a brief overview of how different countries are pursuing policies to combat disinformation.

In total, 12 countries are assessed from across all regions: Argentina, Australia, Brazil, Canada, France, Germany, India, Italy, South Africa, Spain, the United Kingdom and the United States. In addition, we include a policy profile of the European Union (which includes four of the countries in our assessment) to highlight the region's current groundbreaking efforts to combat disinformation. Each country analysis outlines current policy efforts undertaken to combat disinformation and identifies areas where coverage gaps exist.

Argentina

Institutions

Currently, there are limited government bodies addressing disinformation in the country. The institutions that do exist are related to combating disinformation during elections. The National Court of Elections in Argentina (CNE), for example, works to fight electoral disinformation by engaging with press associations, digital platforms and political parties to protect the accuracy of information they disseminate. The CNE is tasked with circulating informational campaigns that digitally educate voters 30 days prior to an election. It also ensures that the identity of individuals purchasing political advertising is made public. Political parties, press associations and digital platforms in Argentina have signed an agreement on digital ethics with the CNE. This action was motivated by concerns over disinformation on social media before the October 2019 presidential election.

In terms of regulatory authorities, the National Communications Entity (ENACOM) is the national communications and media regulator. Among its duties, ENACOM publishes an online repository of websites that have been blocked or reinstated (or both) after judicial court orders, but does not specify the criteria or rules behind decisions. The majority of blocked sites, however, are related to illegal gambling. ENACOM has also published public statements regarding "fake news", such as claims related to COVID-19.

Legislation

There is no legislation on disinformation or online hate speech. Legislation of that nature has been used as a complementary legal framework in some of the other countries in this study. Recent attempts to penalise disinformation have sparked controversy due to the incorrect assessment of information as false[16] and criticism that the government is potentially infringing on press freedom.[17]

The legal frameworks that do exist prioritise freedom of expression and the press, although the country's media has been under pressure in recent years despite these protections. The country's Supreme Court has determined that restrictions must always be interpreted narrowly. A 2020 court case reversed the decision to remove sexual abuse allegations against a former public official, citing freedom of expression. The Argentine Penal Code outlines crimes against the public order, publicly inciting collective violence, and intentionally disgracing or dishonouring an individual.[18]

Policy gaps

Argentina's approach is distinctive in this report because it primarily enacts policies that attempt to educate people about elections and the harm of disinformation through the CNE.[19] These efforts, however, are still weak and could be strengthened with further initiatives.[20] Even though media literacy programmes are likely to be beneficial in the long-term, the current Argentine policy lacks some of the platform-regulation measures of other countries included in this report and does not address how funding and amplification mechanisms foster disinformation.[21] Similar to the situation in the US (see the US report section), the required regulation would entail a cross-party consensus that has until now proved elusive.

Australia

Institutions

Australia has had a multi-pronged policy response to combating disinformation. Domestic security issues in relation to disinformation are addressed by the Homeland Minister of Australia. This ministry has the responsibility for the country's internal affairs and national security. As such, the Homeland Minister has jurisdiction over combating domestic and foreign disinformation campaigns.

On areas specific to disinformation ahead of and during Australia's elections, an Electoral Integrity Assurance Task Force was set up in 2018. While its primary concern has been cybersecurity, it also monitors disinformation. The task force was used during the 2019 full federal election and continues to support other Australian electoral management bodies. In addition to the task force, the Australian Electoral Commission has also supported work to combat disinformation and misinformation during elections.[22]

There are also various other actors in the Australian government that foster broader online safety. The eSafety commissioner in Australia is able to investigate illegal and abhorrent violent material that is online and can act on complaints related to cyberbullying. The Cyber and Critical Technology Cooperation Programme works to counter disinformation by providing online training, advisory support and knowledge exchange to government officials and civil society. In April 2021, they launched a project targeted at countering COVID-19 disinformation through knowledge-sharing and training for their partners in Southeast Asia.

The Australian Communications and Media Authority (ACMA) regulates communications and media in the country, including disinformation. ACMA put in place a voluntary Code of Practice on Disinformation, similar to what has been done in the European Union. However, an industry body, DIGI, has been tasked with the code's development and implementation. DIGI is a non-governmental organisation representing the tech industry in Australia. As such, some organisations in Australia have criticised this decision.

Legislation

In 2018, the country passed the National Security Legislation Amendment, which instated a list of offences for any person(s) attempting to influence Australia's election or democratic process on behalf of a foreign government. This law can be used to prosecute those who engage in disinformation campaigns in Australia under the auspices of foreign governments.

In terms of "soft" regulation, an Australian Code of Practice on Disinformation and Misinformation was launched in late February 2021. As noted, the code was adopted and is to be implemented by the tech industry body, DIGI. The code consists of seven major commitments and addresses disinformation in advertising and paid content. It stipulates that signatories will implement policies that disrupt the monetary incentives for creating and disseminating disinformation; however, it does not enforce specific actions. Code signatories include major online platforms such as Twitter, Google, Facebook, Microsoft, Redbubble and TikTok.[23] The listed signatories have released transparency reports about how they are upholding their commitments under the code.[24] To date, key monetisation platforms such as Amazon, eBay and PayPal have not signed the code.

Policy gaps

These initiatives show that the Australian government is taking some steps to combat disinformation, both through law and policy. However, there are concerns that passing the Code of Practice to an industry body to develop and implement may cause a weakening of the code.[25] Only as the code is rolled out will observers be able to assess whether this has been the case. The Australian code should also consider aligning with the EU Code of Practice (see the EU section of this report), both in terms of its coverage and its signatories (Australia's code has a wider array of signatories but they do not fully overlap).[26]

Brazil

Institutions

So far, efforts have focused on disinformation during Brazil's electoral processes. The Superior Electoral Court, the highest body of electoral justice in the country, has attempted to target what it terms "fake news" in political advertising. They have also hosted debates on fake news and elections and launched a programme to tackle disinformation in 2020.[27] In addition, they have backed a task force created by Brazil's federal police ahead of the 2018 national election. This task force focused on taking down electoral disinformation.[28] The government has faced criticism for referencing laws created during the dictatorship, concerns over censorship and a vague definition of "fake news".

The National Telecommunications Agency, commonly known as Anatel, serves as the telecommunications regulator in Brazil, including for the internet. Anatel's responsibilities include promoting competition, protecting consumer rights and ensuring the quality of telecommunications services.[29]

Legislation

The legal framework in Brazil has aimed to balance freedom of expression with the emerging challenges of the online environment. Until now, these measures have fallen short of addressing online hate speech and, relatedly, disinformation and misinformation. A new proposed law attempts to close this gap, but it has been criticised for proposing highly controversial regulations that could negatively affect the freedom of the media in Brazil.

Freedom of expression is protected under the Brazilian Constitution (1988). However, Article 5 of the Constitution states that "the law must punish any discrimination attacking fundamental rights and liberties". While there is no legal definition of "disinformation" in Brazil, it has been argued that individuals could be prosecuted for related violations using either the country's Penal Code, which punishes people who falsely accuse others, or through the electoral code, which prohibits advertising meant to slander, defame or injure any person or entity exercising public authority.

In 2014, Brazil became one of the first countries globally to institute a law that outlines the principles, rights and duties of online users. Users' rights include the right to online privacy and the respect for human rights online. However, the law, known in Portuguese as the Marco Civil, does not specifically address hateful content online, nor content that might negatively affect minority and protected groups in the country. It also does not mention disinformation, misinformation or "fake news".

While the country has not had specific legislation targeting the content of any media platform, Brazil is now in the process of passing a controversial "fake news" law. The controversy surrounding the law brings to a head the delicate balance between disinformation and free speech. The Law on Freedom, Responsibility and Transparency on the Internet, known popularly as the "Fake News Law", was introduced and approved by the upper house of Congress in June 2020, but it has been held up in the lower chamber, the Chamber of Deputies. One possible reason for the delay is the outcry by local and international organisations over concerns that it will lead to censorship and human rights violations.[30]

The proposed law has also been criticised for its hurried legislative process and consultation, in marked contrast with the Marco Civil, which had an extensive period of consultation (including with international actors) and resulted in the guarantee for all Brazilians of their freedom of expression online.

In September 2021, President Bolsonaro issued a decree to restrict the powers of online platforms to remove accounts and content, including those flagged for sharing misinformation and disinformation. Under the decree, which has not been fully published, platforms must provide "just cause and motivation" before removing an account for disinformation.

Policy gaps

The concerns over Brazil's "Fake News Law" signals the need for regulations targeting disinformation to move beyond a true–false binary. Brazil's current internet rights law (the Marco Civil) could be strengthened by

addressing the issue of disinformation and holding platforms accountable for algorithmic processes that amplify and monetarily reward harmful content. Furthermore, Brazil could also institute guidelines for relevant companies to have transparent, comprehensive and enforced policies regarding disinformation and advertising.

Canada

Institutions

Currently in Canada, there is no standing body or institution set up to deal with general threats of domestic or foreign-driven disinformation.

However, there is a task force that addresses such issues during Canadian elections. In 2019, the Canadian government created a task force to monitor disinformation attempts and notify other agencies and the public accordingly at election time. The mandate of this task force, which brought together the 12 bodies of government, was to secure the integrity of the 2019 Canadian elections and prevent foreign interference through an established process known as the Critical Election Incident Public Protocol (CEIPP).[31]

The task force was created to ensure that the Canadian civil service rather than politicians oversee the issue of disinformation.[32] The actions and efforts of the CEIPP and its related task force have formed the basis of Canada's current policy on disinformation and both mechanisms are to be activated during electoral cycles.

In addition, the government has set up the Digital Citizen Initiative to foster resilience against online disinformation by supporting researchers and funding innovative research projects focused on promoting a healthy information ecosystem, algorithms and artificial intelligence.

Finally, different Canadian institutions work internationally on efforts that target disinformation. Global Affairs Canada, for example, runs a G7 mutual assistance team to mobilise resources in response to disinformation attacks from foreign interference across the member state group. In addition, members of the Canadian Parliament's Standing Committee on Access to Information, Privacy and Ethics (ETHI) have been involved with the international grand committee on disinformation (IGCD) and in advocating for more advertising and algorithmic transparency.

Legislation

There are currently no regulations or policies in Canada that address disinformation or harmful content online. However, some measures have been proposed to set up such a framework.

After the 2019 federal election, the Canadian government issued a mandate that the Minister of Canadian Heritage would be tasked with developing regulations on hate speech content. It was recently announced jointly by the Minister of Canadian Heritage, the Minister of Justice and the Attorney General that modifications to existing legislation and new forthcoming regulations will cover online hate speech but not disinformation.[33]

Other previous actions taken by the Canadian government include passing Bill-C76 in 2018, which attempted to implement increased transparency about political advertising on social media. However, elements of C76 were declared unconstitutional because of free-speech concerns and how the bill would be applied to false statements.

In May 2020, Canada also launched a digital charter, which includes provisions on disinformation and social media. The government has used the charter to call upon social media companies such as Microsoft, Facebook, Google and Twitter to commit to promoting transparency, authenticity and integrity on their platforms. The digital charter also requests regularly published transparency reports by the platforms (similar to what has been done elsewhere). However, it seems that these reports have not been published yet.[34]

Policy gaps

The current legal updates to tackle hate speech and set up a regulatory framework for online harm is positive, but falls short for not including disinformation as part of its focus. Moreover, Canada's current efforts are not focused on the funding and monetisation networks that incentivise and fuel disinformation, such as online advertising. A more comprehensive policy response in Canada could include embedding such measures in an industry-wide code of conduct on disinformation to accompany the proposed legislation.

France

Institutions

The main institution in France tasked with regulating disinformation in the media is the broadcasting regulatory agency, the Conseil supérieur de l'audiovisuel (CSA). The CSA is responsible for investigations into French disinformation and for enforcing platform transparency measures. Online platforms, for example, are required to submit yearly statements to the CSA, stating what actions they have taken to combat disinformation. The CSA is then responsible for publishing frequent reports on these measures and for assessing their effectiveness. Another power of the CSA is that during elections, it can suspend the broadcasting licences of any foreign-owned media operator if it broadcasts disinformation, including through the internet, that could affect French elections. There is also a provision for the CSA to be able to do this outside of election periods if the disinformation poses a threat to national interests.

In terms of foreign influence during elections, two French government agencies have been tasked with powers to combat electoral disinformation: the National Commission for the Control of the Electoral Campaign for the Presidential Election (CNCCEP) and the National Cybersecurity Agency (ANSSI). In the past, the CNCCEP and ANSSI have worked together to educate French presidential candidates' campaigns on cybersecurity and warn them of threats.[35]

Legislation

France has had a long history of regulating the dissemination of disinformation under the rubric of "false news". Under French law regarding the freedom of the press, disinformation has been outlawed with sanctions for decades. The current version of the law covers the publication, distribution or reproduction of false or fabricated news that undermines the public peace as well as fines up to €45,000.[36] Defamation is also outlawed under the same law and when committed in relation to a person's sex, their sexual orientation or gender identity or their handicap, the offending individual(s) will face one year's imprisonment and a fine of €45,000 (or one of these two penalties).

In late 2020, France passed a law against the manipulation of information, which also specifically addresses electoral misinformation. The law enacts strict rules on the media three months prior to any vote. It gives authorities the power to remove "fake" content on social media and even ban the sites that publish it. It also requires more financial transparency for politically sponsored ads.[37] The new law also adds media literacy to the public school curriculum.

A separate piece of legislation was recently passed to target hate speech on the internet, but it was struck down in May 2020 by France's Constitutional Council. Similar to Germany's NetzDG, the law would have required digital media platforms to remove discriminatory and sexually abusive comments within 24 hours of being flagged by users.[38]

Policy gaps

France's long history of outlawing "false news" and offering additional safeguards to protected groups stands out from the other countries covered in this overview. However, there have been concerns about whether such laws are too expansive and may lead to acts of censorship and the government's control of the media.[39] Current laws focus on the nature of the content (i.e. is it false or defamatory) rather than the delivery (via algorithms) and funding (via online advertisements). More policies are needed to address how disinformation is funded and amplified. There is an opportunity to close these gaps as a result of EU-level efforts that could potentially strengthen policy measures against disinformation in France.[40]

Germany

Institutions

The German government does not have a dedicated interagency disinformation task force. However, there is a cross-government task force on hybrid threats headed by the Interior Ministry, which also deals with disinformation.[41]

In addition, there are various German institutions that are tasked with tracking and monitoring disinformation. At the parliamentary level, the Parliamentary Research Services of the German Bundestag (Parliament) has published reports on the dissemination of false information. The Bundeswahlleiter (Federal Returning Officer), who is in charge of organising German elections, has the task of monitoring election-related disinformation.[42]

Regarding regulatory and/or sanctioning powers, under the Telemedia Act (TMG), the German Press Council (Deutscher Presserat) is able to issue reprimands to journalistic companies that do not adhere to agreed standards of journalistic conduct.[43] Fines for the violation of laws related to disinformation are brought by the German Federal Office of Justice.[44]

Legislation

In January 2018, Germany took the dramatic step of enacting an online hate speech law that imposed fines up to €50 million for sites that do not take down "obviously illegal" posts. Known as the Network Enforcement Act (2017) or NetzDG (in German), the law targets social media companies with over 20 million users, such as Facebook, Twitter and YouTube, giving them 24 hours to remove harmful content after notification. It is important to note, however, that the focus is on hate speech, and disinformation is only indirectly addressed if it relates to hate speech content that generates violence. The law has already been used to fine companies such as Facebook.[45]

However, the law has had many critics, either saying that it goes too far or not far enough. One weakness of NetzDG, as noted by the German policy think tank, Stiftung Neue Verantwortung (SNV), is that the regulations and determination of a breach of law are largely outsourced to companies.

There have been several attempts to strengthen the NetzDG in light of these complaints. In 2020, an amendment was passed by Germany's lower house that would update NetzDG to ensure that platforms were proactively reporting any serious hate speech cases to the relevant law enforcement authorities.[46]

Another recently passed law makes hate-motivated insults a criminal offence that can be punished with a monetary fine or up to two years' imprisonment. According to Germany's Justice Minister, the law is meant to safeguard groups attacked by online hate speech, as well as other protected groups (religious, ethnic, etc.).

Finally, there is a new Interstate Media Treaty, which requires online sites to follow good journalistic practices. This treaty offers a mechanism to hold producers of online content more accountable, including for disinformation.[47]

Policy gaps

Sanctions like those mandated by the NetzDG may cause online platforms to take an expansive approach to content removal in order not to fall foul of the regulations. Moreover, despite Germany's legal framework, online hate speech, often driven by disinformation, continues to manifest in increased offline violence.[48] Germany's current legislation does not address the problem of financially driven disinformation. German policy efforts could be strengthened by holding online monetisation platforms – including advertising technology (ad-tech), e-commerce, and e-payment companies – to the same high standard that they hold social media platforms. As noted in France's overview, EU-level efforts offer Germany the opportunity to cover these areas.[49]

India

Institutions

In compiling this overview, we found no government interagency task force or institutional equivalent in India dedicated to combating disinformation. While India does have an election commission, it does not directly address disinformation but institutes a short advertising and campaigning blackout period before an election. This is not to say that disinformation is not a problem in India. Among the 22 countries surveyed as part of Microsoft's Third Digital Civility Index, Indian respondents were most likely to encounter false information and hoaxes.

Legislation

Freedom of expression is protected under the Indian Constitution, but may be reasonably restricted when it poses a threat to Indian sovereignty, security or public order, or constitutes defamation. While current Indian law does not explicitly mention "fake news" or disinformation, the Indian Penal Code outlaws some forms of hate speech[50] and also criminalises any "rumour" that may lead to public alarm. The Indian government has used the National Disaster Management Act, which includes a provision related to "false warnings" (see section 54), during the coronavirus pandemic to take action on COVID-19-related disinformation.

The Information Technology Act, instituted in 2000, regulates digital commerce and outlines certain cybercrimes. It requires intermediaries to publish terms and conditions and forbids content that is "grossly harmful, harassing, hateful, racially, or ethnically objectionable".

During the 2019 election, India enacted a Voluntary Code of Ethics signed by social media platforms in order to increase public confidence in the electoral process. From 2021 onwards, the Internet and Mobile Association of India (IAMAI), a not-for-profit industry body, will observe the voluntary code during all future elections.

More recently, however, attempts to address disinformation have been reportedly highly politicised.[51] As such, the government's controversial new internet

intermediary rules have been scrutinised for the measure's attempt to hold online service platforms to harsher standards of user content and push for the use of automated tools to remove illegal content. A government press release explicitly mentions the intended targets as WhatsApp, YouTube, Facebook and Twitter, but it will also apply to LinkedIn, TikTok, Reddit and other services.

Policy gaps

India serves as another example of why policy developed to combat disinformation should take into account sufficient consultation with outside experts and relevant, independent organisations. Furthermore, the Information Technology Act could be strengthened by introducing standards for ad-tech (advertising technology) policies and enforcement when advertising accompanies disinformation. The 2019 Voluntary Code of Ethics could also be expanded to include such provisions and be made into a general code for platforms to uphold.

Italy

Institutions

Currently, most of the efforts in Italy to combat disinformation focus on electoral cycles. In 2018, for example, amid concerns of electoral disinformation, the Italian government created an online portal to report hoaxes to the police. However, online reporting through the portal, without clear guidance and definitions, raised alarms that it could undermine the freedom of the Italian press by creating an ill-defined oversight mechanism. The portal was quickly taken down and references to it were removed from the relevant websites.[52]

In terms of disinformation outside electoral cycles, the Autorità per le Garanzie nelle Comunicazioni (AGCOM), is Italy's regulator and competition authority for the communications industries in Italy. However, AGCOM has no regulatory responsibilities in the area of online hate speech and/or disinformation on social media, since such content was not included in the definition of AGCOM's audio-visual media jurisdiction. It is also unable to intervene and impose sanctions on broadcasters based in the Italian territory in cases of non-compliance with regulation,[53] although it has attempted to establish rules on hate speech for audio-visual and video-sharing platforms.

An interagency task force was established to respond to the COVID-19 threat in Italy. While the activities and objectives of the task force do not explicitly mention disinformation, it does state that the task force has analysed the online perception of the pandemic, which might include the impact of COVID-19-related disinformation.[54]

Finally, the Italian National Office Against Racial Discrimination, UNAR, has also promoted a series of activities to stem digital hate speech and cyberbullying, which have some overlaps with disinformation campaigns that target specific groups.[55]

Legislation

The current Italian regulatory framework for audio-visual media is the Gasparri Law and the Consolidated Act. These require that audio-visual media services air programmes that respect the fundamental rights of the person and do not promote intolerance towards protected classes. Furthermore, the Italian Penal Code addresses defamation and fines for those who publish or disseminate "false, exaggerated or tendentious news which is likely to disturb public order". However, it has been difficult to enforce the code with social media.[56]

As a result, a new bill was proposed in 2017. It aimed to establish rules for digital platforms and focused on combating "false news" that could cause public fear, hateful content and electoral interference. It called for fines for non-compliance, both for the managers of the platforms and the authors of the related content (which is similar to French legislation as it outlaws disinformation that disturbs the public peace). Critics of the bill argue that the penalty of two years' detention that could result from violating the bill would be repressive and restrict free speech. Currently, the bill has been assigned to the Constitutional Affairs and Justice committees, but has not been passed.

Another more recent law was proposed by the Forza Italia party (meaning "Forward Italy" or "Let's go, Italy") in May 2019. It would require users to provide their social security number to create a social media account. This removal of anonymity aimed to combat hate speech and the spread of "fake news". The resulting criticism and media coverage led to the proposal never being formally presented as draft legislation.

Policy gaps

Overall, Italy's efforts to combat disinformation tend to be less structured and coordinated than those of the other EU member states included in this overview (i.e. France, Germany and Spain). Currently, there are

no concrete government efforts or interagency task forces to address disinformation in the country. Since its regulator, AGCOM, already has regulatory powers over the communications industry, it could be useful to task that body with formulating draft regulations. As noted elsewhere in this report, once the EU regulations via the Digital Services Act and the Digital Markets Act are agreed, the country will need to align its regulatory framework, including to combat the amplification and monetisation of disinformation.

South Africa

Institutions

In response to the threat caused by COVID-19 misinformation, South Africa has created an interagency task force to monitor "fake news" during the pandemic and beyond. It is composed of representatives from the Department of Communications and Digital Technologies, not-for-profit companies such as ZADna (which administers the .za domain name), the telecommunications regulator (the Independent Communications Authority of South Africa, ICASA), and relevant platform owners. The task force is responsible for monitoring complaints and reports from the media and the public. As follow-up, the task force will have the ability to remove content on a variety of platforms and submit cases to the South African Police Service for investigation and prosecution.

In terms of regulations, South Africa's regulator, ICASA, works to ensure that telecommunications serve the public interest and promote programmes that popularise narratives of a non-sexist, non-racial, equal and democratic South Africa.

In addition, the Election Commission of South Africa is working with Media Monitoring Africa, a not-for-profit company, to run the Digital Complaints Committee (DCC). The DCC upholds a Voluntary Code of Conduct, but does not have any legally binding powers. Instead, the DCC uses a reporting system called Real411 where users can report disinformation and hate speech via a mobile app, website or a dedicated WhatsApp number.[57]

Legislation

Freedom of expression is protected under the South African Constitution (1996), except in cases involving "advocacy of hatred that is based on race, ethnicity, gender or religion, and that constitutes incitement to cause harm". The Prevention and Combating of Hate Crimes and Hate Speech Bill was introduced in 2016 and aims for greater enforcement and transparency against hate speech. It is still before the South African National Assembly and current debate has centred on whether it would censor free speech.

After declaring a state of disaster in early 2020 due to the COVID-19 pandemic, President Cyril Ramaphosa temporarily limited some of the rights of South African citizens. The Disaster Management Regulations, which were issued from powers conferred by section 27(2) of the Disaster Management Act of 2002, created several offences regarding publishing COVID-19-related content.[58] It criminalises publication, in "any medium" of information with the "intention to deceive any other person about" COVID-19 (including the virus and treatments). These regulations have already been used to make arrests. These measures have been extended for more than a year, despite criticism from human rights groups over its reported censorship and restriction of freedom of the press.[59]

In addition, in terms of soft policy, there is a Voluntary Code of Conduct upheld by the DCC, which includes South Africa's Press Council and the South African National Editors Forum (SANEF), to address harmful online content.[60]

Despite the fact that South Africa's government, like many others, struggles with disinformation during elections, South Africa currently does not have any policy that specifically targets electoral disinformation. This sets it apart from all the other countries in this study. In the past there have been allegations that political parties used disinformation as part of their election tactics against their opposition.

Policy gaps

South Africa's current regulatory stance could be strengthened by adding a focus on electoral disinformation, as is seen to varying degrees in every other country in this study. Furthermore, reforming and providing greater transparency about the COVID-19 Disaster Management Regulations would help to mitigate concerns of the alleged limitations on the press and free speech. Amending these temporary measures would help to alleviate these concerns and could improve public confidence.

Spain

Institutions

Spain's main institution tasked with combating disinformation is a permanent commission that is responsible for assistance related to the technical and operational assessment of possible disinformation campaigns. It is coordinated by the Secretary of State for Communication and directed by the Department of Homeland Security.

In addition, Spain's Interior Ministry has jurisdiction over national security and upholding constitutional rights. The National Office to Combat Hate Speech falls under its auspices and acts as a trusted flagger for internet service providers to facilitate the removal of hate speech in coordination with the National Security Forces.

Another relevant government entity is the National Markets and Competition Commission (CNMC), a regulatory body. The CNMC promotes the proper functioning, transparency, and competition of different commercial sectors in Spain, including telecommunications.

Finally, in certain cases of public safety and/or national security, the Ministry of Economy and Enterprise has the power to intervene in the functioning of internet services and electronic communications.

Legislation

The Spanish Constitution (1978) guarantees freedom of expression through any means, and only restricts it to protect the rights enshrined in the Constitution. These rights include the dignity of the person, specifically that Spanish citizens may not in any way be discriminated against on account of birth, race, sex, religion, opinion or any other personal or social condition or circumstance. In addition, Spanish hate speech laws carry a higher criminal provision if the offence is committed online.

However, the Spanish Constitutional Court (CC) has since regulated freedom of expression in situations where it is unquestionably insulting and has no relationship with how someone expresses their ideas or opinions. In particular, the CC has ruled that the right to freedom of expression does not include the use of insulting expressions by the press that are deemed unnecessary for journalistic writing.

Days before the 2019 Spanish general elections, the Royal Decree-Law 14/2019 was published to address "challenges posed by new technologies", which included electoral disinformation. Under this decree, the Ministry of Economy and Enterprise has the power to intervene, lock or shut down the internet and electronic communication networks or services, without any judicial intervention to prevent potential abuses.[61] The Royal Decree-Law has remained controversial. Various advocacy organisations such as ARTICLE 19 and Amnesty International have asked for it to be significantly amended to address human rights concerns.

More recently, Spain has attempted to address disinformation through another controversial law. In late 2020, the Spanish government introduced a ministerial order known as the "Procedure for Intervention against Disinformation", which outlines communication procedures to counter disinformation, but does not censor harmful content. The order proposes a permanent committee to enforce the ministerial order, but journalists and media outlets will not be represented on the committee.[62] Despite the law being backed by the European Commission, such provisions have raised concerns about press freedom in Spain.

One unique action Spain has taken is a joint cybersecurity pact with Russia to address disinformation campaigns that could have a negative impact on diplomatic relations. Spain has voiced concerns about possible Russian influence campaigns during elections. As a result, both countries agreed to establish a joint group with the goal of preventing misinformation from harming ties between the two countries.

Policy gaps

Spain's efforts to regulate disinformation have raised serious and valid concerns about its impact on freedom of expression and free access to information in the country – both online and offline. The situation in Spain highlights the importance of collaborating with media experts and non-governmental organisations to ensure that human rights are being protected online while fighting against disinformation. Spain's current policy response to disinformation is not yet aligned with current measures being pursued by the European Union to disrupt and defund disinformation.

United Kingdom

Institutions

In the UK, the responsibility to develop policies to combat disinformation is largely centred with the Minister of State for Digital and Culture and its Department for Digital, Culture, Media and Sport (DCMS).This is the body that has proposed the Online Safety Bill.

However, there are other authorities and institutions that will be involved in enforcement measures and sanctions once this proposed regulatory framework is established.

The Competition and Markets Authority, and namely the Digital Markets Unit (DMU), is to be included in these regulatory efforts. The DMU was set up in April 2021 to "operationalise the future pro-competition regime" that the UK is setting up for its digital market, including large platforms and how they conduct their business (including harm to and for consumers).[63]

Another key actor to be included in this regulatory landscape is OFCOM (the Office of Communications), which is the UK's regulator of its communication services. OFCOM is tasked by Parliament to oversee the enforcement of related regulations as an independent organisation.

In addition to these bodies and institutions, the UK government has more recently set up a counter-disinformation unit to fight false claims about the coronavirus. The unit provides weekly reports to ministers on the trends of coronavirus disinformation online.

Legislation

In May 2021, the Minister of State for Digital and Culture introduced to Parliament a draft of the Online Safety Bill, which is intended to regulate illegal and harmful content on the internet. The proposed draft calls for the most popular social media sites to act on content that is harmful but not unlawful (which includes disinformation). If the draft is approved, these sites will be required to specify in their terms and conditions how they will carry out this obligation. OFCOM is tasked with overseeing the regulation once the bill is adopted. As it is currently proposed, OFCOM will be given the power to fine companies that fail in their new "duty of care" up to £18 million, or 10% of annual global turnover, whichever is higher. OFCOM will also have the power to block access to sites. As the Online Safety Bill is currently drafted, it proposes a new criminal offence for senior managers if their technology firms do not improve safety as part of their "duty of care".

The Online Safety Bill built upon previous government consultations and investigations into disinformation and online harm. The British Parliament, for example, published a 2019 report on disinformation and fake news that was the result of an inquiry spanning more than 18 months.

Policy gaps

Even though aspects of the draft Online Safety Bill seem promising, there are places where GDI believes it should be strengthened. The current draft regulation does not include a definition of disinformation nor is there an explicit mention of the monetisation of disinformation, through online advertising or other channels such as e-commerce and e-payment systems. The draft Online Safety Bill also focuses on "user-to-user services", which means that content on news publishers' own websites generally will not fall within the scope of the law. This limits the reach of the Online Safety Bill and could potentially dampen its ability to reduce disinformation.

United States

Institutions

In the US, various government entities are tasked with combating disinformation, with the responsibilities spread out institutionally.

In terms of foreign disinformation, the main body is the Global Engagement Center (GEC), which is housed under the US State Department. The GEC was set up by the 2017 National Defense Authorization Act to coordinate interagency efforts to counter foreign propaganda and disinformation. It is tasked with tracking, exposing and identifying disinformation narratives. While its original focus was on counter-terrorism, the GEC has recently expanded its work to include mis- and disinformation on COVID-19.

In addition to the GEC, there is also the Cybersecurity and Infrastructure Security Agency (CISA) which has a Mis-, Dis-, Malinformation team that addresses both foreign and domestic cases of disinformation. This team covers disinformation during elections and, since May 2020, has also provided information about COVID-19 disinformation.

In addition to these bodies, there are other government agencies that have regulatory powers to address

cases of disinformation. The Federal Communications Commission (FCC) prohibits broadcasting false information that could cause significant public harm and may act on complaints if broadcasters intentionally distort the news. The Federal Trade Commission (FTC), is tasked with protecting US consumers and enforces truth-in-advertising laws. Specifically, the FTC requires that "ads be truthful, not misleading, and, when appropriate, backed by scientific evidence". Since the outbreak of COVID-19, the FTC has been sending warning letters to companies that violate this policy and are placing advertisements that contain false or misleading information regarding COVID-19.

Legislation

The main piece of US legislation that relates to disinformation is Section 230 of the Communications Decency Act (1996), which shields platforms from civil liability for third-party content published on their service. Section 230 remains controversial. Some technology experts state that removing Section 230 would cripple large internet companies with lawsuits, while others state that it has allowed harmful content to spread unchecked.[64]

As a result, Congress is currently looking at solutions to either build on Section 230 via reform proposals, or to completely override it through new legislation. For example, the SAFE TECH Act, which was introduced in February 2021, would make it clear that Section 230 does not provide platform immunity for issues related to advertisements or other paid content, enforcement of civil rights laws online and online stalking, harassment and intimidation. Another similar initiative is the Protecting Americans from Dangerous Algorithms Act, which was reintroduced in March 2021. This Act seeks to specifically hold social media companies accountable for their "algorithmic amplification of harmful, radicalising content that leads to offline violence", which would include disinformation. The proposed measure would amend Section 230 so that platforms do not have immunity when it comes to extremist or harmful content.

Several other bills that could have a significant impact on the spreading of disinformation in the US have also been recently introduced to Congress. The Algorithmic Justice and Online Platform Transparency Act of 2021, also sometimes referred to as the Markey/Matsui Bill, points out the disproportionate impacts disinformation has on marginalised communities and will create an algorithm task force that will study the discrimination promoted by algorithms. Advertising regulations will also be introduced, but there is no mention of regulating advertising that funds disinformation. Other relevant legislation includes the Corporate Executive Accountability Act, which makes it easier to send executives to jail for serious online crimes if their company makes over $1 billion in annual revenue.

There are also newly pending bills that have the potential to change the digital advertising landscape in the US. The American Choice and Innovation Online Act would outlaw platforms from favouring their own products and services. This could have an impact on Google Ads, which currently is the dominant force in the advertising technology (ad-tech) world, providing 98% of online advertising according to a recent internet survey. Similarly, the Ending Platform Monopolies Act, which would forbid companies with at least 50 million monthly active US users and a market cap of $600 billion or more from operating businesses that would cause them to advantage their own products and services (such as online advertising).

Policy gaps

While the US has some policy initiatives targeting disinformation, there is no single piece of legislation or soft policy (such as a code of practice) that specifically focuses on disinformation, its financial drivers and/or the online harm that it creates. The new draft bills currently proposed do attempt to address this shortfall but they are not fully harmonised with measures currently being pursued in other countries and regions, such as the UK and the EU. If these other bills move forward, they would make companies liable for disinformation and harmful content being peddled on their platforms.

European Union

Institutions

The European Commission has various directorates and cabinets that are tasked with initiatives to combat disinformation.[65] There are also various EU parliamentary committees that have a remit on foreign and domestic disinformation.[66]

Other relevant institutions are the European Union Agency for Network and Information Security (ENISA), which is the EU-wide agency dealing with issues of cybersecurity (which indirectly overlaps with coordinated disinformation campaigns) and the Body of European Regulators for Electronic Communications (BEREC),

which works with member states to implement the telecommunications directives of the European Commission. In addition, the European Data Protection Supervisor (currently Wojciech Wiewiórowski) plays a key role in enforcing the General Data Protection Regulation (GDPR), which helps protect personal data and privacy.

Legislation

There are some overarching EU frameworks that relate to online freedom of speech, information and related protections. The EU Charter of Fundamental Rights, for example, outlines the right to freedom of expression and free access to information (Article 11).[67]

As noted above, three key regulatory initiatives have been proposed to combat disinformation across the European Union: the Digital Services Act (DSA), the Digital Markets Act (DMA) and the EU Code of Practice on Disinformation (voluntary regulation). The DSA's goal is to create a safer digital space in which the fundamental rights of all users of digital services are protected and to promote innovation within the EU and globally. The DSA, when passed, will issue a common set of regulations for intermediaries within a single market.

The sister legislation to the DSA is the Digital Markets Act (DMA), which will require new transparency obligations and a regulatory framework for advertising technology (ad-tech) and other online monetisation companies operating within the EU. For online advertising specifically, relevant platforms and services will be required to provide advertisers and publishers with information about pricing and other relevant information related to the advertising value chain.

In contrast, the EU Code or Practice is a law that has issued new guidance[68] for including the monetary incentives of disseminating disinformation. The EU code is similar in scope to the Australian code and has some common language when discussing issues related to disinformation. However, the EU code states that disinformation can have the purpose of economic gain and also has a section discussing the financial incentives fuelling the spread of disinformation. Still, both codes take a voluntary rather than a regulatory approach to signing and abiding by certain standards of the code.

Another framework, which is not legislation, is the EU Democracy Action Plan (EDAP), which aims to address specific challenges to democratic systems in the EU and its member states. Among the areas it covers is the need to counter disinformation. The framework, while not legally binding, sets out areas where regulations and policy are needed, including advertising.

Policy gaps

The EU has taken the lead in proposing policies and regulations that combat disinformation through a whole-of-industry approach that also targets removing the financial incentives of online disinformation. There are still a few areas where the EU's current legislation could be strengthened and both the Digital Services Act and the Digital Markets Act are currently under consultation in the European Parliament and member states. Both Acts will undergo amendments and the next 12 to 18 months will be critical for defining their regulatory remits.

Endnotes

1 See: https://disinformationindex.org/2021/07/want-less-awful-content-stop-focusing-on-content-moderation.

2 For a full list of GDI's country risk assessments, see: https://disinformationindex.org/research.

3 See: https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries and for India, https://www.trai.gov.in/sites/default/files/PR_No.101of2020_0.pdf.

4 These are in order of magnitude: China = 765 million; India = 391 million; USA = 245 million; Brazil = 126 million; Japan = 116 million; and Russia = 109 million. Data is based on 2017 figures; see: https://ourworldindata.org/internet.

5 The categories were defined using the following parameters: Elections: Actions to address specifically election-related disinformation; Hate speech: Restricted or criminalised hate speech; Advertising: Actions to address the issue of advertising on disinformation sites providing funding to purveyors of harmful content; Interagency task force: The existence of a permanent or temporary task force to combat disinformation within relatively recent history (a decade prior to this investigation, 2011–2021); Non-compliance sanctions: Law, ministerial orders or similar governmental actions that institute some form of sanction against the creation or dissemination of specifically disinformation or deliberately false information, not including defamation or hate speech.

6 In each of the countries (except for the UK and US where GDI extensively works), we asked GDI's local partner or other known expert to review our findings and provide feedback: Argentina: Chequeado; Australia: Reset Australia; Brazil: ITS Rio; Canada: CIGI; EU: EUDisinfoLab; France: Institut Montaigne; Germany: Stiftung Neue Verantwortung; India: Centre for Internet and Society; Italy: IIT/CNR and Sapienza University of Rome; South Africa: Code for Africa; Spain: Universad Carlos III de Madrid (UC3M).

7 It has been argued that a potential solution to Section 230 could be to build upon existing precedent. As it stands, Section 230 does not cover illegal content. It could be expanded so that it does cover harmful content or electoral disinformation that threatens democracy. This would ensure that companies are held accountable for disinformation being shared on their platforms.

8 Minor sections of the law, which created an official online hate speech watchdog, will still stand. For more information, see: https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html. Similar to Germany's NetzDG, the law would have required digital media platforms to remove discriminatory and sexually abusive comments within 24 hours of being flagged by users.

9 For example, the SAFE TECH Act, which was introduced in February 2021, would make it clear that Section 230 does not provide platform immunity for issues related to advertisements or other paid content, enforcement of civil rights laws online and online stalking, harassment and intimidation. Another similar initiative is the Protecting Americans from Dangerous Algorithms Act, which was reintroduced in March 2021. This Act seeks to specifically hold social media companies accountable for their "algorithmic amplification of harmful, radicalising content that leads to offline violence", which would include disinformation. For more information, see the Annex.

10 The model in Australia has been criticised by some local organisations as being captured by industry since the regulator has devolved the code's design and implementation to an industry body. See: https://au.reset.tech/news/big-tech-s-australian-code-of-practice-on-disinformation-is-both-pointless-and-shameless. For its part, the government requested that the Australian Communications and Media Authority (ACMA) provide a report by June 2021 on the code of practice process and the state of disinformation in Australia. The report has not yet been published as of this writing. See: https://www.acma.gov.au/online-misinformation.

11 This task force was recalled into service for the September 2021 snap elections.

12 See p. 3: https://dserver.bundestag.de/btd/19/124/1912489.pdf.

13 The German Press Council is also tasked with enforcing the Press Code, but the code is joined on a voluntary basis, which means that it typically does not cover social media platforms or their users. In the UK, one press body, IPSO, acts as the independent newspaper regulator and imposes sanctions on members who break the code of conduct. This code of conduct contains

stipulations for publishing "inaccurate, misleading or distorted information or images, including headlines not supported by the text". IMPRESS in the UK is another voluntary press-regulating organisation that offers benefits such as legal protection in return for adherence to their journalistic standards. For more information, see: https://www.impress.press/standards.

14 The UK's Department for Digital, Culture, Media and Sport has published a proposed regime framework for consultation until October 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003913/Digital_Competition_Consultation_v2.pdf.

15 This new guidance encourages all parts of the advertising industry, including the brands that participate in online advertising, to join the code and work to defund disinformation. It asks for increased transparency and accountability around the placement of advertisements. Signatories are required to make their recommender systems public, have systems in place for users to flag disinformation and warn users who interact with content marked false by fact-checkers. It also proposes a permanent disinformation task force composed of signatories, experts and representatives from relevant organisations that will adapt the code in view of technological, societal, market and legislative developments. The establishment of a permanent task force would show a long-term commitment to fighting disinformation. See: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585.

16 For more information regarding this and the case of journalist Gustavo Raúl Romero, see: https://freedomhouse.org/country/argentina/freedom-net/2020.

17 For an assessment of Argentina's media restrictions in response to COVID-19, see: https://gjia.georgetown.edu/2021/01/19/argentinas-new-media-regulations-create-jitters-over-information-control.

18 Punishment for crimes against public order and inciting public violence include three to six years' imprisonment. False accusations under the penal code can also result in a fine of 3,000 to 30,000 pesos. Intentionally disgracing or dishonouring an individual is also punishable with a fine from 1,500 to 20,000 pesos.

19 This approach of prioritising educational programmes over regulation to combat disinformation was suggested by William Evanina, the director of the US National Counterintelligence and Security Center, as a possible solution to combating disinformation while not infringing on people's freedom of speech. For information, see: https://www.bloomberg.com/news/articles/2020-10-15/u-s-intelligence-official-says-social-media-big-vulnerability and https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

20 This could include engaging with the public school curriculum: see the France report section.

21 This could be a reflection of the country's recent history with repression of the media under its military dictatorship (1976–1983) and the continued tension that exists between its media and political leadership in an increasingly politically polarised country. Brazil, another country in this report that has struggled with polarisation, has also implemented media literacy initiatives into its policy response to disinformation.

22 In 2019, it started an advertising campaign called "Stop and Consider", which encouraged citizens to examine the source of their information when they see news during the election campaign.

23 The Australian Communications and Media Authority (ACMA) issued a position paper on misinformation and news quality in Australia. The government requested that ACMA provide a report by June 2021 on the code of practice process and the state of disinformation in Australia. The report will include an assessment of the code development process; the content of the code(s) and resulting measures, and the state of disinformation in Australia.

24 Some highlights from the reports include that Google blocked and removed 3.1 billion bad advertisements globally in 2020. In the same year, Facebook removed over 14 million pieces of content that constituted misinformation related to COVID-19. Signatory reports are to be issued annually going forward, after the initial three-month reports were provided.

25 For example, see: https://au.reset.tech/news/submission-on-the-australian-code-of-practice-on-disinformation.

26 For example, while Australia's code does mention the monetary incentives that promote the dissemination of disinformation, it does not outline areas for action to demonetise such content, nor are a sufficient number of online monetisation platforms (such as Amazon, PayPal and eBay) currently signatories to the code.

27 The programme has several components, including promoting organisational cohesion, media literacy, containing disinformation and improving technical resources to combat the problem. The Superior Electoral Court plans to launch a website that will collect information about disinformation and also to publish a book from the disinformation debates they host.

28 For criticisms of this task force, see: https://chargedaffairs.org/brazils-fake-news-problem and for more information: http://www.thebrazillawblog.com/brazilian-task-force-to-combat-fake-news-before-election.

29 Anatel's regulatory agenda for 2021–2022 can be found here: https://sistemas.anatel.gov.br/anexar-api/publico/anexos/download/5c87f7cb798332bf9d890d0fded916bf.

30 For example, the definition of disinformation used in the law is vague, which could allow it to be used to silence political opponents. In addition, the proposed law's definition of an "inauthentic account", which includes using a fake name, could cause conflict between the social profiles and legal names of individuals, such as those from the trans community.

31 The task force existed only for the Canadian election, but it will be activated again when there is a federal election in September 2021.

32 The clerk of the Privy Council serves on the CEIPP and is the head of the Canadian civil service.

33 The proposed law will create a new regulator with fairly broad auditing powers over the online space and will be guided by an oversight board that will be responsible for Canada's privacy laws. Furthermore, it will add a new definition of "hatred" to the Canadian Criminal Code based on the Supreme Court of Canada's decisions. It will also add a peace bond, designed to prevent hate propaganda offences and hate speech, to the criminal code.

34 At the date of this report (September 2021), none of these reports could be found online. Companies will have to issue reports regarding breaches of data and privacy, but reports will most likely not cover transparency of advertisements due to it falling between the jurisdiction of two parts of the Canadian government (democratic institutions are under the Ministry of Intergovernmental Affairs and media regulation is the responsibility of the Ministry of Heritage).

35 For example, during the 2017 presidential election, there was a massive leak of then candidate Emmanuel Macron's emails, with likely indications that the breach was committed by Russia. CNCCEP issued a press release, stating that the media should not report on it, and reminding them that disseminating disinformation can be a criminal offense.

36 The same action will be fined €135,000 if found to disrupt the morale of the French armed forces or impede their war efforts.

37 There are three major provisions to the law: a judge who acts proportionally to halt the spread of misinformation 48 hours after there has been a notification; a requirement that platforms publish who has purchased campaign ads and at what price; and new administrative and executive powers to the broadcasting regulator, the CSA, to ensure that platforms abide by the law.

38 Minor sections of the law, which created an official online hate speech watchdog, will still stand. For more information, see: https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html.

39 For critiques, see: https://foreignpolicy.com/2018/05/29/macrons-fake-news-solution-is-a-problem/; https://www.forbes.com/sites/simonchandler/2020/05/14/french-social-media-law-is-another-coronavirus-blow-to-freedom-of-speech and https://www.nytimes.com/2020/06/18/world/europe/france-internet-hate-speech-regulation.html.

40 The Digital Services Act will establish a common set of rules for intermediaries within a single market. It has the potential to create consistent and adequate ad-tech policies not just in France, but throughout the EU. The Digital Markets Act will have transparency requirements for ad-tech companies operating in the EU, which could increase accountability and drive reform efforts. The EU Code of Practice will require relevant signatories to improve their relevant advertising and ad-placement systems to defund disinformation. These initiatives at the EU-level have the potential to strengthen measures in France to combat the funding of harmful online content, namely disinformation.

41 See p. 3: https://dserver.bundestag.de/btd/19/124/1912489.pdf.

42 See: https://www.bundeswahlleiter.de/bundestagswahlen/2021/fakten-fakenews.html.

43 The German Press Council enforces the Press Code but it is joined on a voluntary basis, which means that it typically does not cover social media platforms or their users.

44 The German think tank, Stiftung Neue Verantwortung (SNV), which specialises in technology policy and society, has studied and issued recommendations regarding initiatives in Germany and the EU that tackle domestic and foreign disinformation. See: https://www.stiftung-nv.de/sites/default/files/regulatory_reactions_to_disinformation_in_germany_and_the_eu.pdf.

45 For example, in July 2019 the Federal Office of Justice imposed a fine of €2 million (about US$2.2 million) on Facebook Ireland Ltd for violating its reporting obligations under the Network Enforcement Act.

46 Instituted amendments include strengthening user mechanisms for appealing content removal and broadening the scope of NetzDG to video-sharing platform services.

47 This point has been argued by German organisations working on the digital agenda, including NetzPolitik. See: https://netzpolitik.org/2020/medienstaatsvertrag-der-lange-kampf-gegen-desinformation.

48 In 2020, there was an increase in hate crimes according to data released by the Federal Criminal Police Office (BKA). For example, hate crimes against LGBTQIA+ people increased by 36% in Germany in 2020, and anti-Semitic and xenophobic hate crimes rose by 15.7% and 19.1% respectively.

49 The Digital Services Act, the Digital Markets Act and the EU Code of Practice all have proposed text that looks at the financial incentives that promote the dissemination of disinformation and the broader risks posed by disinformation to the tech ecosystem and its online users.

50 The code states that it is illegal to be "promoting enmity between different groups on ground of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony".

51 India's disinformation has been documented by a variety of third parties as being allegedly disseminated by domestic political parties via nationwide cyber-armies. These groups target not only political actors but also religious minorities and dissenters.

52 More detailed criticisms of the online portal to report disinformation can be found here: https://www.valigiablu.it/legge-fakenews-censura.

53 The exception is programmes aired during the limited time band (between 16:00 and 19:00) during which minors are required to have additional protection. For more information, see: https://www.article19.org/resources/article-19-comments-on-new-italian-regulation-on-hate-speech.

54 For information regarding the reports published by the COVID-19 task force, see: https://github.com/taskforce-covid-19/documenti and https://www.tandfonline.com/doi/abs/10.1080/23248823.2021.1916858?af=R&journalCode=rita20.

55 Their CONTRO project lasted from 2018 to 2020 and involved an awareness campaign about online discrimination and partnered research regarding hate speech. Results from the project include a mapping of hate speech on Italian social networks and the development of counter-narratives to promote human rights in Italy. More information about the CONTRO project can be found here: http://www.unar.it/contro.

56 An author-centred approach can be ineffective due to fake profiles on social media. For more criticisms of this policy strategy, see: https://british-association-comparative-law.org/2021/03/26/italys-fight-against-fake-news-a-work-in-progress-by-alberto-nicotina-and-simone-riganelli.

57 Although this process is independent from the government, use of it is heavily supported by them and they post content deemed as fake with a red stamp on their website. This has drawn concerns from activist groups over vague definitions of disinformation and concerns that public shaming will have a chilling effect on the press.

58 These regulations were issued from the terms of section 27(2) of the Disaster Management Act, 2002.

59 For the full report detailing the impact of COVID-19 regulations on freedoms in southern Africa, see: https://www.usaid.gov/sites/default/files/documents/INTERNEWS_EFFECTS_OF_COVID19_ON_FREEDOM_OF_EXPRESSION_IN_SELECT_SADC_COUNTRIES_2.pdf.

60 The Voluntary Code of Conduct is technically independent of the government, although it is greatly encouraged and supported by it. For more information, see: https://www.real411.org/about.

61 This power could be exercised in scenarios when there is an immediate and serious threat to public order, public security or national security. For more information, see: https://edri.org/our-work/spain-new-law-threatens-internet-freedoms.

62 The private sector and civil society are mentioned in the ministerial order as playing "an essential role in the fight against disinformation", but are not explicitly included as being part of the committee. In addition, a committee of civil society experts (with journalists, academics, civil society organisations, etc.) has been formed and is developing a report with a series of recommendations to tackle misinformation and disinformation. See: https://www.boe.es/eli/es/o/2020/10/30/pcm1030.

63 The DCMS has published a proposed regime framework for consultation until October 2021: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003913/Digital_Competition_Consultation_v2.pdf.

64 It has been argued that a potential solution to Section 230 could be to build upon existing precedent. Section 230 does not cover illegal content and could be expanded so that it does not offer tech companies protection from spreading significant harmful content or electoral disinformation that threatens democracy. This would shield companies from extraneous lawsuits while still holding them accountable for disinformation being shared on their platform.

65 The most relevant teams in the European Commission responsible for disinformation are the following: VP of Values and Transparency (currently Véra Jourová), leading the EU Democracy Action Plan and monitoring the EU Code of Practice on Disinformation); Executive VP of Europe Fit for The Digital Age (currently Margrethe Vestager), leading issues of digital market competition, including the Digital Markets Act and providing leadership on the liability and safety rules that will come out of the Digital Services Act); and Commissioner for Internal Market (currently Thierry Breton), steering the Digital Services Act (via the Directorate on Digital Transformation) and coordinating on the Digital Markets Act. It also is the home of a team that oversees the EU Code of Practice on Disinformation (via the Directorate on Media Policy).

66 The Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation – which is known as INGE – is responsible for investigating foreign electoral disinformation campaigns. The Committee on the Internal Market and Consumer Protection – also known as IMCO – oversees the EU's rules on the single market, which gives them power to regulate ad-tech platforms and other actors in the information ecosystem, including on illegal harmful content, such as disinformation. The Committee on Civil Liberties, Justice and Home Affairs (LIBE) has some overlapping responsibilities as its focus is on providing EU citizens with an area of freedom, security and justice, which includes protecting them from harmful content online. In addition,

the Committee on Legal Affairs (JURI) addresses corporate due diligence obligations and the shaping of legislation such as the Digital Services Act, which currently covers disinformation, the risks it poses and its financial drivers. The Court of Justice of the European Union plays a similar role to the Supreme Court in the US in that it challenges (rather than striking down) Commission proposals.

67 The European Parliament's LIBE committee has recently completed a study to look at how EU legislative efforts to combat disinformation can be balanced against these duties. For more information, see: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/695445/IPOL_STU(2021)695445_EN.pdf.

68 This new guidance encourages all parts of the advertising industry, including the brands that participate in online advertising, to join the code and work to defund disinformation. It asks for increased transparency and accountability regarding the placement of advertisements. Signatories are required to make their recommender systems public, have systems in place for users to flag disinformation and warn users who interact with content marked false by fact-checkers. It also proposes a permanent disinformation task force composed of signatories, experts and representatives from relevant organisations that will adapt the code in view of technological, societal, market and legislative developments. The establishment of a permanent task force would show a long-term commitment to fighting disinformation. See: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2585.