2 Implementing policies to enhance the transparency, accountability, and plurality of information sources

This chapter provides an overview of policies to reinforce the ecosystem that promotes information integrity. It discusses policies encouraging responsibility and transparency of online and social media platforms and the imperative of countering specific risks in the information space, including foreign information manipulation and interference, the safeguarding of information integrity in times of democratic elections, and the changes introduced by generative AI to the information space. It also provides an overview of the essential role played by plural, independent, and sustainable media markets, both on- and off-line.

2.1. INTRODUCTION

Building information integrity and addressing disinformation rest in large part on the resilience of citizens, as well as on the actors that produce content and the channels via which it is distributed, namely online and social media platforms and traditional media. The share of the population that regularly receives news from traditional and local media sources has declined, as people have increasingly shifted to receiving news on social media platforms. A 2023 study of 16 countries from around the world – all of which scheduled to hold elections within the subsequent year – found that 56% of internet users frequently use social media as their primary source of news, surpassing television at 44% (Quétier-Parent, Lamotte and Gallard, 2023[1]).

Examples from specific countries show similar trends. For example, in the United Kingdom, the share of population that uses print media as its primary source of news has fallen from 59% in 2013 to 14% in 2023, while the share of the population that uses social media as its primary source has increased from 20% to 38%. In the same period, the use of social media as a prime media source increased from 27% to 48% in the United States, and from 18% to 29% in Germany (Newman et al., 2023[2]). While data on news consumption patterns is inherently difficult to collect and compare across countries, the broad trends, particularly within younger populations, consistently show a shift toward the use of social media as a primary source of news.

The trend away from traditional media is particularly clear at the local and regional levels and is widespread across OECD countries and beyond, reflecting the continued evolution in the move toward a digital, mobile, and platform-dominated media environment. These trends also suggest that younger generations, who have grown up with digital media, will likely continue to primarily engage with online platforms rather than legacy platforms for getting and sharing information (Newman et al., 2023[2]).

Today, both online and offline engagement is increasingly shaped by information flows on online platforms. The impact of online platforms goes beyond its use as a direct source of information, as feedback loops – where mis- and disinformation, including conspiracy theories, that spreads online is picked up by traditional media outlets – thereby further amplifying and giving credibility to the content (OECD, 2022[3]). Online platforms also offer novel and efficient avenues for amplifying foreign information manipulation and interference campaigns, which attempt to illegitimately shape public opinion and discourse, undermine trust in democracy, and increase polarisation, often in parallel with other foreign interference efforts.

Given the increasingly important role played by online platforms in the information space and the incentives for private companies' algorithms to amplify engaging (and often sensational or polarising) content, building the understanding of how these technologies can be misused to threaten basic elements of democratic life will be essential to inform effective policy responses. As it stands, limited understanding of how online and social media platforms function, of data flows within and across them, and of how they are being used, inhibits effective policy responses.

What is more, the reduced reach of, and trust in, traditional media combined with risks of market concentration and capture have further eroded access to quality content and information integrity in many countries. A plural and independent media sector plays an essential role in facilitating public discourse, and reinforcing democracy cannot be achieved without strengthening the role of quality and trusted news media sources.

For that reason, policy interventions to promote transparent and diverse media and information spaces can be grouped around:

- Identifying a range of efforts encouraging accountability and transparency of online and social media platforms,
- Promoting plural, independent, and competitive media and information markets, and
- Countering specific risks, such as foreign information manipulation and interference, elections and disinformation, and those posed by generative artificial intelligence.

2.2. ENCOURAGING ACCOUNTABILITY AND TRANSPARENCY OF ONLINE AND SOCIAL MEDIA PLATFORMS

Given the prominent role and impact that online and social media platforms have in the information space, the benefits of accountability and transparency in the way they are designed and operated are increasingly understood. The priority in this space should be to analyse how policies can call for accountability, build understanding of their business models and the related risks to democratic processes, mitigate harms, and promote healthier information spaces.

A prominent threat to information integrity in democratic systems is the use of digital platforms, including social media, by domestic and foreign actors to manipulate and disinform the public. To mitigate similar risks in traditional media, for example, news outlets have historically been subject to various regulatory frameworks. Such oversight is due to traditional media's role in creating, editing, and selecting content, as well as their use of limited public resources (e.g. broadcast spectrum). These policies often cover areas like standards, ownership restrictions, and licensing requirements, and complement strong self-regulatory practices of the profession.

Online platforms, however, do not claim editorial control over the user-generated content they host, making it a challenge to apply traditional media regulatory approaches. Social media platforms often enjoy specific legal protections as online intermediaries, shielding them from liability for user-generated content, for example via Section 230 of the 1996 Communications Decency Act in the United States.

Part of the challenges governments face in finding the right mix of approaches to protect information integrity owes to the global scope and reach of online platforms. Policies are typically implemented within jurisdictions whose size – even if encompassing multiple countries, as in the European Union – does not match the global scope and reach of online platforms. Such mismatch is a particular challenge when it comes to increasing platform transparency, since fragmented and inconsistent international obligations hinder the development of a comprehensive picture of data flows and information integrity risks, policies put in place to mitigate them, and the related results in the online information environment (Lai, Shiffman and Wanless, 2023[4]). Additionally, the role of private ownership of online platforms, which are effectively public spaces for news dissemination and debate often operating opaquely under their own terms of service and community guidelines, is important to bear in mind. Together, this context limits understanding of how information flows and, consequently, what policies work to mitigate the harms of disinformation.

To this end, governments can prioritise, as appropriate:

- Moving beyond self-regulation and clarifying the role and strategies of state-led policies, and
- Policy levers to encourage accountability and transparency.

2.2.1. Moving beyond self-regulation and clarifying the role and strategies of state-led policies

Self-regulation, which takes place when a group of firms or individuals exert control over their own membership and behaviour, has to date been the predominant approach taken in setting standards for online platforms. In information integrity, self-regulation refers to voluntary compliance to codes of conduct, guidelines, and other mechanisms to address issues like content moderation, privacy, or ethical practices. Such mechanisms are widely considered to benefit from the higher levels of relevant expertise and technical knowledge of the industry – in this case the platforms themselves – which in turn helps drive greater effectiveness and efficiency.

Notably, self-regulation can incorporate diverse arrangements, from completely private to varying degrees of government engagement, including around government involvement in developing or approving draft rules (Baldwin, Cave and Lodge, 2011[5]). Self-regulation allows for flexibility and industry-specific approaches; particularly for media and journalism organisations, this approach can play an important role in building capacity of news organisations to develop quality, factual content and prevent the inadvertent spread of misinformation. Self-regulatory mechanisms, such as press councils, can also play a critical role in monitoring the abuse of laws against journalists and advocating on their behalf (Lim and Bradshaw, 2023[6]).

For example, the Santa Clara Principles present a prominent self-regulatory effort focused on issues of information integrity and transparency that is not led by governments.[1] Adopted in 2018, these principles are a voluntary set of recommendations for companies that are designed to provide transparency and meaningful due process to impacted users of online platforms. The principles call for clarity of platforms' content moderation efforts; clear notice to affected users; and a robust appeals process. The Santa Clara Principles are designed to help guide, evaluate, and compare companies' practices and activities. Additionally, the Coalition for Content Provenance and Authenticity (C2PA) seeks to increase transparency of specific content. The C2PA was founded February 2021 by Microsoft and Adobe and included Arm, BBC, Intel, and Truepic; today, membership also includes Google, Sony, Meta, OpenAI, and several camera manufacturers, content creators, and non-governmental organisations. It addresses disinformation online by creating technical standards for certifying the source and history (or provenance) of specific content, to help verify who, how, when, and where it was created or edited, should the authors wish to include that information.[2]

In the Netherlands, the Ministry of the Interior and Kingdom Relations developed a Code of Conduct Transparency Online Political Advertisements in 2021 to prevent the spread of misleading information during elections, highlighting the potential involvement of the state in otherwise self-regulatory initiatives. The Code of Conduct is voluntary and open to all political parties and online platforms to help promote "transparency, privacy, security, fairness, and integrity of elections." Notably, participation is voluntary and the code of conduct notes that it does not replace other regulatory initiatives. While compliance is not enforceable, the code provides a signaling function of illustrating good conduct (at its launch, 11 out of 13 parliamentary parties and Facebook, Google, Snapchat, and TikTok had signed) (Government of the Netherlands, 2021[7]).

And yet, without democratic oversight or reporting requirements, self-regulatory regimes may generate questions of accountability. What is more, where self-regulation operates as a voluntary mechanism, the public may end up being ill-protected by regimes that effectively control the most responsible members of a field but leave unregulated those firms that are least inclined to serve the public or consumer interest (Baldwin, Cave and Lodge, 2011[5]).

X's announcement in May 2023 that it was withdrawing from its voluntary participation in the 2018 European Union Code of Practice on Disinformation[3] points to the limitations of voluntary codes of practice and principles (Lomas, 2023[8]). The Code was the first self-regulatory instrument to which leading industry actors, including Facebook, Google, Microsoft, Mozilla, TikTok, and Twitter (now X), voluntarily agreed. X's withdrawal was preceded by an announcement in February 2023 by the European Commission that the company's first baseline transparency report for the Code of Practice fell short of the expectations set by the other platforms in terms of the data it provided and information on commitments to work with fact checkers (European Commission, 2023[9]), further clarifying the challenge self-regulatory tools pose in enabling transparent, consistent, and comprehensive monitoring and reporting.

Mitigating the challenges of voluntary self-regulation, co-regulatory approaches incorporate industry expertise and self-governance and can allow for governments to take over oversight, enforcement, or ratification of self-regulation mechanisms (Baldwin, Cave and Lodge, 2011[5]). For example, the European Code of Practice was updated and revised in 2022, with the aim for it to become a co-regulatory instrument and serve as a strengthened monitoring framework under the Digital Services Act's (DSA) framework. The updated version of the Code contains 44 commitments and 128 specific measures covering issues around demonetisation and reducing financial incentives for spreaders of disinformation; increasing transparency of political advertising; reducing manipulative behaviour and fake accounts; supporting researcher access to platforms' data; among others.

In Australia, the Code of Practice on Disinformation and Misinformation was published in February 2021 by the Digital Industry Group Inc. (DIGI). While the code is voluntary and aims to provide safeguards against harms from the spread of false and misleading content on digital platforms, the Australian Communications and Media Authority (ACMA) oversees the Code of Practice and works with DIGI and the signatories to assess signatories' transparency reports, examine how signatories handle user complaints, and encourage more platforms to sign up to the code (see Box 2.1).

Box 2.1. Australia – Voluntary Code of Practice on Disinformation and Misinformation

Based on the Australian government's request in 2019 and learnings from the European Union's Code of Practice on Disinformation, the Digital Industry Group Inc (DIGI), a non-profit industry association, published the Australian Code of Practice on Disinformation and Misinformation in 2021. The aim of the code is to provide transparency about the safeguards digital platforms employ against harms from the spread of disinformation and misinformation.

The voluntary code currently has eight signatories: Adobe, Apple, Google, Meta, Microsoft, Redbubble, TikTok and Twitch. All signatories commit to:

- reducing the risk of harms arising from disinformation and misinformation; and
- publishing an annual transparency report about the steps they are taking to combat misinformation and disinformation.

Depending on the nature of their service, signatories may also commit to providing information about their efforts to:

- disrupting advertising and monetisation incentives for the spread of mis- and disinformation
- working to ensure the security and integrity of the platform's services and products
- empowering users to make better-informed choices of digital content and helping them identify false and misleading content
- increasing transparency around political advertising
- supporting research that improves public understanding of mis- and disinformation.

DIGI is the administrator of the Code. In October 2021, DIGI strengthened the code by instituting a governance framework and establishing a complaints facility for the public to report breaches by signatories of their commitments. In December 2022, DIGI published an updated version of the Code. Updates focused on making it easier for smaller companies to adopt the Code and clarifying the specific products and services covered.

While the ACMA currently has no formal regulatory role in relation to disinformation and misinformation, it oversees the operation of the Code, which includes reporting on digital platforms' disinformation and news quality measures and engaging consistently with DIGI, signatories and other parties on the operation of, and potential improvements to, the Code, and encourages more platforms to join.

Source: Government of Australia (2024[10]), "Online misinformation", Australian Communications and Media Authority, https ://www.acma.gov.au/online-misinformation.

The limitations posed by existing self- and co-regulatory regimes increase the risk that they will not sufficiently mitigate the threats posed by those actors that do the most to undermine information integrity in democracies, as well as by those who merely do not wish to engage. Such risks point to the importance of government involvement in designing, enforcing, and updating regulatory responses, where relevant and appropriate. While designing policies that protect and promote freedom of expression and active, well-informed democratic debate require engagement with civil society and private sector actors, responses cannot be left to them alone. This said, these self-regulatory efforts have had value over the years in fostering dialogue between governments and platforms on the issues at stake and helping to identify the various policy options at hand. These experiences provide an important basis on which to build.

2.2.2. Policy levers to encourage accountability and transparency

As noted in the introduction, given risks to freedom of expression that content-specific policies raise, responses should largely focus on clarifying the responsibilities online platforms have regarding their role as essential actors in the information space. In this respect, governments should ensure a clear and predictable legal framework, where the rules are clear to avoid incentivising privatised censorship (Council of Europe, 2021[11]).

Furthermore, the largely opaque operations of major tech companies prevent understanding of the role of online platforms in shaping the information environment and the actions they have taken to mitigate harmful behaviours (Lai, Shiffman and Wanless, 2023[4]). Strategies focused on increasing transparency can help build understanding around how online platforms operate and can help ensure that online platforms' rules and implementation are clear, predictable, and proportionate. Because of the information asymmetry between online platforms and governments about how content is spread and what interventions work, transparency is also an important tool in helping governments and independent researchers better understand the information space, which in turn will help monitor the impact and effectiveness of responses and inform policymaking (OECD, 2022[3]). This opportunity speaks to the broader need to enhance measurement capabilities of relevant policy actions in this space.

Online platforms do not generally have an incentive to share information with researchers, regulators, or the public on policies, processes, algorithms, or content flows primarily due to cost, privacy, and competition concerns. By making information more accessible and accurate, policies may help ensure information is provided to facilitate better understanding of the information space and the actors therein and allow for independent verification of platform claims. Risks in other industries provide meaningful examples in this respect: until governments required its disclosure, accurate information was unavailable to the public in markets as diverse as the nicotine content of cigarettes, fuel economy for cars, or food safety (Baldwin, Cave and Lodge, 2011[5]).

Several laws have recently been implemented or discussed that focus on a wide range of transparency issues. The European Union's Digital Services Act (DSA), the UK Online Safety Act, as well as draft U.S. legislation, such as the Digital Services Oversight and Safety Act, and the Platform Accountability and Consumer Transparency Act, all reflect growing demands for greater platform transparency (Lai, Shiffman and Wanless, 2023[4]). Government regulation to promote transparency and accountability can also build on existing or similar self-regulatory efforts, as seen in the European Union, where the voluntary Code of Practice on Disinformation is now embedded in the DSA.

Greater transparency is only part of the solution for the problem of information manipulation on social platforms. Artificial amplification of content, for example via social media bots disguised as human users, can distort conversations online by boosting the apparent popularity of certain messages and accounts. This artificial amplification can be particularly harmful during elections, natural disasters, or other crisis situations.

Governments are increasingly identifying policy responses to improve the authenticity of the information space online. For example, in 2018, California introduced the Bolstering Online Transparency Act (BOT Act), which prohibits online bots from hiding their identities to appear as a human user (State of California, 2018[12]). In 2023, the Lithuanian Parliament began discussions regarding amendments to the Law on Public Information and the Criminal Code, which could give Lithuanian government the right to order social platforms and other information providers to "remove artificially increased numbers of page views, comments, shares, likes, followers, and/or subscribers of content within eight hours, or to withdraw the possibility of access to this content." The discussions also included the potential for criminal sanctions and imprisonment for the artificial dissemination of content on platforms.[4]

Across policy responses, consideration should be given to their potential impact on competition. Larger online platforms are better equipped to navigate more onerous liability and transparency rules (such as through buying or developing filtering technologies and complying with deadlines for removing and reporting on content) (Council of Europe, 2021[11]). Specifically, it may be useful to vary the extent and burden of mandated transparency relative to a platform's size, so that compliance does not become a barrier to entry. For example, the DSA imposes additional requirements for Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) related to identifying and auditing systemic risk, enhanced transparency reporting on content moderation, advertising transparency, and access to data about content shared on the platforms (European Union, 2022[13]).

Ultimately, it is important to outline the specific objectives, values, and aims that increased transparency requirements are seeking to achieve, as there are several trade-offs and considerations that governments should bear in mind. Regulations in this space, where relevant, should be guided by proportionality, as designing and delivering regulations in a proportional way is an essential approach to improving efficiency, strengthening effectiveness, and avoiding unnecessary administrative burden (OECD, 2021[14]). Policy responses focused on platforms should be used as a mechanism by which governments – and the public more widely – can better comprehend and respond to the behaviours and business models of key actors whose technology dominates that space, understand and mitigate specific risks, and build knowledge of the information environment more widely.

To that end, policies encouraging accountability and transparency for online platforms and services may apply to a wide range of topics, including:

- the role of online intermediary liability protection in balancing platforms' roles and responsibilities,
- transparency around moderation policies and policy development, risk assessment and management processes, and algorithms, to provide valuable comparative information on how online platforms operate, and
- Increased transparency of online platform behaviour and content data to build understanding of the information space.

Online intermediary liability regimes should clarify platforms' roles and responsibilities

A key regulation in the information space concerns online intermediary liability, which establishes the legal responsibility or accountability of intermediaries, such as internet service providers or social media platforms, for the content shared or created by their users. The growing importance of online intermediaries in how people get and share information has heightened the emphasis on defining their legal liability for harms caused by content shared by – or activities carried out by – users of intermediaries' services (Shmon and Pederson, 2022[15]).

Broadly, online intermediary liability regimes attempt to balance the extent to which platforms are held liable for content shared on their platforms with the need to support freedom of expression, innovation, and promoting an online environment conducive to democratic engagement (Shmon and Pederson, 2022[16]). Intermediary liability regimes, and the "safe harbour" they provide to liability for user-generated content, range in scope. These laws generally try to weigh three goals: 1) enabling platforms to take content moderation actions (indeed, platforms typically have greater obligations and fewer legal protections for content that poses the greatest threats or that is otherwise illegal); 2) protecting speech and public participation by reducing platforms' incentives to over-enforce or restrict users' lawful speech unnecessarily; and 3) encouraging innovation and economic growth by providing space for market entrants to develop and build platforms by shielding them from being exposed to overly burdensome moderation requirements or legal risk (Keller, 2019[17]). Related to the information space, intermediary liability laws are particularly relevant for enabling platforms to pursue content moderation decisions for content that is not otherwise illegal, while reducing the incentive for imposing undue restrictions on speech.

Section 230 of the United States Communications Decency Act of 1996 is an example of an immunity-based approach. This clause has widely been seen to be instrumental in fostering innovation and growth of the internet and online platforms (OECD, 2011[18]). Section 230 provides immunity from liability to providers and users of an "interactive computer service" that publish information provided by users of the platforms. This protection has empowered online services to develop and maintain open platforms that facilitate free expression (OECD, 2011[18]). Section 230 also, importantly, removes liability for platform decisions regarding moderation, filtering, and amplification of user-generated content, enabling platforms to moderate and disseminate content largely as they see fit (see Box 2.2 for the specific language).

Box 2.2. Relevant language from Section 230 of the United States Communications Decency Act (1996)

(1) "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) No provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."

(Per the law, "the term 'information content provider' means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service.")

Section 230 does not, however, extend to immunity violations of federal criminal law, intellectual property law or electronic communications privacy law.

Source: For more information, see Communications Decency Act, 47 U.S.C. § 230 (1996).

The immunity approach has also, however, led to criticisms regarding lack of accountability of online platforms (or "duty-of-care") for the content they host. The aim of this approach, as seen, for example, in the UK Online Safety Act of 2023, is for online platforms to take measures to assess risks, as well as prevent and mitigate reasonably foreseeable harmful and illegal content. Beyond broad immunity, there are three common, and not mutually exclusive, approaches to narrowing intermediary liability. For example, the awareness or "actual knowledge" approach holds websites and online platforms accountable only for content of which they are aware or have "actual knowledge". Japan's Provider Liability Limitation Act, enacted in 2001, falls into this category. A second approach is the "notice and takedown" approach, which requires online services to comply with judicial requests. The 2014 Brazilian Marco Civil da Internet, for example, provides general liability exemption for content generated by third parties, with exceptions for copyright, unauthorised disclosure of private images containing nudity and/or sexual activities, and obligations to comply with judicial decisions ordering content removal.[5] Furthermore, New Zealand's Harmful Digital Communications Act 2015 provides liability exemption if websites comply with notice of complaint processes.

The scale of content shared online will continue to make private platforms powerful actors in determining what is seen and shared; privately owned platforms will by necessity continue to serve as moderators for conversation and debate among citizens (Douek, 2021[19]). To that end, intermediary liability protections should be designed in a way that fosters a free and open internet while enabling platform responsibility to address legitimate concerns around false, misleading, and otherwise harmful or illegal content.

Increasing transparency and understanding of how online platforms are designed and function

Broadly, disclosure requirements allow consumers to make decisions on their acceptability of the processes employed in producing products or services (Baldwin, Cave and Lodge, 2011[5]). One avenue for mandating transparency therefore includes a focus on the policies, policy development, processes, and algorithms employed by online platforms. Requiring platforms to disclose information on terms of service and privacy policies; disclosure on use of behavioural data and user data shared with third parties; procedures, guidelines, and tools that inform the content moderation and algorithmic decision making; and processes of complaint handling can empower users to better understand data handling practices and rule enforcement. Disclosures can play a useful role in safeguarding users' rights and promoting accountability by platforms, as public scrutiny can highlight potential biases or unfair practices. Clarifying these processes may also reduce concerns of those companies that advertise on online platforms of reputational risks to being associated with the spread of disinformation, facilitating a market-based inducement to healthier online information spaces.

The goal of policies in this space is to “institutionalise, incentivise, and verify” the rules and systems that platforms and other relevant actors put in place to oversee the information spaces they control (Douek, 2021[19]). These transparency requirements are particularly important given the rapid evolution of platform practices and policies, as they allow regulators and the public to verify the effectiveness of the rules and content moderation systems online platforms have put in place. Such oversight can also help identify blind spots in company processes (Douek, 2021[19]).

For example, individuals are often unaware of how their online statements, content, and behaviour are turned into data and how algorithms used by online platforms sort content to profile and target them through advertising (OECD, 2022[20]). Efforts to increase transparency of privacy policies of online platforms can provide users with valuable information on how their personal data is used.

These discussions, however, cannot be separated from broader privacy debates across democracies. Specifically, privacy regulations can limit the unchecked gathering of personal information, making it harder for malicious or other actors to manipulate or influence individuals through targeted content. By limiting access to the information that enables personalised targeting and polarising messages, data privacy laws can potentially help prevent unwanted message targeting (Campbell, 2019[21]). The GDPR (General Data Protection Regulation) in the European Union, for example, provides a wide range of legal provisions designed to safeguard individuals' personal data and privacy rights, including that organisations that collect, process, or store personal information obtain explicit consent for data processing, provide transparent privacy policies, and ensure appropriate security measures. Additionally, these laws grant individuals greater control over their data, including the right to access, correct, or erase their information, as well as the right to know how their data is being used (European Council, 2022[22]). By safeguarding individuals' personal data and enforcing data handling practices, privacy laws can create a more transparent and accountable environment online.

Transparency requirements may also increase information sharing on platform architecture and algorithms. There is a limited public understanding of how the algorithms that drive information curation, amplification, and engagement on platforms are developed and deployed. These algorithms, in turn, have faced criticism for helping to drive radicalisation of users and promoting and amplifying harmful content. To address these concerns, transparency requirements can enable greater understanding of the kinds of algorithms used by online platforms and provide insight into their impacts and consequences (Lai, Shiffman and Wanless, 2023[4]).

Legislation could enable researchers and regulators (as the DSA does in the EU market) to have greater insight into the algorithms used in content moderation, prioritisation, advertising, and recommendation, as well as how these algorithms affect the spread of content on the platforms. These insights would allow for external and independent assessment to better inform policymakers and the public of information integrity risks and help guide policies to mitigate them (MacCarthy, 2021[23]).

Facilitating the standardisation of the information provided regarding how online services formulate, communicate, and enforce their rules can encourage the creation of best practices for public policy development and inform ways to measure the impact of those interventions (Lai, Shiffman and Wanless, 2023[4]). The DSA includes requirements for the publication of transparency reports and more information about content moderation and terms of service. The Australian Government’s draft Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill[6] proposes new powers for the independent regulator, the Australian Communications and Media Authority’s (ACMA), which aim to address harmful misinformation and disinformation online, while upholding the right to freedom of expression that is fundamental to democracy. The proposed powers are consistent with the key recommendations in the ACMA's June 2021 *Report to government on the adequacy of digital platforms' disinformation and news quality measures*. One of the key elements proposed in the report is a focus on enabling the ACMA to gather information from digital platform providers on their systems and processes to combat harmful online misinformation and disinformation (see Box 2.3).

Box 2.3. Overview of Australia's Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill

On 20 January 2023, the Australian Government announced its intention to introduce new legislation granting ACMA proposed new powers to combat harmful online misinformation and disinformation.

On 25 June 2023, the Australian Government released an exposure draft of the Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill for public consultation, which closed on 20 August 2023. The Bill focuses on improving digital platforms' transparency around how they handle and manage misinformation and disinformation on their services. The draft Bill builds on the existing voluntary Australian Code of Practice on Disinformation and Misinformation that major digital platforms have already signed up to.

The main objectives of the draft Bill are to provide new functions to ACMA to encourage, and if needed require, online platforms to take steps to counter the threat posed by the spread of misinformation and disinformation. The draft Bill proposes new powers for the ACMA, including record-keeping, information gathering, and would reserve code- and standard-making powers. The powers would:

- enable the ACMA to gather information from digital platform providers, or require them to keep certain records about matters regarding misinformation and disinformation
- enable the ACMA to request and assist industry to develop a code of practice covering measures to combat misinformation and disinformation on digital platforms, which the ACMA could register and enforce
- allow the ACMA to create and enforce an industry standard (a stronger form of regulation), should a code of practice be deemed ineffective in combatting misinformation and disinformation on digital platforms.

The draft Bill also includes a number of safeguards to protect freedom of speech and public debate and the framework would be open to regular system reviews and parliamentary oversight.

Source: Australian Competition and Consumer Commission (2019[24]), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf; Australian Government (2023[25]), *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—guidance note*, https://www.infrastructure.gov.au/department/media/publications/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-guidance.

Increasing transparency of information flows and content on online platforms

Beyond process and policy transparency, countries have used policies around the sharing of metadata with external researchers to build general understanding around disinformation flows and how platforms moderate or remove (or not) types of content. Data transparency requirements for online platforms can provide valuable insights and context about user interactions and behaviours, information flows within and across platforms, and patterns of engagement, all of which can facilitate the development of a robust evidence-base for measurement moving forward.

Increasing access to behaviour and content data to build societal understanding of the information space online

Increased clarity and consistency of information provided could help build a better understanding around what data is most helpful when designing and measuring the impact of interventions. These transparency efforts may also continue to identify specifically how such data can be provided and analysed in a way that respects privacy and competition concerns and clearly outlines which actors have access to data (Lai, Shiffman and Wanless, 2023[4]). Given the importance of online platforms in the information space, facilitating greater transparency about how content is spread across their platforms will likely be a necessary component to better understand the information space. Finally, increasing the visibility into actions of online platforms and the way content flows may help provide an incentive for them to clarify and improve content moderation policies and actions (MacCarthy, 2021[23]).

One category of relevant data includes user-level information to provide general insights into who the users of platforms are and how they engage on the platform. Reporting may include aggregated information about types of users (using age groups, gender, and location data). It may also include types of content of public posts, comments, and engagement. Such public data (not including private posts or messages) that does not include personally identifiable information could provide a helpful baseline of what groups are most active and common types of online behaviour to help identify patterns and changes over time (Lai, Shiffman and Wanless, 2023[4]).

Enabling independent researchers to verify and confirm platforms' public disclosures could be a useful model to help hold services accountable. Mandating that steps are taken to ensure research is conducted for legitimate aims and that researchers implement privacy and security protections for datasets used will be important guardrails to prevent abuse (Goldman, 2022[26]) (Forum on Information and Democracy, 2020[27]). Transparency requirements do not necessarily mean the information will be made public; indeed, the level of detail required can and probably should differ across audiences, given the risk that potentially sensitive content may be misused if made available to the public (Lai, Shiffman and Wanless, 2023[4]).

For example, Article 40 of the Digital Services Act (DSA) gives digital regulators within each EU member states the ability to mandate that platforms share data with researchers under clearly outlined processes (see Box 2.4).[7] While questions remain around compliance, including whether researcher access programmes can be extended to other countries and how to handle data of residents outside of Europe, the DSA puts into practice many of the aims of this category of transparency regulation (Lenhart, 2023[28]).

Box 2.4. DSA Article 40 – Data access and scrutiny

Article 40 of the DSA is designed to promote transparency of data held by online platforms and to facilitate public interest research that will build understanding of how online platforms work. Specifically, it provides the process by which "vetted researchers" can apply for specific public data accessible on online interfaces to "conduct research that contributes to the detection, identification and understanding of systemic risks." The DSA also notes that very large online platforms and very large online search engines shall be required to respond to data access requests, and provide the data to the researchers unless providing access to the data "will lead to significant vulnerabilities in the security of their service or the protection of confidential information…and trade secrets."

Notably, the DSA also establishes 'vetted researchers', who are given the ability to apply for specific data requests. Digital services co-ordinators, who will co-ordinate and oversea the application of the DSA, will grant this status to researchers who:

- demonstrate that they are affiliated to a recognised research organisation
- demonstrate that they are independent from commercial interests
- disclose the funding of the research
- demonstrate that they can fulfil the specific data security and confidentiality requirements, that they can protect personal data, and that they describe in their request the appropriate technical and organisational measures that they have put in place
- demonstrate that their requests are proportionate to the purposes of their research, and that the expected results of that research will contribute to the public interest
- commit to making their research results publicly available free of charge, within a reasonable period after the completion of the research.

Source: European Union (2022[13]), Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?ur.

Reporting requirements could also include greater transparency around requests from third parties, such as researchers and data brokerage firms, for access to data. As it stands, there is a limited understanding of who has access to user data and how that data is used. Governments could therefore require additional reporting by platforms on data sharing with third parties, including on whom platforms sell data to, who they buy data from (such as data brokers), and information on the relationships that platforms have with other actors who handle, buy, request, or have access to user data (Lai, Shiffman and Wanless, 2023[4]). Illuminating these relationships could be a useful mechanism to track data flows and better understand who has access to what kinds of information. To that end, privacy laws may be helpful in clarifying what personal data is considered public while also clarifying the acceptable use of data for research (Lenhart, 2023[28]).

Researchers would also benefit from greater harmonisation and facilitation of data access. Removing barriers to access could reduce costs and allow more informative analysis across multiple social media networks and countries. Facilitating cross-border research, for example clarifying areas of potential legal conflict and exploring compromise on data sharing or safe harbours that allow cross-border access to data for researchers, will be particularly useful to develop a cross-border understanding of the information space (Lenhart, 2023[28]). This again would require upholding privacy rights, securing proprietary corporate information, and avoiding capture by commercial and government interests, though the aim of data collaboration could facilitate a more harmonised approach to building resilience and improving information integrity (Scott, 2023[29]).

Increasing transparency of political advertisements on online platforms

Policies may also seek to increase transparency around political advertisements on platforms. Political advertisements are defined as those that are made by or on behalf of a candidate or party, that communicate a message relating to a political matter of national or local importance, or are likely to influence the outcome of an election.[8] The data could include increasing information around provenance of the content (for example, while campaigns and political organisations may be required to report how they spend money on advertisements, the same may not be true for how advertising agencies and consultancies spend money on their behalf, which some research suggests could make up the vast majority of the spending); increasing the detail provided and standardising reporting; and storage and research access to reduce the variation in the data and access provided by existing platform ad libraries (Brennen and Perault, 2021[30]). Increasing information around political advertisers' actions on platforms may also be gathered from reporting requirements on a user's advertising activity. Reporting could include details on the audiences targeted as well as the content of the advertisements. This data could increase understanding around the advertisers' influence targets, at least regarding broad groups of users (Lai, Shiffman and Wanless, 2023[4]).

Several efforts have been made in this direction, including the 2019 decision of Israel's Central Elections Committee, which banned anonymous election ads on all platforms, including social media, from both within Israel and abroad. In effect, the ruling applied the restrictions in the Elections Law (Propaganda Methods) of 1959, which primarily deals with advertising on billboards, radio, TV, regional radio stations, and published election surveys, to advertising on the internet (The Times of Israel, 2019[31]). Most recently, in Europe, the DSA required that platforms provide "information necessary for users to understand when and on whose behalf the advertisement is presented".

Another component of political advertising policy could consider requiring the creation and maintenance of political advertisement databases that are standardised, publicly accessible, and searchable (Brennen and Perault, 2021[30]). In addition to the content of the advertisements, the source of the advertisement and money behind it, as well as targeting data and profiling used, could be included. Such a public repository would be valuable to researchers, advocates, and regulators to better understand the flow of information around elections and policy debates, as well as help inform future regulatory actions, as appropriate (MacCarthy, 2021[23]). Along these lines, the DSA will require Very Large Online Platforms and Very large Online Search Engines to "ensure public access to repositories of advertisements presented on their online interfaces to facilitate supervision and research into emerging risks brought about by the distribution of advertising online

[…] Repositories should include the content of advertisements […] and related data on the advertiser, and, if different, the natural or legal person who paid for the advertisement, and the delivery of the advertisement, in particular where targeted advertising is concerned (European Union, 2022[13]).”

2.3. PROMOTING PLURALISTIC, INDEPENDENT, AND COMPETITIVE MEDIA AND INFORMATION MARKETS

A diverse and independent media sector, and an information ecosystem that supports journalism and facilitates the creation of high-quality news creation, play an essential role in enabling open and democratic societies by providing reliable information, bringing issues to the public agenda, facilitating debate, serving as a watchdog for the public interest, and holding public actors accountable (OECD, 2014[32]). Reduced access to and trust in providers of accurate and verifiable information prevents citizens from accessing shared facts, inhibits informed decision-making and democratic debate, and opens the door for further amplification for the spread of mis- and disinformation.

The 2023 World Press Freedom Index – which evaluates the environment for journalism in 180 countries and territories – reveals that the proportion of OECD countries where the environment is “good” for journalism has more than halved over eight years. While 49% of OECD countries were ranked as "good" in the 2015 World Press Freedom Index, this fell to 21% in 2023. Globally, the share fell from 21% to 4%, which emphasises the relative strength of OECD members (RSF, 2023[33]). Trust data also highlight the challenging dynamics facing traditional media. Notably, only four out of ten (38.8%) respondents to the 2021 OECD Survey on Drivers of Trust in Public Institutions reported trusting the news media (OECD, 2022[34]), and other research found that trust in the news continued to fall globally between 2022-2023 (Newman et al., 2023[2]).

These dynamics are taking place in a context of ongoing threats to the safety of journalists. Estimates of journalists killed worldwide between 2010 and 2020 range from 937 (RSF, 2020[35]) to 956 (UNESCO, 2021[36]). Beyond constituting illegal acts, physical harms, and human rights violations, attacks against journalists limit free expression and deprive others of their rights to receive information, thus hampering freedom of expression, limiting civic space, and reducing the ability for informed public debate (OECD, 2022[20]). In addition to the ensuring freedom of expression, governments must protect journalists, media workers, and researchers, and monitor, investigate, and provide access to justice for threats and attacks against them. This is the aim, notably, of the 2016 Council of Europe Recommendation on the protection of journalism and safety of journalists and other media actors (Council of Europe, 2016[37]). Along a similar line, the Council of Europe Safety of Journalists Platform[9] and the EU Media Freedom Rapid Response (MFRR) Monitor[10] report on serious threats to the safety of journalists and media freedom, while the Council of Europe Journalists Matter is a campaign that seeks to promote press freedom and protect journalists from violence, threats, and harassment while performing their duties.[11]

Traditional media have also faced financial problems due to dwindling advertising revenue, as the advertising market shifted to digital especially to online platforms. In the United States, for example, newspaper publishers in 2020 earned less than half of what they earned in 2002 (United States Department of Justice, 2022[38]). The Australian Competition and Consumer Commission (ACCC) found that the number of journalists in traditional print media businesses fell by 20% from 2014 to 2018 (Australian Competition and Consumer Commission, 2019[24]). Smaller regional media outlets are often particularly hard hit. In the United Kingdom, the regional newspaper advertising market was worth GBP 2.5 billion in the 1990s; at the end of 2022, it was valued at GBP 241 million (Sweney, 2023[39]). Increasing digital subscription are compensating only a minor part of the former incomes.

The decline of small regional media often leaves entire regions without quality local media. The United States has lost almost 2 900 newspapers since 2005 (now leaving only 6 000 newspapers in the country), many of which were the sole provider of local news in small and mid-sized communities. In addition, the country has lost almost two-thirds of its newspaper journalists – 43 000 – in that same period (Medill Local News Initiative, 2023[40]). The Australian government found that there had been a significant reduction in the number of articles published covering local government and local court issues in the 15 years to 2019, which is concerning given the important role such coverage plays in exposing corruption and in holding governments, corporations, and individuals to account (Australian Competition and Consumer Commission, 2019[24]). The "media deserts" created by shortages in local media can lead to vacuums in the information environment that are often filled by news from online platforms and social media, further amplifying the opportunities for mis- and disinformation to spread. Evidence from Germany also shows that the decline of local media outlets has a negative impact on political polarisation (Ellger et al., 2021[41]).

In addition to the focus on online platforms' role in the information space, the structure of traditional media markets remains an essential public policy issue to help ensure the public has the information necessary for effective democratic engagement. Media capture, market concentration, and threats to local and community media can hamper broad public debate and promote one-sided views that can undermine information integrity (OECD, 2022[20]). Government policies can therefore play a constructive role in supporting democratic discourse through the promotion of media freedom, diversity, and independence. While these interventions are not specifically directed at countering disinformation, they nonetheless point to how governments can prioritise shifting media markets to help them serve as a necessary source of information within democracies.

The challenges facing media throughout democracies are a particular concern given the role the sector plays in supporting an informed citizenry, a well-functioning democracy, good governance, and reduced corruption. To that end, government responses designed to strengthen the traditional media sector include:

- Protecting and enhancing journalist safety
- Enhancing transparency and political independence of traditional media, and
- Preventing media capture and supporting a pluralistic and independent media environment

2.3.1. Information integrity requires a focus on journalist safety, transparency, and preventing media capture

Ensuring freedom of opinion and expression requires uncensored and unhindered access to the press and other media. To that end, establishing mechanisms to protect journalists and systematically investigating, monitoring, and providing access to justice for threats and attacks are also essential to ensuring journalists have the freedom to participate fully in the democratic process (OECD, 2022[20]). For example, the modified Luxembourg Criminal Code (*Loi du 7 août 2023 portant modification du Code pénal*) includes new penalties for attacks against journalists during demonstrations. In addition, persons who threaten individuals can be subject to imprisonment, with an aggravating factor if the target is a journalist. The code also specifies that the disclosure of private and professional information ('doxxing') can lead to criminal liability for the perpetrator, with again an aggravating factor if the target is a journalist (Grand Duchy of Luxembourg, 2023[42]).

Beyond a focus specifically on journalists, a related avenue to help prevent interference is to mitigate media capture and promote editorial independence. Media capture refers to situations where individuals or groups exert significant control over media organisations in a way that influences content and coverage. In these contexts, the media's ability to serve its democratic role as a "watchdog" is compromised (Nelson, 2017[43]). The risk of capture of a media outlet by political or private interests increases as the sector becomes more concentrated (Government of France, 2022[44]), where media ownership is consolidated in the hands of a few entities or individuals. These owners can in turn promote one-sided views that can lead to polarisation and impede balanced and diverse democratic debate (OECD, 2022[20]).

Policies can play a role first in maintaining a diverse and pluralistic market for traditional media by limiting market concentration in the sector. For example, policies can take the form of control on cross-media ownership (i.e. controls on joint ownership of broadcast channels in the same geographic region). Indeed, laws designed to prevent concentration proactively often form the main pillar of a state's efforts to guarantee media diversity and prevent concentration of opinion in the media sector (European Audiovisual Observatory, 2016[45]) (Nelson, 2017[43]). Notably, the EU Media Pluralism Monitor[12] is a tool that measures the state of media pluralism across 34 countries and makes recommendations for policy action.

Promoting diversity of media ownership through anti-trust and fair competition rules involves a range of considerations. A report by the French government recommended assessing the impact of transactions on pluralism on a case-by-case basis, using an analysis based on qualitative indicators (promoting diversity of content, independence of information) and quantitative indicators (audience, coverage, economic viability of the operators) (Government of France, 2022[44]). This approach is similar to that taken in the United Kingdom. The 2003 Communications Act outlines public interest considerations for broadcasting and cross-media mergers, including that there be a "sufficient plurality of persons with control of the media enterprises"; that there be a wide range of broadcasting available that is both high quality and calculated to appeal to a wide variety of tastes and interests; and for media to have a genuine commitment to the accuracy and impartiality standards laid out elsewhere in the statute (Government of the UK, 2003[46]). Norway introduced an obligation for media enterprises and owners to provide information about ownership interests to the Norwegian Media Authority in order to create greater transparency, awareness, and knowledge of ownership interests in Norwegian media (Government of Norway, 2016[47]).

Second, policies that reinforce transparency in countries' media markets can play an important role in ensuring media independence from political and commercial interests and freedom from foreign or domestic political influence. Opaque ownership makes it difficult to identify underlying bias, potentially further undermining trust in the news media. Transparency is therefore a necessary – but not sufficient – policy response to reinforcing media plurality and increasing trust in the media sector (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]).

Notably, the European Court of Human Rights has recognised a positive obligation on States that are parties to the European Convention on Human Rights to "put in place an appropriate legislative and administrative framework to guarantee effective [media] pluralism" and that such plurality cannot be fully effective without clear information. To that end, it recognised the value of media transparency and independence to democracy, specifically in the interests of individuals in having access to information "on all matters of public interest" and the ability of the media to perform their "vital role of 'public watchdog'" (European Court of Human Rights, 2001[49]). In addition, the 2018 Council of Europe Recommendation on media pluralism and transparency of media ownership notes that media freedom and pluralism are "crucial corollaries of the right to freedom of expression…and… are central to the functioning of a democratic society as they help to ensure the availability and accessibility of diverse information and views, on the basis of which individuals can form and express their opinions and exchange information and ideas" (Council of Europe, 2018[50]).

Requirements include transparency around media ownership, for example, by mandating full disclosure of owners, the size of the shareholdings, and their other economic and political interests. Ownership should refer to the "beneficial owner," or the "natural person(s) who ultimately owns[…]and/or exercises ultimate effective control (FATF, 2023[51])." The information provided should also "identify the natural person(s) who are the beneficial owner(s), and the means and mechanisms through ownership, control or other means (FATF, 2023[51])." Such information can provide policymakers, regulators, and the public with the relevant data needed to develop, monitor, and enforce ownership limits and prevent capture (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]). More can be done in this space. In Europe, for example, while most countries (24 of 31)[13] require the disclosure of ownership information to public bodies, a minority (14 of 31) require disclosure to the public (Craufurd Smith, Klimkiewicz and Ostling, 2021[48]). In addition to beneficial ownership, information should also cover details of financial and other relations that could result in editorial influence and conflicts of interest, such as ownership in other industries with significant government interests, the holding of political office, and ensuring that government advertising budgets are allocated in an open and competitive way and independent of political influence (Nelson, 2017[43]).

Third, governments may also take clear positions on enforcing editorial independence. For example, Norway's Media Liability Act seeks "to facilitate open and informed public debate by ensuring editorial independence" by mandating that publishers appoint an independent editor. Specifically, this means that the owner or company management "cannot instruct or overrule the editor on editorial issues, nor can they demand to have access to…material before it is made available to the public."[14]

For its part, the proposed European Media Freedom Act seeks to protect media independence by strengthening safeguards against political interference in editorial decisions, as well as promoting transparency of media ownership and of the allocation of state advertising. It also seeks to defend media pluralism by promoting the stable funding of public service media and requiring member states to assess the impact of media market concentrations on media pluralism and editorial independence and to create a new independent European Board for Media Services, comprised of national media authorities. Importantly, it also includes safeguards against the unjustified removal of media content produced according to professional standards. This "media privilege" considers membership of press councils as one of the benchmarks for identifying reliable news media, and broadly seeks to promote media and journalism's role in democratic discourse (European Commission, 2022[52]).

2.3.2. Governments can play an important role in supporting a diverse and independent media environment

Quality journalism is important for democracy and states should put in place effective policies to support it (Council of Europe, 2023[53]). Quality journalism, in particular quality investigative journalism, requires important financial resources. Governments can play an important role in supporting the survival and transformation of the media sector by providing various means of financial support, with safeguards around government influence on content.[15] At the national level, funding can take the form of support for independent public service broadcasters; direct subsidies and competitive or selective funds for private or non-profit media; and indirect measures such as tax subsidies. Governments may also provide Official Development Assistance (ODA) as a part of their efforts to support and develop diverse and independent journalism in aid-recipient countries (Forum on Information and Democracy, 2021[54]).

National-level support mechanisms

Independent public service broadcasters, which are partly or fully funded by public funds but are nevertheless editorially independent,[16] can play an instrumental role in strengthening information integrity, as they are seen as important sources of news in most OECD countries. Many public broadcasters also have a fact-checking function that enables them to play a direct role in countering disinformation. Examples include "*Vrai ou Faux*" by Franceinfo, a joint initiative by two French broadcasters, Radio France and France Télévision, as well fact-checking branches at Deutsche Welle and in the Lithuanian and Estonian public broadcasters. The Australian Broadcasting Corporation (ABC) also partners with Royal Melbourne Institute of Technology (RMIT) on "RMIT ABC Fact Check" to determine the accuracy of claims by politicians, public figures, advocacy groups, and institutions engaged in the public debate.

Direct and indirect financial support from governments may also go toward private media outlets that meet specific audience or other criteria, often in the form special taxation regimes and discounts on postage fees. Direct government support and indirect measures such as tax incentives remain important tools in supporting news media, provided they are transparent, objective and predictable (Council of Europe, 2023[53]). These policies have a historical legacy – in the United States, the Postal Service Act of 1792 provided postal subsidies as an indirect way of using public funds to support the economics of local newspapers (Medill Local News Initiative, 2023[40]). Within Europe, such indirect subsidies are the most common form of state subsidy, with 19 of 24 countries in a recent study having put in place transparent rules to allocate indirect subsidies. Such subsidies are widely considered less risky than more direct interventions given that indirect subsidies are harder to distribute in a selective way (Bleyer-Simon and Nenadić, 2021[55]). For example, in Norway, media organisations receive a value-added tax exemption (25%), not including certain electronic news services. Research has found that in high-income countries, indirect subsidies such as VAT exemptions for private print media and newspapers match and sometimes outweigh direct subsidies to public service media (Forum on Information and Democracy, 2021[54]).

Governments may also provide direct financial support, including for cultural, minority language media or for investigative journalism, fact checking projects, or for broader support and capacity building for traditional (particularly local and regional) media. Belgium created the *Fonds pour le journalisme* in 2009, which provides funding directly journalists and is managed independently by the Belgian Association of Professional Journalists. Additionally, the Luxembourg Law of 30 July 2021 ties the amount of aid available for the media sector to the quantity of professional journalists employed by the outlet, recognised as such by the independent press council and subject to the sector's self-regulatory code. An advisory commission with members of the press and editors, the national university, and members of the Government administration analyse the criteria and oversee the 10 million annual support budget (Grand Duchy of Luxembourg, 2021[56]).

Direct funding is often limited or available for special content, such as minority language media or the promotion of specific topics. The Italian Budget Law of 2024, for example, funded a system of support for the media industry through a permanent "Single Fund for Pluralism and Digital Innovation in the Information and Media Publishing Sector." Among others, the eligibility requirements for receiving funds include minimum salary levels and staffing a minimum number of professional journalists with full-time, permanent contracts (at least four journalists for publishers of daily newspapers and at least two journalists for publishers of periodicals). Allocations will also favour publishers that recruit journalists and professionals aged 35 years or less, with professional skills in the fields of digital publishing, communication and cybersecurity, and with a focus on countering disinformation (Gazzetta Ufficiale, 2023[57]). Finland, furthermore, provides EUR 800 000 to cultural magazines and EUR 500 000 to minority language newspapers (Bleyer-Simon and Nenadić, 2021[55]). Provided the funds are allocated in a transparent, publicly accountable, and relatively predictable manner, direct subsidies can be important tools to support the media and information space (Forum on Information and Democracy, 2021[54]).

Governments may financially support private media by buying advertisements. However, such direct support must be done in a transparent and impartial way to prevent media capture by the government or elected officials. If not done transparently and impartially, state advertising can be a problematic form of support that may be used to buy or maintain political influence. Notably, within the European Union, 19 of 24 countries recently studied do not have guidelines to transparently allocate state advertising among news media (Bleyer-Simon and Nenadić, 2021[55]).

For its part, Ireland's Future of Media Commission Report recommended expanding the media sector and increasing its plurality by adapting the current Broadcasting Fund into a platform-neutral "Media Fund" to finance schemes for public service content providers, including for local news reporting and supporting the digital transformation. The report also recommends reducing tax for newspapers and digital publications and for investments in non-profit media organisations to receive tax exemptions (Government of Ireland, 2022[58]).

Support measures can also be directed at reaching vulnerable and hard to reach groups. For example, the Estonian government supports Russian language content creation, which is seen as an efficient means to provide reliable information to non-Estonian speakers in the country. This information is designed to compete with Russian state-funded propaganda aimed at the non-Estonian-speaking minority. Funding went to public broadcaster ERR as well as private media outlets. The support programme was created in co-operation with the media outlets with specific attention to freedom of expression and political neutrality (ERR, 2023[59]).

Community media is another important element in ensuring a diverse and free media environment. Community media broadly refers to broadcasting, newspapers and multimedia outlets that are independent from governments, commercial institutions and political parties and directed by and largely owned by local communities and/or communities of interest which they serve (Chapman, Bellardi and Peissl, 2020[60]). One avenue for government action is through building out the internet infrastructure to enable the growth of local and community news providers. Areas without broadband connections or with high internet connection costs have reduced economic incentives for broadcast outlets and digital start-ups to provide news and information to residents in those communities. Addressing issues around the lack of access to high-speed internet, including in places that also have lost local news sources, can (among other positive outcomes) help reduce the digital divide and strengthen the competitive field for local and community news providers (Medill Local News Initiative, 2023[40]).

The importance of community media is reiterated in the Council of Europe's Recommendation on Media Pluralism and Transparency of Media Ownership, which encourages member states to "support the establishment and functioning of minority, regional, local and not-for-profit community media, including by providing financial mechanisms to foster their development (Council of Europe, 2018[50]).” Similarly, the Organisation for Security and Co-operation in Europe (OSCE) recommends that states recognise the distinct nature of not-for-profit community media, guarantee their independence, and allow them to provide members of the communities they serve with opportunities and training that enable them to produce their own media content (OSCE, 2019[61]).

Luxembourg has put in place a financial aid mechanism of EUR 100 000 per year for community media outlets that rely on the voluntary participation of individuals in editorial activities and that support media education, integration, and social cohesion (Grand Duchy of Luxembourg, 2021[56]). For its part, as of 2020, the United Kingdom had 255 community radio stations, reaching 3.5 million local listeners and involving 20 000 volunteers (Chapman, Bellardi and Peissl, 2020[60]). In addition to adding to the diversity of a country’s media ecosystem, facilitating public engagement in the production of locally relevant journalism can serve as an important venue for building media literacy.

International efforts to strengthen media and information environments

Government support for a diverse and independent media sector is also recognised as a priority for international co-operation and development. In many countries, development agencies are supporting information integrity through partnerships with local media outlets and journalists working in the field. ODA for media and information environments has increased from USD 325 million in 2002 to USD 1.2 billion in 2021. However, this represented only 0.5% of total ODA in 2021, and excluding investments in infrastructure (such as broadband and telephone connections), ODA for media and information has remained flat at around USD 500 million per year since 2008 (OECD, 2024[62]).

Development assistance to media and information generally falls within three policy areas. First is a focus on strengthening government initiatives. These projects support efforts to promote freedom of expression, media support for governance and accountability (including media sector development and the role of media in elections), access to information and government transparency, and digital democracy and internet freedoms. A second focus is on expanding access to technologies and physical infrastructure, including support for technological innovations, infrastructure (telephone and broadband), and telecommunication regulation reforms. A third category includes a focus on support to media and communication efforts to disseminate information on specific development objectives, such as around efforts to advance health, environmental or other development objectives. It also includes strategic communication programmes to disseminate information about the priorities and interests of development partners (see Box 2.5 for examples) (OECD, 2024[62]).

Box 2.5. ODA initiatives to strengthen media and information environments

In France, the Ministry of Europe and Foreign Affairs supports Canal France International (CFI), the French media co-operation agency working to encourage the development of medias in countries that receive development aid. It supports media organisations and civil society stakeholders based in these countries committed to providing free, democratic, and unbiased information, while also developing an awareness of sustainable development requirements. Since 2016, the French development agency, *l'Agence française de développement* (AFD), also has a mandate from the French Ministry of Europe and Foreign Affairs to finance projects dedicated to freedom of the press and training for journalists, strengthening of media, and efforts to counter disinformation. Among other initiatives, AFD signed a multi-year partnership agreement with Reporters Without Borders in 2022, which is being implemented in 66 countries on four continents. It includes funding for 18 local organisations in Europe, the Middle East, and North and West Africa specialising in trainings on journalist safety, fact-checking and investigative journalism.

Spain's development agency, *Agencia Española de Cooperación Internacional para el Desarrollo* (AECID), launched "*Programa Democracia*" in 2023 to support social dialogue and knowledge exchanges between Spain, other European countries, Latin America, and the Caribbean, with the objective to reinforce democratic values. One of the key pillars of this programme is the protection of human rights and fundamental freedoms via the support of journalists, activists, and academics and the defence of a diverse and pluralistic media space that favours reasoned dialogues in these regions.

The Deutsche *Gesellschaft für Internationale Zusammenarbeit* (GIZ), the German development agency, also finances projects to enhance journalistic quality and innovation of independent media organisations. Together with the European Union as co-financer and DW Akademie and Internews Europe as implementing partners, GIZ is supporting a three-year project (2022-2025) on media freedom and pluralism in the Western Balkans. The project focuses on helping independent media outlets improve their reporting and revenue-generating capacities.

In 2023, the United States Agency for International Development (USAID) launched the Pro-Info Initiative, which will provide USD 16 million to help promote digital and media literacy and support emerging technologies and "pre-bunking" efforts in countries where they operate.

Sources: (CFI, 2023[63]); (AFD, 2022[64]); (AECID, 2023[65]); (GIZ, 2022[66]); (USAID, 2023[67]).

Evaluations show that international co-operation and ODA can play a particularly important role in helping media actors survive, thus keeping citizens as well informed as possible in fragile political contexts and in conflict settings. Long-term and large investments can also have system-wide effects, such as the transformation of Ukraine's media sector. In the short- and medium-term, thematic programmes can be effective, such as shining a light on corruption and holding perpetrators to account through investigative journalism networks. Over the longer-term, supporting the capacity of journalists, strengthening media outlets, and developing the wider media enabling environment can ensure larger audiences are reached with better quality and more engaging information.

On the other hand, impact is insufficiently measured, and opportunities to develop joint donor strategies and evaluations in partner countries remain largely untapped. A 2023 study by USAID classified countries either under the so-called global north group and global south group and found a "severe imbalance" in evidence related to what works to counter misinformation in the countries classified as Global North versus those classified under Global South. The review found that 80% of the studies identified were conducted in the Global North, making it a challenge to draw conclusions about effective strategies for countering misinformation in the Global South (USAID, 2023[68]).

Evidence on how information environments benefit other development and diplomatic objectives, and how ODA programmes related to the information space can be most effective, would strengthen the political weight of international support and could lead to increases in both ODA and expert staffing. Recently, ODA supported initiatives to combat disinformation have been piloted, in particular in relation to COVID and electoral processes in partner countries, but this remains marginal as it is a new field for many donors and expertise is limited.

To support and strengthen these efforts, several normative initiatives are being developed and implemented. The OECD DAC's Network on Governance is developing updated "Principles for Relevant and Effective Support to Media and the Information Environment", and the Freedom Online Coalition adopted Donor Principles for Human Rights in the Digital Age in October 2023.[17]

Continuing to develop partnerships between development agencies, local actors, and international bodies is an important avenue to providing funding and promoting the exchange of best practices in a context where independent journalism in local languages faces eroding business models and, in some contexts, security risks and restrictions on press freedom (UNESCO, 2022[69]). For example, the U.S. Department of State Global Engagement Center (GEC) has undertaken several efforts to support independent media in those countries where it is being attacked. Separately, activities have included support for continuity of operations; trainings on journalistic skills, locally relevant studies of media capture tactics, and business sustainability planning for independent media; stakeholder mentorship; and the promotion of regional networking among entities who promote free expression. GEC also exposes disinformation narratives and tactics directly and works with foreign partners to build resiliency to foreign information manipulation and interference (FIMI).

Separately, the International Fund for Public Interest Media (IFPIM) was established in 2021 as an independent, multi-stakeholder initiative designed to address the challenges facing the media sector in low- and middle-income countries and to help identify pathways toward long-term sustainability.[18] In Europe, the Local Media for Democracy project aims to support the local media landscape with measures to build resilience, independence, and sustainability. Ultimately, via mapping news deserts in the EU and targeted media funding, the project seeks to support an enabling environment where a pluralistic and independent media landscape can exist (European Federation of Journalists, 2023[70]).

Several considerations help guide the design of government support mechanisms for media. For example, steps need to be taken to ensure the design of support models to private media, which were often created for traditional print and broadcast media, are appropriate to the new communication environment (Forum on Information and Democracy, 2021[54]). At the same time, in highly polarised societies, governmental support for public, private, or community media could be potentially used by malign actors to accuse the government of spreading false and misleading content. To mitigate such concerns, governments should ensure that there is a strong firewall between the media entity and government in terms of content and put in place clear and transparent rules for funding allocation and provide information about subsidies, project financing, and project activities. It is particularly important that procedures and control mechanisms demonstrate to the public that governmental support has no direct impact on the produced content and that political considerations do not affect distribution of financial or other support to media outlets. Similarly, when media outlets receive support from other governments or from international organisations, they run the risk of appearing to be under the control of an external actor. Any government support mechanism for media, especially support mechanisms for foreign media, must lay out clear and public rules to ensure that editorial stances are not influenced by outside assistance.

2.3.3. Strengthening economic incentives to promote better functioning online information spaces

While not directly connected to counteracting disinformation, identifying economic drivers that help provide incentives to online platforms to promote information integrity is an important approach. From a consumer perspective, while online platforms have brought substantial benefits, including lower information and communication prices, greater accessibility and convenience, and access to new content and means of engagement, several concerns have been identified with respect to competition in digital markets. Notably, digital-intensive sectors have demonstrated a tendency toward greater market concentration and falling entry rates of new firms (OECD, 2019[71]; OECD, 2022[72]). This is partly a result of strong merger activity in these markets. For example, between 2001 and 2021, Google bought 258 companies; Facebook (now Meta) employed a similar practice, buying 90 companies in a period of 16 years (2005 to 2021), meaning they closed one deal every two months (Nadler and Cicilline, 2020[73]) (American Economic Liberties Project, 2021[74]). In addition, there are certain inherent characteristics of digital markets that make them prone to concentration, including the presence of network effects (the phenomenon through which the value of a product or service increases when more people use it), data feedback loops (which enable platforms that derive significant volumes of data from their large user bases to continually improve their products and services), and strong economies of scale.

Concentration may in turn have reduced competition for and availability of trustworthy sources of news (Nadler and Cicilline, 2020[73]). Moreover, with fewer options available to consumers, concentration may also reduce incentives for large online platforms to compete on quality aspects. These trends are a concern because evidence shows that healthy market competition helps spur innovation, as well as promote long-term growth and well-being (OECD, 2022[75]).

Several jurisdictions have implemented, or have proposed, specific policies to address competitive harms in digital markets. By encouraging new entrants and innovation, these strategies seek to spur competition between online platforms, potentially encouraging market-based incentives to healthier information spaces, though this outcome is far from certain. For example, regulations may address, as appropriate, data-related concerns, including obligations to implement data portability and interoperability measures. Enabling consumers to switch services more easily may prevent anti-competitive conduct and encourage innovation. Governments may also include issues related to the 'gatekeeper' status of online platforms, including measures to limit bundling and self-preferencing their own goods and services. Some regulators have also put in place additional merger requirements that increase scrutiny of attendant competition risks (OECD, 2022[75]).

The European Commission (EC), for example, has taken this approach through the Digital Markets Act (DMA). The EC has focused on creating and maintaining a level playing field for digital services; ensuring responsible behaviour of online platforms; fostering trust, transparency and ensuring fairness on online platforms; and keeping markets open by promoting a fairer business environment and encouraging new services to enter the market (OECD, 2022[3]).

The nature of the relationship between digital platforms and news publishers is complex. From the news publishers' perspective, this relationship is characterised by a tension between the short-term operational opportunities of using digital platforms as effective channels of distribution of news content and the long-term concern to become "too dependent" on these platforms (Nielsen and Ganter, 2018[76]). From the digital platforms' perspective, there are conflicting views as to the value of news content, particularly compared to other type of third-party content, for their businesses and revenue (OECD, 2021[77]).

In light of these dynamics, one avenue to promote competition in this space has been to put in place requirements for online platforms to remunerate news media companies for linking to content. In Australia, the news media bargaining code came into effect in March 2021. It addresses the bargaining power imbalances between specifically designated online platforms (notably, those that have a "significant bargaining power imbalance with Australian news businesses") and publishers (Australian Competition and Consumer Commission, 2020[78]). The code requires designated digital platforms to negotiate in good faith with news businesses that have registered an intention to bargain. If an agreement about remuneration cannot be reached within three months, there is a compulsory arbitration mechanism within the framework to resolve disputes over remuneration (Australian Competition and Consumer Commission, 2020[78]). A government review found that by the end of its first year of operation, more than 30 commercial agreements had been struck between digital platforms (Google and Meta) and a range of Australian news businesses outside the code. It is unlikely these agreements would have been made without the Code (Government of Australia - The Treasury, 2022[79]).

Similarly, in July 2019, France enacted a law transposing the EU directive on copyright and related rights, including providing remuneration criteria for the use of news abstracts on online platforms (Autorité de la concurrence, 2020[80]). In April 2020, the French competition authority imposed interim measures requiring Google to negotiate in good faith with publishers and news agencies on the remuneration due to them under the law after finding that Google had likely engaged in anti-competitive conduct designed to circumvent the law (Autorité de la concurrence, 2020[80]). Furthermore, in 2023, Canada passed the Online News Act, which "aims to ensure that dominant platforms compensate news businesses when their content is made available on their services," and creates a bargaining framework to encourage platforms to reach voluntary commercial agreements with a range of news businesses, which would proceed to mandatory bargaining and arbitration process if unsuccessful (Government of Canada, 2023[81]).

The potential downsides to this approach can be seen, however, in the restrictions to free and open linking across the internet imposed by the regulations, and the risk that online platforms remove access to professional and traditional news sources in particular jurisdictions entirely. Indeed, Meta announced that "people in Canada will no longer be able to view or share news content on Facebook and Instagram," as the value Meta receives from allowing users to post links to news articles is less than the cost for paying the outlets for links that were previously made voluntarily (Meta, 2023[82]). Moving forward, the aim will be to continue to identify approaches that support an independent and diverse media sector, while upholding a free and open information space.

2.4. COUNTERING SPECIFIC RISKS IN THE INFORMATION SPACE

Given the dynamic global information space, the fast-paced technological innovation shaping it, and increasing geopolitical tensions, risks to the information spaces are rapidly evolving, with new risks emerging or new opportunities for those aiming to perpetrate disinformation campaigns. In this context, reinforcing information integrity demands that policymakers pay close attention to political, economic, technological or societal trends that can affect the risk landscape in this area.

While not new, the threat of foreign information manipulation and interference (FIMI) has continued to grow as malign actors use new technologies in novel ways. Off-the-shelf generative AI tools will enable more tailored FIMI operations by a broader range of actors, enabling the creation of higher quality content, at greater speed and scale, and at lower cost. The 2nd EEAS Report on Foreign Information Manipulation and Interference Threats found that FIMI threat actors strategically and opportunistically make use of the attention created by certain events, such as elections, emergencies, and political summits to pursue their interests (EEAS, 2024[83]). 2024, the so-called super election year – with more than 4 billion people likely to vote – will offer increased opportunities for malevolent actors to interfere in elections and try to shape political outcomes.

These examples showcase the importance of designing specific policy responses for these novel or emerging threats. Together, foreign interference fuelled by geopolitical tensions, the largest election year in history, and the power of generative AI becoming easily accessible elevate the level of information integrity risks. In this context, building understanding of the scope of the challenges and identifying policy responses could focus on:

- Responding to the threats posed by the spread of foreign information manipulation and interference (FIMI)
- Strengthening the information space in the context of elections by providing timely and reliable information to the public on how to exercise their rights, and
- Responding to the changes introduced by generative AI to the information space.

2.4.1. Risks posed by foreign information manipulation and interference

An important avenue for strengthening the information space is to recognise and respond to threats of foreign malign interference. If done transparently through official channels, foreign influence is legal and can contribute to democratic debates. Risks to democratic processes arise, however, from efforts by foreign agents to interfere in democratic processes and information spaces in ways that undermine decision-making, reduce trust in democratic systems, increase polarisation, and that hide the actors' activities and intent.

While a single, universally accepted definition of foreign interference does not yet exist, the concept broadly refers to efforts by foreign actors to interfere illegitimately in decision-making processes of a target country. It encompasses actions both by state and non-state actors, as well as their proxies. Foreign interference is also marked by the co-ordination of activities and the malign nature of actions that seek to negatively impact values, procedures, and political processes. While all governments seek to influence deliberations on issues of importance to them as part of their foreign policy toolbox, globalisation and digitalisation have amplified the challenge of foreign interference and made it much more of a civilian concern, with open democracies being more fragile to foreign interference than more closed systems. Several governance loopholes can be addressed in this regard to make democracies more resilient to foreign interference.

In the information space, foreign information manipulation and interference (FIMI) seeks to shape public opinion and discourse, often with the aim of strengthening parallel interference efforts (see Box 2.6 for definitions). Foreign malign actors often seek to exploit global information flows to gain influence, affecting countries globally, contributing to democratic backsliding, and threating political instability and violent conflict through disinformation campaigns (Office of the Director of National Intelligence, 2023[84]).

Domestic or foreign actors may spread disinformation as part of a foreign malign influence operation. Domestic actors can act as the witting or unwitting proxies of foreign malign actors, motivated by political, economic, social, or monetary gains. A key objective of FIMI actors is to destabilise society and government within the target state and confuse public debate around key issues, with disinformation often to be designed to be spread through domestic discussion and online. One tactic used to achieve this is exacerbating existing political and social fissures. This approach allows foreign actors to achieve more effective and seemingly authentic outreach, to save resources, and to hide the origins of the interference activities.

Box 2.6. Defining foreign interference and Foreign Information Manipulation and Interference (FIMI)

Toward a definition of foreign interference

The concept of “foreign interference” is broad. For example, the European Parliament’s definition notes that “foreign interference is illegitimate interference in the politics and democracy of the European Union and its Member States by foreign powers” (European Parliament, 2023[85]).

For its part, the United States Department of Homeland Security (DHS) defines foreign interference as “malign actions taken by foreign governments or foreign actors designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets for the purpose of undermining the interests of the United States and its allies” (United States Department of Homeland Security, 2018[86]), while the United States Code uses the term “foreign malign influence”, defined in 50 USC § 3059(e)(2), as “any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt or covert means, (A) the political, military, economic, or other policies or activities of the United States Government or State or local governments, including any election within the United States; or (B) the public opinion within the United States.”

The Australian Attorney General’s Department understands the concept of foreign interference as “covert, deceptive and coercive activities intended to affect an Australian political or governmental process that are directed, subsidised or undertaken by (or on behalf of) foreign actors to advance their interests or objectives” (Australian Government Attorney-General’s Department, 2019[87]).

A common understanding and definition of foreign interference could be useful to distinguish it from legitimate foreign influence and reduce the risk of foreign interference through international co-operation. Based on existing national definitions in OECD countries, common elements of foreign interference activities generally include the lack of transparency of the activities conducted; that the activities are conditioned, tasked or instructed, directly or indirectly, by a foreign state; and that they are intended to be harmful to the target country.

Foreign Information Manipulation and Interference (FIMI)

The European Union uses the term “foreign information manipulation and interference” (FIMI), which mainly focuses on disinformation threats, but is also related to the broader foreign interference picture: “Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and co-ordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory” (European External Action Service, 2023[88]).

Source: European Parliament (2023[85]), Legal loopholes and the risk of foreign interference. In depth-analysis requested by the ING2 special committee, https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702575/EXPO_IDA(2023)702575_EN.pdf; United States Department of Homeland Security (2018[86]), *Foreign Interference Taxonomy*, https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_october_15.pdf; Australian Government Attorney-General’s Department (2019[87]), *Foreign Influence Transparency Scheme. Factsheet 2 “What is the difference between ‘foreign influence’ and ‘foreign interference’?”*, https://www.ag.gov.au/sites/default/files/2020-03/influence-versus-interference.pdf; European External Action Service (2023[88]), *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en.

FIMI operations often seek to influence specific domestic and foreign policy decisions of target states, sow divisions in societies, denigrate democratic values, processes and institutions, and rally support for the policies of the perpetrating state (EEAS, 2023[89]). Foreign and malign information initiatives also seek to weaken target states by targeting foreign policy interests, as well as reducing the population's trust in government institutions, widening political cleavages and societal polarisation, and undermining democratic resilience (U.S. Department of State, 2020[90]) (OECD, 2022[91]).

Foreign state actors have also used a wide range of channels, tools, and practices to create and spread disinformation through potentially vast networks consisting of official, proxy, and unattributed communication channels, including state-backed media, global television networks, fake social media accounts and fake news websites. One avenue is via state-owned and controlled media of authoritarian states, such as Sputnik, RT, and TASS in Russia, and Xinhua and CCTV in China. The importance of these channels can be seen in Russia, for example, where government spending on "mass media" for the first quarter of 2022 was 322% higher than for the same period in 2021, reaching 17.4 billion roubles (roughly EUR 215 million). Almost 70% of Russia's spending on mass media in Q1 2022 was spent in March, immediately after Russia's invasion of Ukraine (The Moscow Times, 2022[92]). The outlets that receive these funds, including RT and Rossiya Segodnya, which owns and operates Sputnik and RIA Novosti, are state-linked and state-owned outlets that "serve primarily as conduits for the Kremlin's talking points and can be more accurately thought of as tools of state propaganda (United States Department of State, 2022[93]) (Cadier et al., 2022[94]).

The Chinese government has expanded the distribution of content favourable to its positions through the reach of its state-owned media, purchasing foreign media outlets, and by publishing favourable content in foreign media outlets. For example, as noted in the U.S. Department of State GEC report "How the People's Republic of China Seeks to Reshape the Global Information Environment," Xinhua, the Chinese government's official state news agency, maintained 181 bureaus in 142 countries and regions as of August 2021. The Chinese government has also purchased controlling stakes in media outlets in Europe, Asia, and Africa, in many cases evading media transparency rules and often shifting news and editorial coverage to more pro-Chinese positions (U.S. Department of State, 2023[95]). In addition, government-controlled media has used content-sharing agreements with foreign local media outlets to supply information products for free or at heavily subsidised prices to local media outlets, and in some cases prohibiting recipients from entering into content-sharing agreements with Western-sourced wire services. Such an approach can discretely promote pro-Chinese positions while limiting the reach of other outlets. These types of agreements – in which information provided by Chinese outlets appears in local media without attribution – risks distorting information environments and reduces the ability of citizens to make transparently informed decisions (U.S. Department of State, 2023[95]).

In response, for example, the Baltic states were the first EU countries to impose temporary bans on the broadcasting of some Russian TV channels, directly or indirectly run by the Russian state, which actively spread disinformation, propaganda and incitement to hatred. Following Russia's war of aggression against Ukraine in 2022, the European Union introduced a Union-wide ban on broadcasting of the two Russian state-run channels, RT (Russia Today) and Sputnik. In December 2022, the European Union expanded the list of banned Russian TV channels to address the "systematic, international campaign of media manipulation and distortion of facts in order to enhance its strategy of destabilisation of its neighbouring countries, and of the Union and its Member States (Official Journal of the European Union, 2022[96])."

Malign actors also use cyber-attacks to steal and distribute sensitive information as a more active effort to support wider disinformation campaigns. For example, prior to the 2017 French presidential election, a co-ordinated attempt to undermine Emmanuel Macron's candidacy included the hacking and leaking two days before the second and final round of the presidential election of more than 20 000 emails stolen from the computers of campaign staff. This cyber-attack was timed to coincide with the campaign blackout period which prevents campaigning mandated by law and was co-ordinated with a disinformation campaign that in parallel spread rumours and forged documents. On X alone, a co-ordinated effort to spread related content by promoting the hashtag #MacronLeaks appeared in almost half a million tweets in twenty-four hours (Vilmer, 2019[97]). In addition to the harms caused by illegally accessing private information and the risks posed by cyber-attacks to democratic processes more widely, this campaign highlights how malign actors can use hacked governmental data, commercial secrets, and personal information to obscure and undermine public debate.

Actors can use opportunities provided by online platforms to amplify the reach of content to spread foreign information manipulation and interference campaigns. Beyond hijacking social platform accounts of elected or other public officials, malign actors pursue less overt means of artificial amplification, including by stealing accounts and creating "bot farms" to spread content. This co-ordinated exploitation of accounts post, share, and like target materials in ways that mimic – and may then develop into – actual engagement on platforms and even spread to off-line news sources.

Moving forward, generative AI technologies will provide greater opportunities for the creation and distribution of false and misleading content. Malign actors may use these rapidly evolving technologies to generate realistic looking and difficult to detect automatically fake user profiles, text, audio, and video materials, as well as to manage bot networks. To this end, foreign information manipulation and interference should be seen as part of larger efforts to undermine democratic processes. Disinformation efforts are an important national security tool for nations and nonstate actors whose goal it is to undermine democracy (Danvers, 2023[98]). Attacks against elected and public officials and candidates can directly distort the political process. Undermining citizens' perception of the fairness, transparency, and security of the electoral process erodes trust in democratic system more widely. Maintaining information integrity is therefore a key measure to upholding the integrity of democracies.

Existing policies to counter foreign interference can be applied to new communication technologies and challenges

Disinformation activities benefit from ambiguity and obscurity; using transparency enforcement mechanisms can facilitate disclosures and provide an avenue to punish covert and malign foreign interference by government actors. To that end, applying existing regulation to counter foreign interference to new communication technologies and challenges is a promising policy response. For example, in the United States, the application of the Foreign Agents Registration Act (FARA), which originally passed in 1938, shows how existing legislation to increase transparency of foreign governments' influence activities can be adapted for use in combatting the spread of disinformation online. In 2018, the United States indicted 13 Russian nationals and three Russian companies (the Internet Research Agency LLC, Concord Management and Consulting LLC, and Concord Catering) under FARA for creating false accounts, concealing advertising, and organising and co-ordinating political rallies in an effort to interfere in the U.S. elections (United States Department of Justice, 2022[38]) (Box 2.7).

Box 2.7. The application of the Foreign Agents Registration Act (FARA) to the fight against disinformation

U.S. Congress passed the Foreign Agents Registration Act (FARA) in 1938 to increase transparency of foreign governments' influence activities. The Foreign Agents Registration Act Unit, which is part of the U.S. Department of Justice's National Security Division, administers and enforces FARA.

The Act requires any actors (political agents, lobbyists, public relations counsel, fundraisers, corporations, organisations, among others) working on behalf of or in the interest of a foreign government or foreign principal outside of the United States, including Americans, to disclose their affiliations and activities as well as receipts and disbursements in support of those activities. One of the main goals of the Act is to fight against the use of propaganda activities by making efforts of foreign actors easier to identify by the U.S. Government and public. "Political activities" covered by FARA include any activity that the actor believes will or intend to influence the government regarding its domestic and foreign policies.

While FARA has been a tool to combat foreign propaganda and influence campaigns for several decades, the government has more recently used it to prevent covert foreign disinformation activities. For example, in 2017, the Florida-based company RM Broadcasting was providing a platform for the broadcast of radio programmes from a Russian state-owned news agency, thus acting as an agent of a foreign principal, even though it was not registered as such. RM Broadcasting was ordered to register under FARA to make it easier for radio listeners to understand the source of their news. In 2018, furthermore, several Russian nationals and Russian companies were charged with attempted interference of the 2016 U.S. Presidential election; a basis of the indictments was the agents' failure to comply with FARA.

While the scope of FARA is broad, there are several exceptions for accredited diplomatic or consular officers, actors engaging in bona fide trade or commerce activities, religious, scholastic, academic, or scientific pursuits or fine arts. As the risk posed by the spread of disinformation, particularly by foreign actors, has been further recognised in the United States as a priority in recent years, criminal proceedings against actors who failed to register under FARA have also increased.

Source: The United States Department of Justice (2023[99]), Foreign Agents Registration Act, https://www.justice.gov/nsd-fara; The United States Department of Justice (2022[100]), Court finds RM broadcasting must register as a foreign agent, https://www.justice.gov/opa/pr/court-finds-rm-broadcasting-must-register-foreign-agent; The United States Department of Justice (2021[101]), Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere

Similarly, in Australia, the Foreign Influence Transparency Scheme seeks to provide the public with visibility of the nature, level and extent of foreign influence on Australia's government and politics (Government of Australia, 2023[102]). It does this by requiring individuals and entities who undertake registrable activities on behalf of a foreign government for the purpose of influencing Australian political or governmental processes to disclose these details on a public register. Specifically, the scheme includes communications activities as a registrable activity to ensure people consuming information are aware of its source.[19] The scheme is not designed specifically to combat mis- and disinformation; however by making the source behind the communication activities transparent, such schemes can provide useful options to illuminate covert and potentially malign communication activities, ultimately building trust in the information space more broadly.

2.4.2. Disinformation in the context of elections

When disinformation operations are strategically conducted during electoral cycles, they directly interfere with the essential core of democracy, can undermine the trust placed in the electoral process and the bodies in charge of it, discredit political opponents, increase the risk of disputed election results and sow social unrest (UNDP, 2023[103]); (International IDEA, 2024[104]).

According to an IPSOS and UNESCO survey conducted in 16 countries where general elections will be held in 2024, 87% of respondents expressed concern about the impact of disinformation on upcoming elections in their country, with 47% being "very concerned" (IPSOS, UNESCO, 2023[105]). In addition, an increasingly digital environment brings new benefits and dangers in the context of elections. Technology can increase citizens' opportunities to find useful information for their voting decisions and foster voter mobilisation. At the same time, technology-enabled solutions can also be used to influence the electorate by spreading disinformation, for instance through artificial amplification or AI-generated deepfakes and political micro-targeting.

As elections are usually planned and their dates well-known in advance, disinformation propagators can have time to organise sophisticated operations. In addition, elections can indeed be seen as an "ideal high-impact opportunity" to conduct their information influence operations (Polyakova and Fried, 2019[106]). It is important also to note that engaging in electoral interference strategies and activities do not necessarily necessitate tangible impacts on the results of the elections to have a negative impact: sometimes casting doubts on the legitimacy of the elected candidate can achieve the expected results by those interfering. In this context, it is also important to prepare a policy response, so that detection capacities can be deployed as early as possible to reduce the risk of interference. This said, it is important to highlight that no measure to tackle disinformation during elections should interfere with legitimate political debates or justify disproportionate measures restricting the free flow of information, including the blocking of content or Internet access (UNESCO, 2022[107]).

Given the role that elected officials, candidates, and political parties play in the information ecosystem, including in generating and amplifying content, and in some cases amplifying disinformation, reiterating the importance of information integrity in elections can play a key role. The Code of Conduct Transparency Online Political Advertisements developed by the Netherlands in 2021, for example, sought to prevent the spread of misleading information during elections by receiving commitments from platforms and political parties to acknowledge a responsibility in maintaining the integrity of elections and to avoid disseminating misleading content (Government of the Netherlands, 2021[7]).

A response to the threat of information manipulation in the context of elections includes the development of a wide range of government competences, often through the creation of specialised task forces, focused on justice, national security and defence, public communication, and election management which would ideally be established well ahead of the planned elections (see Box 2.8). Stakeholders on election frontlines, including independent electoral management bodies (EMB), political parties and candidates, journalists, and civil society organisations, need to be aware of the risks that disinformation poses to free and fair elections.

A key focus of efforts focused on countering electoral disinformation is around facilitating co-operation and co-ordination across governments to share information about relevant threats and deploy appropriate response strategies. Co-ordination enables relevant offices to work together to take appropriate action while respecting political neutrality. Governments can also focus on building the public's long-term understanding of disinformation flows and risks and enhance preparedness ahead of elections. Civic education on a country's electoral legal framework prevents information gaps that can be exploited by disinformation propagators. More broadly, voter education can help safeguard electoral integrity on issues such as campaign finance and advertising rules.

Government efforts in this space also enable short-term reactions to immediate information threats in the context of electoral disinformation. In recent Brazilian elections, the judiciary co-ordinated with digital platforms to facilitate engagement and compliance of court decisions around illegal content. In this way, the Brazilian government sought to establish open and agile dialogue channels during electoral periods between digital platforms and public authorities, while ensuring that any decisions taken with regards to content moderation were made in a transparent, public manner and in accordance with the country's laws.

In addition, government offices and task forces may provide timely and reliable information to citizens on how to exercise their rights, including voter registration and election day voting procedures, particularly in response to specific disinformation campaigns (International IDEA, 2023[108]).

Box 2.8. Ensuring information integrity during elections via special taskforces

Electoral Integrity Assurance Taskforce – Australia

In Australia, the Electoral Integrity Assurance Taskforce (EIAT), made up of agencies across federal government, was established in 2018 to provide information and advice to the Australian Electoral Commissioner on matters that may compromise the real or perceived integrity of an Australian federal election or referendum. Potential threats to electoral integrity can come in the form of cyber or physical security incidents, disinformation campaigns, and through perceived or actual interference in electoral processes. Notably, this taskforce focuses on referring information about relevant threats to the appropriate agencies in Australia and facilitates co-operation and co-ordination, enabling them to work together to take appropriate action while respecting strict political neutrality.

The Taskforce and its Board are comprised of the following agencies: Australian Electoral Commission, Department of Finance, Department of Prime Minister and Cabinet, Department of Infrastructure, Transport, Regional Development, Communications, and the Arts, Attorney-General's Department, Department of Home Affairs, the Australian Federal Police, the Australian Signals Directorate, the Australian Transaction Reports and Analysis Centre, Department of Foreign Affairs and Trade, the Australian Security Intelligence Organisation, and the Office of National Intelligence.

The work of this task force is also complemented by AEC-led campaigns such as "Stop and Consider", encouraging voters to think critically about the sources of electoral information they see or hear, and the AEC Disinformation Register, focusing on harmful disinformation related exclusively to the procedural aspects of conducting elections and referendums.

Electoral Justice Permanent Programme on Countering Disinformation – Brazil

Brazil's Electoral Justice Permanent Programme on Countering Disinformation was established by the Superior Electoral Court (TSE) in August 2021, building on a similar programme established in 2019 that sought to prevent and combat the spread of mis- and disinformation about the 2020 elections.

To respond to the challenges that disinformation imposes on the integrity of elections and on democracy more widely, the Programme has adopted a "network" model, bringing together representatives from government agencies, press and fact-checking organisations, Internet providers, civil society organisations, academia, and political parties. 154 partners take part currently.

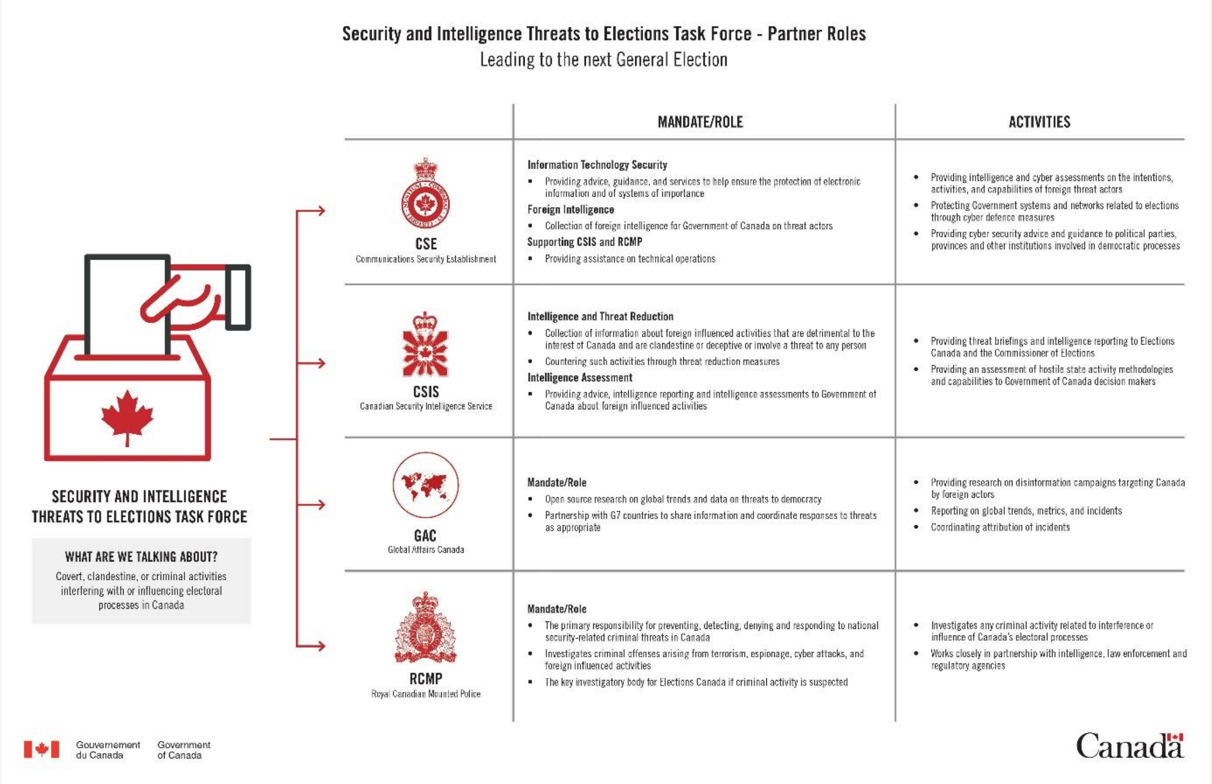
The Programme focuses on three actions: (i) Informing, which seeks to disseminate official, reliable, and quality information related to the electoral process; (ii) Empowering, which is aimed at media literacy and building societal understanding of both the threats posed by the spread of disinformation as well as civic education around the functioning of the electoral process in Brazil; and (iii) Responding, which is focused on identifying disinformation campaigns and countering its negative effects.

Critical Election Incident Public Protocol & Security and Intelligence Threats to Elections (SITE) Task Force – Canada

In anticipation of the 2019 election, Canada put in place the Plan to Protect Canada's Democracy presenting concrete actions to safeguarding democratic institutions and processes. The Plan includes four pillars of action: enhancing citizens' preparedness, enhancing organisational readiness, combating foreign interference, and building a healthy information ecosystem.

As a result of this Plan, Canada established a Critical Election Incident Public Protocol, which lays out a simple, clear, and impartial process by which Canadians would be notified of a threat to the integrity of a General Election.

Canada also established a Security and Intelligence Threats to Election (SITE) Task Force to identify and prevent covert, clandestine, or criminal activities from influencing or interfering with Canada's electoral process. The primary responsibilities of the Task Force are to raise awareness of foreign threats to Canada's electoral process and to prepare the government to assess and respond to those threats, including disinformation campaigns. The Task Force comprises representatives from the Communications Security Establishment, the Royal Canadian Mounted Police, Global Affairs Canada, and the Canadian Security Intelligence Service.



Security and Intelligence Threats to Elections Task Force - Partner Roles

Leading to the next General Election

SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

WHAT ARE WE TALKING ABOUT?

Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada

	MANDATE/ROLE	ACTIVITIES
CSE Communications Security Establishment	**Information Technology Security** ▪ Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance **Foreign Intelligence** ▪ Collection of foreign intelligence for Government of Canada on threat actors **Supporting CSIS and RCMP** ▪ Providing assistance on technical operations	• Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors • Protecting Government systems and networks related to elections through cyber defence measures • Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes
CSIS Canadian Security Intelligence Service	**Intelligence and Threat Reduction** ▪ Collection of information about foreign influenced activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person ▪ Countering such activities through threat reduction measures **Intelligence Assessment** ▪ Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influenced activities	• Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections • Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers
GAC Global Affairs Canada	**Mandate/Role** ▪ Open source research on global trends and data on threats to democracy ▪ Partnership with G7 countries to share information and coordinate responses to threats as appropriate	• Providing research on disinformation campaigns targeting Canada by foreign actors • Reporting on global trends, metrics, and incidents • Coordinating attribution of incidents
RCMP Royal Canadian Mounted Police	**Mandate/Role** ▪ The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada ▪ Investigates criminal offenses arising from terrorism, espionage, cyber attacks, and foreign influenced activities ▪ The key investigatory body for Elections Canada if criminal activity is suspected	• Investigates any criminal activity related to interference or influence of Canada's electoral processes • Works closely in partnership with intelligence, law enforcement and regulatory agencies

Gouvernement du Canada Government of Canada

Canada

Source: Australian Electoral Commission (2023[109]), "Electoral Integrity Assurance Taskforce", https://www.aec.gov.au/about_aec/electoral-integrity.htm; Government of Brazil Electoral Justice Permanent Programme on Countering Disinformation Strategic Plan 2022, https://international.tse.jus.br/en/misinformation-and-fake-news/tse-brazil-counter-disinformation-program-2022-f.pdf; Government of Canada (2021[110]), "Security and Intelligence Threats to Elections (SITE) Task Force", https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html; Government of Canada (2023[111]), "Rapid Response Mechanism Canada: Global Affairs Canada", https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng.

2.4.3. Governments will need to respond to the changes introduced by generative AI to the information space

While risk-based regulation is increasingly used to mitigate the risks in the role that online platforms play in spreading information (including mis- and disinformation), such an approach should also respond to the role of Artificial Intelligence (AI) tools and systems, how those affect the information space, and how they are used as a disinformation tool that undermines human rights, for example by being used to silence women and members of marginalised communities participating in public life. The rapid development of advanced AI systems has indeed the potential to lead to innovations that can both benefit societies, while also posing new risks (GPAI, 2023[112]).

In the information space, generative AI[20] tools may help identify inauthentic accounts or patterns, thereby helping governments improve their situational awareness around disinformation campaigns and complementing the moderation work by digital platforms. The tools may also be used to support the development of educational materials and activities, as well as to facilitate translation, summaries, and analysis, greatly facilitating and reducing the cost of these activities for public officials, journalists, and CSO actors alike (Landemore, 2023[113]).

The ability for generative AI to create and disseminate highly convincing content also raises the risk posed by rapid growth of realistic false or misleading news, articles, and visual media, posing an additional risk to people's trust in the information space, particularly online. In addition to content generation, generative AI could also help create a large amount of realistic fake profiles on online platforms, help animate networks of fake accounts, and overcome the detection capabilities recently created by governments, platforms or other stakeholders to identify co-ordinated inauthentic behaviour on platforms. By vastly reducing the cost of and language barriers to creating convincing text or visuals, and by making it increasingly difficult to distinguish between genuine and manipulated content, generative AI tools have the potential to magnify the challenges already introduced by online platforms. This situation may further erode the foundation of trust that individuals place in the information they consume, leading to heightened scepticism and uncertainty.

To that end, the OECD Recommendation on Artificial Intelligence calls for AI actors to commit to transparency and responsible disclosure regarding AI systems in order to: 1) foster a general understanding of AI systems; 2) ensure stakeholders are aware of their interactions with AI systems, including in the workplace; 3) enable those affected by an AI system to understand the outcome; and 4) enable those adversely affected by an AI system to challenge its outcome and understand the logic that served as the basis for the prediction, recommendation, or decision (OECD, 2019[114]).

Regarding the potential impact on the information space more specifically, focusing on generative AI tools (as opposed to the wider universe of AI applications and effects related to autonomous weapons, facial recognition technology, self-driving cars, and economic impacts), is a helpful framework for analysis. Policies could consider requiring that consumer-facing generative AI systems make public the training data used to build the systems, ensuring that the principles used to guide the tools are available to allow for comparison between tools and public oversight of what guardrails systems have put in place (or not, as the case may be), and watermarking of content produced (Giansiracusa, 2023[115]).

Along these lines, the proposed EU AI Act, presently under discussion, follows a risk-based approach and establishes obligations for providers and users depending on the level of risk the AI can generate. On the one hand, the EU AI Act will seek to prohibit AI systems with an "unacceptable level of risk to people's safety", including systems that "deploy subliminal or purposefully manipulative techniques, exploit people's vulnerabilities or are used for social scoring (classifying people based on their social behaviour, socio-economic status, personal characteristics)" (European Parliament, 2023[116]). The act would also require the creation of risk assessment and mitigation plans and require that generative AI tools follow transparency requirements, such as disclosing what content was generated by AI. The EU AI Act would also require tools to be designed to prevent the generation of illegal content and to publish summaries of copyrighted data used for training (European Parliament, 2023[116]). The EU's approach in this space illustrates how the application of a risk-based approach can inform other regulatory responses to technologies that play an important role in the information space beyond online and social media platforms. Similarly, governments have sought to counter the risks posed by deepfakes, audio or visual media content that seem authentic but are in fact synthetic or manipulated.

Deepfakes present a disinformation risk by presenting believable, though fake, images and audio. While synthetic media is not new, the access to technology, scale, speed, and quality of deepfakes has increased a focus on the role of policy responses. Many of the efforts to prevent risks posed by deepfakes seek to enhance transparency around the content itself and the processes followed by the systems to help validate provenance and accuracy, as well as to build on existing legal restrictions on content use. An approach focused on transparency can avoid regulatory overreach that may limit the technology's use for protected speech, such as satire. Along those lines, the EU 2022 Strengthened Code of Practice on Disinformation commits signatories that develop or operate AI systems to report on their policies for countering prohibited manipulative practices that generate or manipulate content (such as deepfakes). In addition, many of the laws passed in US states have focused on nonconsensual deepfake pornography given the clear harms caused and limited speech benefits. In this regard, nine states have enacted laws that regulate deepfakes, mostly in the context of pornography and elections influence (Poritz, 2023[117]). In 2023, furthermore, the Office of the President of the United States issued an *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, which specifically seeks in part to protect individuals from "AI-enabled fraud and deception by establishing standards and best practices for detecting AI-generated content and authenticating official content (U.S. White House, 2023[118])."

Ultimately, by identifying, analysing, and prioritising relevant risks, taking a risk-based approach can help ensure regulation is targeted and proportional, and that it does not introduce burdensome rules with little positive impact (OECD, 2021[14]). In the information space, such an approach aims to better understand, flag, and mitigate proactively the risks posed by relevant actors and to encourage or require actors to put in place mechanisms and processes that limit the risks posed by disinformation and build trust in the information space.

2.5. CONSIDERATIONS AND PATH FORWARD

Digital communications and online platforms have altered how information is created and shared and altered the economic models that underpin the information space. Online platforms have facilitated the spread of polarising, sensational, and false or misleading information, while operating in nascent regulatory environments. The global reach of these platforms surpasses national (and even supra-national) regulatory jurisdictions. At the same time, voluntary self- and co-regulatory regimes are limited in that they allow some actors to sidestep obligations, underscoring the importance of government involvement in designing, enforcing, and updating regulatory responses, as appropriate.

Done appropriately and with the aim of supporting democratic engagement, the health, transparency, and competitiveness of information spaces can be supported by appropriate, effective, and agile policymaking. To that end, policies to promote the transparency and accountability of online platforms are an option to help build understanding of their business-models and the related risks to democratic processes, help mitigate threats, including those posed by foreign information manipulation and interference, and foster healthier information spaces.

In addition to focusing on online platforms, a strong, pluralistic, and diverse media sector with solid journalists is a foundation for reinforcing information integrity and an essential component of democracy. Reinforcing information integrity will require promoting the transparency and health of these spaces through effective design, monitoring, and implementation of relevant policies. By providing sources of fact- and evidence-based content informed by standards of professional quality, journalists and the media sector more widely – including national, local, and community outlets and multiple on- and offline sources – can counter the impact of mis- and disinformation and inform public debate in democracy. The role of these sources of news and information in democracies, however, continues to face changes and challenges exacerbated by the development of online communication technologies and the role social media platforms have played in shaping the information environment.

To that end, the emerging understanding suggests that governments should pursue the following objectives to strengthening the positive role of media and online platforms in the information space:

- Uphold a free, independent, and diverse media sector as an essential component of open and democratic societies. In addition to the legal foundation for ensuring freedom of opinion and expression, governments must protect journalists, media workers, and researchers, and monitor, investigate, and provide access to justice for threats and attacks against them. Adopting national action plans for the safety of journalists, engaging with press councils and mapping and monitoring risks and threats are additional actions that can be taken.
- Design policies to reinforce a diverse, pluralistic, and independent market for traditional media. Limiting market concentration, promoting transparency and diversity of media, and mandating editorial independence can all play an important role in preventing undue influence from political and commercial interests.

- Support independent and high-quality public service media. These outlets are often among the most trusted sources of news and can play an important role in democracies as providers of independent, quality, and trusted news and information.
- Explore direct and indirect financial support – including special taxation regimes and targeted funding – to media outlets that meet specified criteria and help achieve democratic objectives, such as reinforcing local, community, cultural, minority language, or investigative journalism. Governments should also recognise the distinct nature of not-for-profit community media and guarantee their independence. Reinforcing a diverse and independent media sector is also an important component for international support and overseas development assistance. Throughout these efforts, however, governments should put in place clear and transparent rules for funding allocation, and provide information about subsidies, financing, and project activities. Such processes should be designed to show and ensure that governments have no direct impact on content development, and to help prevent political bias in funding selection.
- Avoid unduly restricting speech through overly broad content-specific regulations that do not meet stringent, transparent, and objectively defined criteria that are consistent with the State's international human rights obligations and commitments. This is particularly important given the difficulties in defining "disinformation" and that legislating "legal but harmful" content risks limiting speech.
- Recognise the role that intermediary liability protections play in fostering a free and open internet and in balancing platforms' responsibilities to address legitimate concerns around false, misleading, and otherwise harmful or illegal content.
- Increase transparency and responsibility, including, where relevant, through regulatory efforts, of relevant actors to better understand and mitigate potential and actual impacts of generative AI tools with respect to disinformation. Such an approach will be particularly important given the novelty, rapid evolution, and uncertainty related to how and to what extent these new technologies will amplify the challenges of trust in the information space. Understanding the principles used to guide the development and application of generative AI tools; increasing transparency of the data sets used in their design; watermarking AI generated content; and requiring testing, risk identification and mitigation, and monitoring will help build trust. At the same time, restricting uses of deepfakes in some specific and well-defined contexts, such as in processes related to election administration, might help mitigate the threat posed by false and misleading content.
- Enhance transparency and information sharing around policies, policy development, processes, and decisions of online platforms to enable better understanding of their operations and impacts of business models, risk mitigation measures, and algorithms, as appropriate. Putting in place mechanisms, including regulatory mechanisms, as appropriate, to increase platform disclosures related to their terms of service, efforts to prevent and address human rights impacts, and privacy policies; procedures, guidelines, and tools that inform the content moderation and algorithmic decision making; and complaint handling processes can empower users to better understand data handling and rule enforcement. This information can also encourage platform accountability to users, as public scrutiny can reinforce positive actions to address adverse impacts while highlighting potential biases, human rights risks, or unfair practices. Facilitating the standardisation of such information can also encourage the creation of best practices for policy development and inform ways to measure the impact of those interventions.
- Facilitate greater access to data for academics, journalists and other researchers that helps build understanding of how content spreads across platforms and throughout information spaces, including through regulatory requirements, as appropriate. Analysing public data (not private posts or messages) that does not include personally identifiable information could also generate insights into online behaviour, patterns, and changes over time,

thereby facilitating impact assessments of policies. Enabling governments and independent researchers to verify and confirm platforms' public disclosures, including around political advertising, can also promote accountability. Promoting standardised reporting mechanisms, mandating that steps are taken to ensure research is conducted for legitimate aims, and that researchers implement privacy and security protections will be important efforts to ensure quality research and to help prevent abuse.

- Apply policies to counter foreign malign interference to the information space. Applying existing policies designed to counter foreign interference, when they exist and as appropriate, to online communication technologies is a useful avenue to build trust. By making the identity of foreign agents and owners of media outlets known, such schemes can help illuminate covert and potentially malign communication activities.
- Safeguard information integrity in times of democratic elections. Putting in place mechanisms to monitor specific threats and to provide timely and reliable information to citizens to enable them to exercise their rights will be key in this fast-changing information environment. Readily available, high-quality information that is tailored for specific at-risk communities regarding identified threats will enable governments to prevent information gaps that can be exploited by disinformation propagators.
- Identify economic drivers that encourage new entrants, innovation, and data portability to spur competition between online platforms, potentially encouraging market-based responses to support better functioning information spaces.

REFERENCES

AECID (2023), “Democracy Programme”, Spanish Agency for Development Cooperation, https://www.aecid.es/programa-democracia. [65]

AFD (2022), “Comment le groupe AFD contribue à la liberté d’information dans le monde”, Agence française de développement, https://www.afd.fr/fr/actualites/comment-le-groupe-afd-contribue-la-liberte-dinformation-dans-le-monde. [64]

American Economic Liberties Project (2021), *Big Tech Merger Tracker*, https://www.economicliberties.us/big-tech-merger-tracker/. [74]

Australian Competition and Consumer Commission (2020), *Draft news media bargaining code*, https://www.accc.gov.au/by-industry/digital-platforms-and-services/news-media-bargaining-code/news-media-bargaining-code. [78]

Australian Competition and Consumer Commission (2019), *Digital Platforms Inquiry Final Report*, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf. [24]

Australian Electoral Commission (2023), *Electoral Integrity Assurance Taskforce*, https://www.aec.gov.au/about_aec/electoral-integrity.htm (accessed on 31 August 2023). [109]

Australian Government (2023), *Communications Legislation Amendment (Combatting Misinformation and Disinformation) Bill 2023—guidance note*, Australian Government - Department of Infrastructure, Transport, Regional Development, Communications and the Arts, https://www.infrastructure.gov.au/department/media/publications/communications-legislation-amendment-combatting-misinformation-and-disinformation-bill-2023-guidance. [25]

Australian Government Attorney-General’s Department (2019), *Foreign Influence Transparency Scheme. Factsheet 2 “What is the difference between ‘foreign influence’ and ‘foreign interference’?”*, https://www.ag.gov.au/sites/default/files/2020-03/influence-ve. [87]

Autorité de la concurrence (2020), *Related rights: the Autorité has granted requests for urgent interim measures presented by press publishers and the news agency AFP (Agence France Presse)*. [80]

Baldwin, R., M. Cave and M. Lodge (2011), *Understanding Regulation*, Oxford University Press, https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001. [5]

Bleyer-Simon, K. and I. Nenadić (2021), *News Media Subsidies in the First Wave of the COVID-19 Pandemic – A European Perspective*. [55]

Brennen, J. and M. Perault (2021), *How to increase transparency for political ads on social media*, Brookings, https://www.brookings.edu/articles/how-to-increase-transparency-for-political-ads-on-social-media/. [30]

Cadier et al. (2022), *Russia-Ukraine Disinformation Tracking Center*, https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/. [94]

Campbell, A. (2019), *How data privacy laws can fight fake news*, https://www.justsecurity.org/65795/how-data-privacy-laws-can-fight-fake-news/. [21]

CFI (2023), “Our mission”, Canal France International, https://cfi.fr/en/content/our-mission. [63]

Chapman, M., N. Bellardi and H. Peissl (2020), *Media literacy for all: Supporting marginalised groups through community media*. [60]

Council of Europe (2023), *Good practices for sustainable news media financing*, https://rm.coe.int/msi-res-2022-08-good-practices-for-sustainable-media-financing-for-sub/1680adf466. [53]

Council of Europe (2021), *Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation*, https://rm.coe.int/content-moderation-en/1680a2cc18. [11]

Council of Europe (2018), *Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership*, https://www.coe.int/en/web/freedom-expression/adopted-texts/-/asset_publisher/m4TQxjmx4mYl/content/recommendation-cm-rec-2018-1-1-of-the-committee-of-ministers-to-member-states-on-media-pluralism-and-transparency-of-media-ownership. [50]

Council of Europe (2016), *Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection and journalism and safety of journalists and other media actors*, https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2016-4-of-the-committee-of-ministers-to-member-states-on-the-protection-of-journalism-and-safety-of-journalists. [37]

Craufurd Smith, R., B. Klimkiewicz and A. Ostling (2021), “Media ownership transparency in Europe: Closing the gap between European aspiration and domestic reality”, *European Journal of Communication*, Vol. 36(6), pp. 547–562, https://doi.org/10.1177/0267323121999523. [48]

Danvers, W. (2023), *Disinformation may be one of Russia and China’s greatest weapons*, https://thehill.com/opinion/national-security/3932031-disinformation-may-be-one-of-russia-and-chinas-greatest-weapons/. [98]

Douek, E. (2021), ”Governing Online Speech: From “Posts-as-Trumps” to Proportionality and Probability”, *Columbia Law Review*, Vol. 121/No. 3, https://columbialawreview.org/content/governing-online-speech-from-posts-as-trumps-to-proportionality-and-probability/. [19]

EEAS (2024), *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence*, https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en. [83]

EEAS (2023), *1 st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf. [89]

Ellger, F. et al. (2021), *Local Newspaper Decline and Political Polarization - Evidence from a Multi-Party Setting*, Center for Open Science, https://doi.org/10.31219/osf.io/nhwxs. [41]

ERR (2023), *Estonian Russian-language private media receive €1 million from state*, https://news.err.ee/1608898790/estonian-russian-language-private-media-receive-1-million-from-state. [59]

European Audiovisual Observatory (2016), *Media ownership - Market realities and regulatory responses*, https://rm.coe.int/media-ownership-market-realities-and-regulatory-responses/168078996c. [45]

European Commission (2023), *Code of Practice on Disinformation: New Transparency Centre provides insights and data on online disinformation for the first time*, https://ec.europa.eu/commission/presscorner/detail/en/mex_23_723. [9]

European Commission (2022), *European Media Freedom Act: Commission proposes rules to protect media pluralism and independence in the EU*, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_5504. [52]

European Council (2022), *The General Data Protection Regulation*, https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/. [22]

European Court of Human Rights (2001), *Thoma v. Luxembourg*. [49]

European External Action Service (2023), *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a framework for networked defence*, https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023.pdf. [88]

European Federation of Journalists (2023), *Local Media for Democracy*, https://europeanjournalists.org/local-media-for-democracy/. [70]

European Parliament (2023), *AI Act: a step closer to the first rules on Artificial Intelligence*, https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence. [116]

European Parliament (2023), *Legal loopholes and the risk of foreign interference. In depth-analysis requested by the ING2 special committee*, https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702575/EXPO_IDA(2023)702575_EN.pdf. [85]

European Union (2022), *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)*, Publications Office of the European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?ur. [13]

FATF (2023), *Guidance on Beneficial Ownership for Legal Persons*, Financial Action Task Force, Paris, https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html. [51]

Forum on Information and Democracy (2021), *A New Deal for Journalism*, https://informationdemocracy.org/wp-content/uploads/2021/06/ForumID_New-Deal-for-Journalism_16Jun21.pdf. [54]

Forum on Information and Democracy (2020), *Working Group on Infodemics: Policy Framework*, https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf. [27]

Gazzetta Ufficiale (2023), *LEGGE 30 dicembre 2023, n. 213.*, https://www.gazzettaufficiale.it/eli/gu/2023/12/30/303/so/40/sg/pdf. [57]

Giansiracusa, N. (2023), *Three Easy Ways to Make Chatbots Safer*, https://www.scientificamerican.com/article/three-easy-ways-to-make-ai-chatbots-safer/. [115]

GIZ (2022), *Support to Media Freedom and Pluralism in the Western Balkans*, https://www.giz.de/en/worldwide/114194.html. [66]

Goldman, E. (2022), “The Constitutionality of Mandating Editorial Transparency”, *Hastings Law JournalHa*, Vol. 75/5, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=3985&context=hastings_law_journal. [26]

Government of Australia (2024), “Online misinformation”, Australian Communications and Media Authority, https://www.acma.gov.au/online-misinformation. [10]

Government of Australia (2023), *Foreign Influence Transparency Scheme*, https://www.ag.gov.au/integrity/foreign-influence-transparency-scheme. [102]

Government of Australia - The Treasury (2022), *News Media and Digital Platforms Mandatory Bargaining Code: The Code’s first year of operation*, https://treasury.gov.au/publication/p2022-343549. [79]

Government of Canada (2023), *Rapid Response Mechanism Canada: Global Affairs Canada*, https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/index.aspx?lang=eng. [111]

Government of Canada (2023), *The Online News Act*, https://laws-lois.justice.gc.ca/eng/acts/O-9.3/. [81]

Government of Canada (2021), *Security and Intelligence Threats to Elections (SITE) Task Force*, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html (accessed on 31 August 2023). [110]

Government of France (2022), *Concentration in the media sector in the digital era: From legal rules to regulation - Executive Summary*, https://www.igf.finances.gouv.fr/files/live/sites/igf/files/contributed/IGF%20internet/2.RapportsPublics/2022/Executive_summary_anti_concentration.pdf. [44]

Government of Ireland (2022), *Report of the Future of Media Commission*, https://www.gov.ie/pdf/?file=https://assets.gov.ie/229731/2f2be30d-d987-40cd-9cfe-aaa885104bc1.pdf#page=null. [58]

Government of Norway (2016), *Act relating to transparency of media ownership*, https://lovdata.no/dokument/NLE/lov/2016-06-17-64. [47]

Government of the Netherlands (2021), *Dutch Code of Conduct Transparency Online Political Advertisements*, https://www.idea.int/sites/default/files/news/news-pdfs/Dutch-Code-of-Conduct-transparency-online-political-advertisements-EN.pdf. [7]

Government of the UK (2003), *Communications Act 2003*, https://www.legislation.gov.uk/ukpga/2003/21/section/375. [46]

GPAI (2023), *Global Partnership on Artificial Intelligence - 2023 Ministerial Declaration*, https://gpai.ai/2023-GPAI-Ministerial-Declaration.pdf. [112]

Grand Duchy of Luxembourg (2023), *Loi du 7 août 2023 portant modification: 1) du Code pénal; 2) du Code de procédure pénale*, https://legilux.public.lu/eli/etat/leg/loi/2023/08/07/a516/jo. [42]

Grand Duchy of Luxembourg (2021), *Law of 30 July on an aid scheme in favour of professional journalism*, https://legilux.public.lu/eli/etat/leg/loi/2021/07/30/a601/jo/en. [56]

International IDEA (2024), *Protecting Elections in the Face of Online Malign Threats*. [104]

International IDEA (2023), "The Information Environment Around Elections", https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections. [108]

IPSOS, UNESCO (2023), *Survey on the impact of online disinformation and hate speech*. [105]

Keller, D. (2019), *Build Your Own Intermediary Liability Law: A Kit for Policy Wonks of All Ages*, Center for Internet and Society, Stanford Law School, https://cyberlaw.stanford.edu/publications/build-your-own-intermediary-liability-law-kit-policy-wonks-all-ages. [17]

Lai, S., N. Shiffman and A. Wanless (2023), *Operational Reporting By Online Services: A Proposed Framework*, https://carnegieendowment.org/files/202305-Operational_Reporting-final.pdf. [4]

Landemore, H. (2023), "Fostering More Inclusive Democracy with AI", *Finance and Development*, Vol. 60/4, pp. 12-14, https://www.scribd.com/document/689545094/What-AI-Means-for-Economics-By-IMF. [113]

Lenhart, A. (2023), *A Vision for Regulatory Harmonization to Spur International Research*, Lawfare, https://www.lawfareblog.com/vision-regulatory-harmonization-spur-international-research. [28]

Lim, G. and S. Bradshaw (2023), *Chilling Legislation: Tracking the Impact of "Fake News" Laws on Press Freedom Internationally*, Center for International Media Assistance, https://www.cima.ned.org/publication/chilling-legislation/#cima_footnote_3. [6]

Lomas, N. (2023), *Elon Musk takes Twitter out of the EU's Disinformation Code of Practice*, https://techcrunch.com/2023/05/27/elon-musk-twitter-eu-disinformation-code/. [8]

MacCarthy, M. (2021), *How online platform transparency can improve content moderation and algorithmic performance*, Brookings, https://www.brookings.edu/articles/how-online-platform-transparency-can-improve-content-moderation-and-algorithmic-performance/. [23]

Medill Local News Initiative (2023), *The State of Local News: The 2023 Report*, https://localnewsinitiative.northwestern.edu/projects/state-of-local-news/2023/report/. [40]

Meta (2023), *Changes to News Availability on our Platforms in Canada*, https://about.fb.com/news/2023/06/changes-to-news-availability-on-our-platforms-in-canada/. [82]

Nadler, J. and D. Cicilline (2020), *Investigation of Competition in Digital Markets*, https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519. [73]

Nelson, M. (2017), *What is to be done? Options for combating the menace of media capture*, Center for International Media Assistance, https://www.cima.ned.org/wp-content/uploads/2015/02/Capture12_CombatingMenace-of-Media-Capture.pdf. [43]

Newman, N. et al. (2023), *Digital News Report 2023*, Reuters Institute, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf. [2]

Nielsen, R. and S. Ganter (2018), "Dealing with digital intermediaries: A case study of the relations between publishers and platforms", *Media & Society*, Vol. 20/4, https://journals.sagepub.com/doi/full/10.1177/1461444817701318. [76]

OECD (2024), *Mapping and analysis of ODA to media and the integrity of information environments*. [62]

OECD (2022), *Building Trust and Reinforcing Democracy: Preparing the Ground for Government Action*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/76972a4a-en. [3]

OECD (2022), *Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions*, Building Trust in Public Institutions, OECD Publishing, Paris, https://doi.org/10.1787/b407f99c-en. [34]

OECD (2022), "Digital enablers of the global economy: Background paper for the CDEP Ministerial meeting", *OECD Digital Economy Papers*, No. 337, OECD Publishing, Paris, https://doi.org/10.1787/f0a7baaf-en. [75]

OECD (2022), "Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses", *OECD Policy Responses on the Impacts of the War in Ukraine*, OECD Publishing, Paris, https://doi.org/10.1787/37186bde-en. [91]

OECD (2022), *Handbook on Competition Policy in the Digital Age*, OECD, Paris, https://www.oecd.org/daf/competition-policy-in-the-digital-age/. [72]

OECD (2022), *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*, OECD Publishing, Paris, https://doi.org/10.1787/d234e975-en. [20]

OECD (2021), *Competition Issues concerning News Media and Digital Platforms*, https://web-archive.oecd.org/2021-11-19/616885-competition-issues-concerning-news-media-and-digital-platforms-2021.pdf. [77]

OECD (2021), *OECD Regulatory Policy Outlook 2021*, OECD Publishing, Paris, https://doi.org/10.1787/38b0fdb1-en. [14]

OECD (2019), *Going Digital: Shaping Policies, Improving Lives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264312012-en. [71]

OECD (2019), "Recommendation of the Council on Artificial Intelligence", *OECD Legal Instruments*, OECD/LEGAL/0449, OECD, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. [114]

OECD (2014), *Accountability and Democratic Governance: Orientations and Principles for Development*, DAC Guidelines and Reference Series, OECD Publishing, Paris, https://doi.org/10.1787/9789264183636-en. [32]

OECD (2011), *The Role of Internet Intermediaries in Advancing Public Policy Objectives*, OECD Publishing, Paris, https://doi.org/10.1787/9789264115644-en. [18]

Office of the Director of National Intelligence (2023), *2023 Annual Threat Assessment Report*, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf. [84]

Official Journal of the European Union (2022), *COUNCIL DECISION (CFSP) 2022/2478 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.LI.2022.322.01.0614.01.ENG. [96]

OSCE (2019), *The Tallinn Guidelines on National Minorities and the Media in the Digital Age*, https://www.osce.org/files/OSCE-Tallinn-guidelines-online%203.pdf. [61]

Polyakova, A. and D. Fried (2019), *Democratic defense against disinformation 2.0*. [106]

Poritz, I. (2023), *States Are Rushing to Regulate Deepfakes as AI Goes Mainstream*, https://www.bloomberg.com/news/articles/2023-06-20/deepfake-porn-political-ads-push-states-to-curb-rampant-ai-use. [117]

Quétier-Parent, S., D. Lamotte and M. Gallard (2023), *Elections & social media: the battle against disinformation and trust issues*, Ipsos – UNESCO Study on the impact of online disinformation during election campaigns, https://www.ipsos.com/en/elections-social-media-battle-against-disinformation-and-trust-issues. [1]

RSF (2023), *2023 World Press Freedom Index – journalism threatened by fake content industry*, https://rsf.org/en/2023-world-press-freedom-index-journalism-threatened-fake-content-industry. [33]

RSF (2020), *RSF's 2020 Round-up: 50 journalists killed, two-thirds in countries "at peace"*, https://rsf.org/en/news/rsfs-2020-round-50-journalists-killed-two-thirds-countries-peace. [35]

Scott, M. (2023), *I have a plan to fix social media*, https://www.politico.eu/newsletter/digital-bridge/i-have-a-plan-to-fix-social-media/. [29]

Shmon, C. and H. Pederson (2022), *Platform Liability Trends Around the Globe: From Safe Harbors to Increased Responsibility*, https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-safe-harbors-increased-responsibility. [16]

Shmon, C. and H. Pederson (2022), *Platform Liability Trends Around the Globe: Recent Noteworthy Developments*, https://www.eff.org/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments. [15]

State of California (2018), *Senate Bill No. 1001*, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001. [12]

Sweney, M. (2023), *'The model is broken': UK's regional newspapers fight for survival in a digital world*, https://www.theguardian.com/media/2023/mar/26/regional-newspapers-fight-for-survival-in-a-digital-world. [39]

The Moscow Times (2022), *Billions for propaganda. Budget spending on state media tripled against the backdrop of the war*, https://www.moscowtimes.ru/2022/04/12/milliardi-na-propagandu-rashodi-byudzheta-na-gossmi-podskochili-vtroe-na-fone-voini-a19511. [92]

The Times of Israel (2019), *Election judge bars anonymous internet ads despite Likud objection*, https://www.timesofisrael.com/election-judge-bars-anonymous-internet-adds-despite-likud-objection/. [31]

The United States Department of Justice (2023), *Foreign Agents Registration Act*, https://www.justice.gov/nsd-fara. [99]

The United States Department of Justice (2022), *Court finds RM broadcasting must register as a foreign agent*, https://www.justice.gov/opa/pr/court-finds-rm-broadcasting-must-register-foreign-agent. [100]

The United States Department of Justice (2021), *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere. [101]

U.S. Department of State (2023), *How the People's Republic of China Seeks to Reshape the Global Information Environment*, https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/. [95]

U.S. Department of State (2020), *GEC Special Report: Pillars of Russia's Disinformation and Propaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf. [90]

U.S. White House (2023), *Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence*, https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/. [118]

UNDP (2023), *Promoting information integrity in elections*. [103]

UNESCO (2022), *Elections in Digital Times: A Guide for Electoral Practitioners*. [107]

UNESCO (2022), *Finding the funds for journalism to thrive: policy options to support media viability*, United Nations Educational, Scientific and Cultural Organization. [69]

UNESCO (2021), *UNESCO observatory of killed journalists*,, United Nations Educational, Scientific and Cultural Organization, https://en.unesco.org/themes/safety-journalists/observatory?field_journalists_date_killed_value%5Bmin%5D%5Byear%5D=2022&field_journalists_date_killed_value%5Bmax%5D%5Byear%5D=2022&field_journalists_gender_value_i18n=All&field_journalists_nationality_tid_i. [36]

United States Department of Homeland Security (2018), *Foreign Interference Taxonomy*, https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_october_15.pdf. [86]

United States Department of Justice (2022), *Recent FARA Cases*, https://www.justice.gov/nsd-fara/recent-cases. [38]

United States Department of State (2022), *Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propoaganda Ecosystem*, https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf. [93]

USAID (2023), *Administrator Samantha Power Delivers Remarks at the "Advancing Technology for Democracy" Event*, https://www.usaid.gov/news-information/speeches/mar-30-2023-administrator-samantha-power-delivers-remarks-at-the-advancing-technology-for-democracy-event. [67]

USAID (2023), *Interventions to Counter Misinformation: Lessons from the Global North and Applications to the Global South*, https://pdf.usaid.gov/pdf_docs/PA0215JW.pdf. [68]

Vilmer, J. (2019), *The "Macron Leaks" Operation: A Post-Mortem*. [97]

NOTES

[1] For additional information, see: https://santaclaraprinciples.org/.

[2] For additional information, see: https://c2pa.org/.

[3] For additional information, see: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[4] Information provided by the Government of Lithuania.

[5] For additional information, see: https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180. Note that draft Bill 2630/2020 seeks to update the Marco Civil da Internet by, in part, including a "duty-of-care" for digital platforms to take action on specific illegal content.

[6] For additional information, see: https://www.infrastructure.gov.au/have-your-say/new-acma-powers-combat-misinformation-and-disinformation.

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2002:201:FULL.

[8] See of S.1989 – Honest Ads Act Section 8(4)(ii) (https://www.congress.gov/bill/115th-congress/senate-bill/1989/text) and Proposal for a Regulation of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising Article 2(2)(b) (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0731).

[9] For additional information, see: https://fom.coe.int/en/accueil.

[10] For additional information, see: https://www.mfrr.eu/monitor/.

[11] For additional information, see: https://www.coe.int/en/web/freedom-expression/safety-of-journalists-campaign

[12] For additional information, see: https://cmpf.eui.eu/media-pluralism-monitor-2023/.

[13] Countries in the study included: Austria; Belgium; Bulgaria; Croatia; Cyprus; Czechia; Denmark; Estonia; Finland; France; Germany; Greece; Hungary; Ireland; Italy; Latvia; Lithuania; Luxembourg; Malta; The Netherlands; Poland; Portugal; Republic of North Macedonia; Romania; Serbia; Slovak Republic; Slovenia; Spain; Sweden; Türkiye; United Kingdom.

[14] For additional information, see: https://lovdata.no/dokument/NLE/lov/2020-05-29-59.

[15] For more information on background and recommendations related to improving the policy, funding, and enabling environment for independent professional journalism, see: (Forum on Information and Democracy, 2021[54]).

[16] Such as the requirement in Luxembourg that the public service media must be organised in a way that "ensures autonomy and independence from the State and social, economic and political entities with regard to editorial decisions" – see Luxembourg's *Law of 12 August 2022 on the organisation of the public establishment 'Public Service Media 100,7' and amending the amended Law of 27 July 1991 on electronic media* for additional information.

[17] For additional information, see: https://freedomonlinecoalition.com/donor-principles-for-human-rights-in-the-digital-age/.

[18] For additional information, see: https://ifpim.org/.

[19] For text of the legislation, see: https://www.legislation.gov.au/Details/C2019C00133.

[20] Generative AI refers to artificial intelligence systems capable of generating text, images, or other media in response to prompts.

From:

Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity

Access the complete publication at:
https://doi.org/10.1787/d909ff7a-en

Please cite this chapter as:

OECD (2024), “Implementing policies to enhance the transparency, accountability, and plurality of information sources”, in *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/b45bbb4d-en