HIGHLIGHTS
BROCHURE

Facts Not Fakes

Tackling disinformation, strengthening information integrity

OECD
BETTER POLICIES FOR BETTER LIVES

The urgent threat posed by disinformation demands actions.

Rising disinformation has far-reaching consequences in many policy areas ranging from public health to national security or the fight against climate change. The deliberate spread of false and misleading information can **cast doubt on factual evidence, jeopardise the implementation of public policies and undermine people's trust in the integrity of democratic processes and institutions.**

The digital transformation of societies has reshaped how people interact and engage with the information space. Anyone with an Internet connection can produce and distribute content. While this increased accessibility offers unprecedented access to knowledge, can foster citizen engagement and innovative news reporting, it also provides fertile ground for the rapid spread of false and misleading information.

Providing conceptual guidance

Misinformation can be defined as false or inaccurate information that is shared unknowingly and is not disseminated with the intention of deceiving the public.

Disinformation can be defined as false, inaccurate, or misleading information deliberately created, presented, and disseminated. A piece of information created with the intention to deceive or mislead, may be shared without malicious motives by people who genuinely believe it to be true, hence perpetuating disinformation.

Information integrity is the result of an information environment that is conducive to the availability of accurate, evidence-based, and plural information sources enabling citizens to be exposed to a variety of ideas, make informed choices, and better exercise their rights. Disinformation poses a pervasive threat to information integrity.

Disinformation has always existed. **What is new today is the scale of these operations and the constant evolution and sophistication of the techniques used to deliberately deceive or mislead people.**

Mis- and disinformation are exacerbated by the surge in viral content, fuelled by economic incentives and recommendation algorithms that often prioritise the value of information as a commodity over its benefit to society. This comes at the expense of quality journalism, already facing increasing financial pressures, changes in media ownership and high-risks environments. Moreover, new technologies are increasingly designed to respond to the psychological and behavioural drivers that underpin how people search for, process, and consume information.

When do the threats posed by disinformation become particularly daunting?

Unequal access to learning resources, local media deserts and insufficient levels of media and digital literacy increase the vulnerability of certain communities to misinformation and disinformation

Abuse of Artificial Intelligence to create inauthentic audio-visual content that is increasingly realistic (e.g. deepfakes), amplify disinformation (e.g. via bots), and enable micro-targeted messaging

Targeted disinformation spread during electoral cycles with the intention of influencing voters' ability to make informed decisions can interfere with essential democratic activities and undermine trust

Manipulation of information and interference by foreign agents can create and exploit social frictions in a strategic and coordinated manner to destabilise democracy

Disinformation threats, with characteristics specific to each local context, endanger democracy and highlight the need to strengthen the integrity of information spaces. Upholding information integrity is essential to safeguarding freedom of expression, including the freedom to seek, receive, and impart information and ideas.

How can governments step up to the challenge?

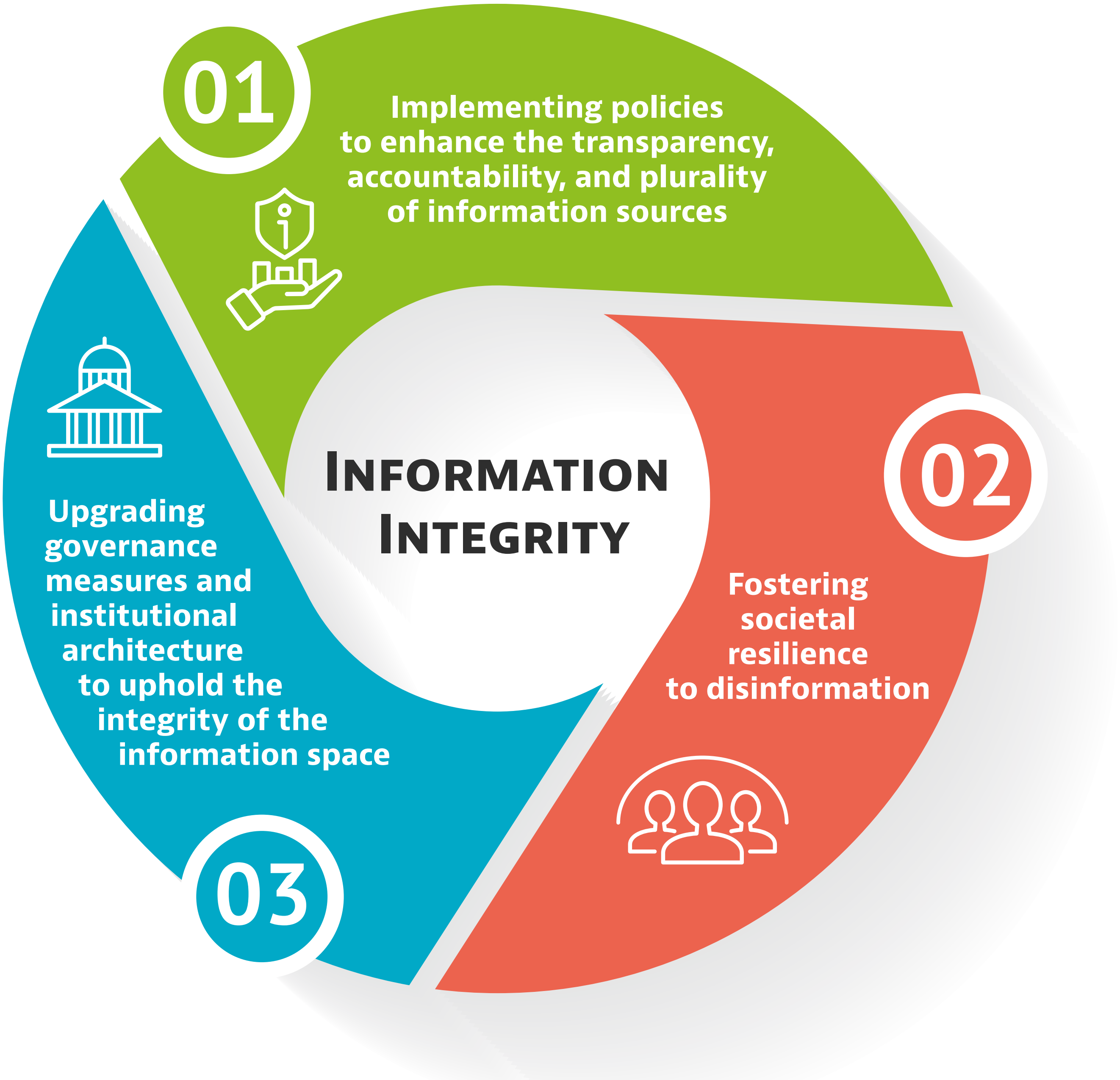
Many countries have started examining the adequacy of existing policies and institutions to effectively address current and future realities of a rapidly evolving information environment.

The report "***Facts not fakes: Tackling disinformation, strengthening information integrity***" is a first baseline assessment of how countries can upgrade their policies and institutional structures to support an environment where reliable information can thrive, while ensuring the vigilant protection of human rights. It also examines the synergies between different policy areas to provide a better understanding of the conditions that contribute to information integrity.

Building on the findings of a survey of 24 OECD countries,[1] the report presents case studies of initiatives to strengthen information integrity through the collective efforts of all societal actors, identifies areas for improvement, and lays out considerations and a path forward for how governments can play a constructive role in this area.

The report presents an analytical framework aimed at strengthening information integrity by examining three complementary policy dimensions, recognising that while country contexts may differ, **common areas of policy action exist.**

A framework to strengthen information integrity.


INFORMATION INTEGRITY
01
Implementing policies to enhance the transparency, accountability, and plurality of information sources
02
Fostering societal resilience to disinformation
03
Upgrading governance measures and institutional architecture to uphold the integrity of the information space

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

Building information integrity and addressing disinformation rest in large part on the actors that produce content and the channels through which it is disseminated, including digital platforms (online and social media), as well as traditional media.

Regarding digital platforms, policies in this space need to move beyond self-regulation, as appropriate. This entails exploring policies that increase the degree of accountability and transparency of online platforms, to ensure that their market-power and commercial interests do not contribute to disproportionately vehicle disinformation. Transparency is also key in relation to content moderation practices and algorithms, helping provide valuable comparative information across online platforms. Simultaneously, there is a need to mitigate threats by improving understanding of the potential risks associated with digital platforms. Examples include the EU Digital Service Act and the UK Online Safety Act 2023.

Regarding the media and journalists, policies in this space need to focus on a diverse, plural, and independent media sector, with a needed emphasis on local journalism - so that it maintains its crucial role as a watchdog for the public interest. Fostering a diverse and competitive media landscape will require limiting market concentration, promoting transparency and diversity of media ownership, and editorial independence. Along these initiatives, supporting independent and high-quality public service media, as well as exploring direct and indirect financial support to journalists and media outlets, adhering to transparent criteria, will be key to strengthen the integrity of the information space. Examples include the proposed EU Media Freedom Act and Norway's Media Liability Act.

Policies will also need to counter specific risks in the information space, including the spread of disinformation during electoral periods, foreign information manipulation and interference campaigns, and the implications of artificial intelligence. Developing policies to better understand and mitigate the potential impact of AI on disinformation, including generative tools, is critical to harness the power of these technologies. In addition, illuminating covert and potentially malign communication activities by applying policies such as the Foreign Agents Registration Act (FARA) in the United States or the Foreign Influence Transparency Scheme in Australia can help counter foreign malign interference in the information space. Safeguarding information integrity during electoral cycles by monitoring threats and providing timely and reliable information will also be important tools to enable citizens to exercise their democratic rights.

02 Fostering societal resilience to build individual and collective defences against disinformation

As society becomes increasingly exposed to multiple sources of information, from traditional media to social media platforms, individuals need to be equipped with the tools and skills to navigate this complex environment. **Empowering individuals to cultivate critical thinking skills and to identify and counter the spread of false and misleading information is therefore crucial.** This can be achieved by integrating media and information literacy (MIL) into educational curricula, implementing tailored training programmes for educators and professionals of all ages, evaluating the impact of MIL initiatives, and promoting research to understand the populations most vulnerable to the risks of disinformation. Examples include Portugal's National Plan for Media Literacy, Finland's National Media Education Policy and Canada's Digital Citizen Initiative. **Policies should also focus on promoting proactive and transparent communication efforts, free from political influence, aimed at ensuring the public is well-informed about disinformation threats.**

Engagement with the public and non-governmental stakeholders should ultimately be guided by efforts to protect and strengthen civic space to foster more open, transparent, and accountable governance. Examples include the Swedish Psychological Defence Agency. **Finally, all sectors of society need to be mobilised to formulate comprehensive, evidence-based policies in support of information integrity.** Examples include Ireland's Future of Media Commission.

03 Upgrading governance measures and institutional architecture to uphold the integrity of the information space

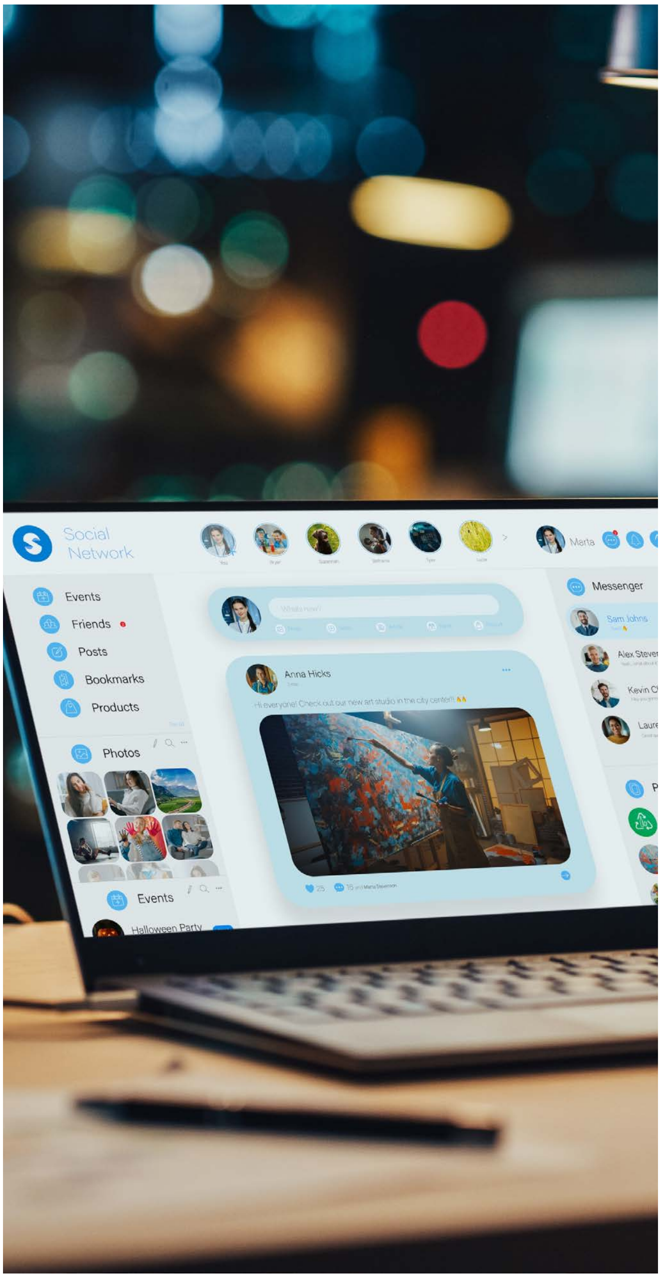
Government policies need to be guided by a strategic vision. A multifaceted challenge like disinformation, involving multiple actors, channels, and tactics, needs to be addressed in a strategic manner. However, according to the report, **national strategies for tackling disinformation remain the exception rather than the rule.**

It is important that governments consider the advantages of developing explicit national strategies that delineate institutional responsibilities, prevent duplication of efforts and information asymmetries across government. To help articulate this process some countries have established working groups. For instance, *Ireland's National Counter Disinformation Strategy Working Group*, created in 2023, resulted from a recommendation of Ireland's Future of Media Commission that advocated for a more cohesive and strategic approach to combat the damaging impact of disinformation on Irish society and democracy.

Internal co-ordination will also support these efforts. The ways in which countries co-ordinate their responses to disinformation threats and efforts to enhance information integrity are varied and evolving rapidly. At the national level, responsibilities are found across the public sector, including the centre of government, line ministries, security and intelligence agencies, and regulators.

According to data from the report, **only half of the countries surveyed have at least one cross-government mechanism dedicated to co-ordinate national efforts to identify and respond to disinformation threats and/or to provide technical advice on policies related to this matter.** These are generally established either as central units (such as offices or cells) that have an official mandate to co-ordinate responsibilities, and/or as formal task forces or working groups composed of public servants from across the government.

The complexity of efforts to reinforce information integrity in democracies calls for establishing co-ordination mechanisms to facilitate co-operation within and between governments.



Government co-ordination mechanisms to tackle disinformation

Cross-government coordination unit

Government unit, office or cell that has an official mandate to co-ordinate policies and actions – across different administrative agencies/levels – that seek to tackle the threats posed by disinformation and enhance information integrity.

These coordination mechanisms facilitate the allocation of human and financial resources and avoid the duplication of policy efforts ensuring both vertical (central authority) and horizontal collaboration (internal coherence and efficiency) between government bodies.

Examples include:

- France's VIGINUM
- Lithuania's National Crisis Management Centre
- Sweden's Psychological Defense Agency
- United States' Global Engagement Centre

Task force

Expert group of public officials set up to provide co-ordinated technical advice to the government on how to tackle specific threats posed by disinformation and/or to develop targeted measures to enhance information integrity.

Different task forces, of permanent or temporary nature, can be created within the same country, allowing for more responsive interventions and technical work such as dealing with information manipulation in the context of elections.

Having a function similar that of a task force, an advisory committee may also be established, but these usually involve experts from outside the government.

Examples include:

- Australia's Electoral Integrity Assurance Taskforce
- Canada's Security and Intelligence Threats to Elections (SITE) Task Force

Source: Authors

Collaborative solutions are needed, as no government can solve this problem alone.

Peer learning can contribute to better policies across democratic countries facing similar issues. There are multiple international fora and co-ordination mechanisms, each presenting different configurations of country alliances and thematic priorities. International organisations, specialised or *ad hoc* groups, and government-led convenings and framework agreements account for the primary methods by which countries engage on these issues bilaterally and multilaterally. According to data from the report, **90% of surveyed countries indicated that strengthening co-operation with partner countries is a priority area for improvement when it comes to tackling disinformation threats.**

oe.cd/facts-not-fakes

OECD
Reinforcing
Democracy
Initiative

OECD
BETTER POLICIES FOR BETTER LIVES

[1] The report "Facts not fakes: Tackling disinformation, strengthening information integrity", includes data from 24 OECD member countries obtained from the survey "Institutional architecture and governance practices to strengthen information integrity" designed by the OECD DIS/MIS Resource Hub team. The countries participating are Australia, Canada, Chile, Colombia, Costa Rica, Estonia, Finland, France, Greece, Italy, Ireland, Latvia, Lithuania, Luxembourg, Netherlands, Norway, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Türkiye and the United States. Responses were provided by government authorities from April to September 2023. Given the rapid pace of developments in the field of disinformation and information integrity, it is important to note that this data reflects the state of affairs in September 2023.