DIRECTORATE GENERAL OF DEMOCRACY AND HUMAN DIGNITY
DIRECTORATE FOR DEMOCRACY

EUROPEAN CONVENTION ON HUMAN RIGHTS
CONVENTION EUROPÉENNE DES DROITS DE L'HOMME
1950 - 2025 75

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

CDMSI(2025)17rev
4 December 2025

Steering Committee on Media and Information Society
CDMSI

28th Meeting

Strasbourg, 3-5 December 2025

Resisting disinformation: 10 building blocks to strengthen information integrity

Adopted by the Steering Committee on Media and Information Society on 4 December 2025

This document is final, subject to editorial revision

*Document elaborated with the support of **Konrad Beyeler-Simon** and **Urbano Reviglio**, Research Associates at the Centre for Media Pluralism and Media Freedom, European University Institute, Florence, Italy.*

The following experts participated in an expert consultation process organised by the CDMSI and provided valuable input for which the CDMSI is grateful.

- **Marie Bohner**, Head of Development and partnerships, Digital investigation, Agence France-Presse, France
- **Sally Broughton Micova,** Associate Professor of Communications Policy and Politics, University of East Anglia), United Kingdom
- **Bastien Carniel**, Data and Policy Lead, Science Feedback; President, Vigilia.Tech
- **Eileen Culloty**, Assistant Professor, School of Communications, Dublin City University, Ireland
- **Thomas Häussler**, Media Specialist, Federal Office of Communications (OFCOM), Switzerland
- **Krisztina Rozgonyi**, Senior Scientist, Austrian Institute of Technology, Austria
- **Joanna Szymanska**, Head of Programmes and Strategy for Europe, Article 19, United Kingdom)
- **Damian Tambini**, Associate Professor and Distinguished Policy Fellow, London School of Economics, United Kingdom
- **Vitor Tomé**, Expert for the Council of Europe and the European Commission, Lecturer, Autonoma University of Lisbon, Portugal
- **Cristian Vaccari**, Chair of Future Governance, Public Policy, and Technology at the University of Edinburgh, United Kingdom
- **Giovanni Zagni**, Director, Pagella Politica and Facta, Member of the Executive Board of EDMO, Italy.

Resisting disinformation:
Ten building blocks to strengthen information integrity

Contents

Introduction

At a time of geopolitical tension, economic turbulence and accelerating environmental and technological change, democratic societies are confronted with complex decisions that demand informed public debate. Yet, as acknowledged by the 2025 Report of the Secretary General of the Council of Europe calling for a New Democratic Pact for Europe,[1] the information environment on which this debate relies is increasingly polluted by misleading, deceptive, or manipulative content. For at least a decade now, "disinformation" has come to be one of the most pressing challenges to democratic societies, blurring the boundaries between facts and falsehood, opinion and manipulation, ultimately undermining public trust and informed choices. It is therefore unsurprising that the United Nations Global Risk Report 2024 listed disinformation among the gravest risks for states and as a threat that many of them feel ill-prepared to.[2]

This policy document draws attention to the importance of a comprehensive national strategy to counter disinformation and strengthen information integrity, emphasising its role in fostering societal resilience to information disorder and reinforcing trust in democratic institutions and processes. Based on existing Council of Europe standards, it singles out areas of action that such strategies may cover, as well as the foundational principles to ground such strategy on the values of the Organisation. Therefore, it provides an important contribution to the New Democratic Pact for Europe,[3] a collective and inclusive strategic process launched by the Council of Europe in 2024 to develop concrete structural solutions and innovative practices aimed at strengthening the foundations of democracy and making it more tangible for everyone.

Previous Council of Europe documents have defined "disinformation" as "verifiably false, inaccurate or misleading information *deliberately* created and disseminated to cause harm or pursue economic or political gain by deceiving the public".[4] However, there is a growing consensus that disinformation in this narrow sense is only a part of the problem, and its spread is hardly separable from a range of other forms of content that may be harmful to information integrity – some of which may lack harmful intent or may not contain clear-cut false information. Therefore, in this document the term "disinformation" will be used in a broader sense, encompassing a variety of related harmful phenomena such as information operations, propaganda and foreign information manipulation and interference (FIMI), as well as other "information disorders" affecting our societies.[5] While these concepts may differ in their nature and origins, they all cover information-related actions that contribute to the disruption of public discourse, the erosion of trust and societal polarisation. Ultimately, they impact on people's decisions in private and public life, shaping opinions, behaviours and participation in democratic processes.

In response to the broader range of harmful information phenomena, beyond narrowly defined disinformation, the concept of "information integrity" has emerged as a constructive and more comprehensive approach to tackling information disorder, safeguarding public trust and supporting democratic processes. In a recent recommendation on the topic, the Organisation for Economic Co-operation and Development (OECD) defines information integrity broadly as the product of an "information environment that promotes access to accurate, reliable, evidence-based, and plural information sources and that enable[s] individuals to be exposed to plural and diverse ideas, make informed choices, and better exercise their rights".[6] Information integrity thus evokes an holistic approach to information

disorder that seeks to reinforce the systems, norms and practices that sustain the availability, reliability and pluralism of information on which democratic processes depend. As called for by a United Nations report on Global Principles for Information Integrity, this objective can be achieved through building societal trust and resilience, creating healthy incentives, promoting public empowerment, supporting independent, free and pluralistic media and fostering transparency and research.[7]

Several existing Council of Europe instruments, widely referred to in this document, are also designed to foster a healthy and pluralistic information environment in which reliable information is produced, disseminated and readily accessible. They often address disinformation and misinformation as distinct but closely interrelated challenges, recommending concrete actions for states and other relevant actors. Drawing on these instruments, and with the aim of providing a coherent and comprehensive framework for member states, the Committee of Ministers of the Council of Europe has tasked its Steering Committee on Media and Information Society (CDMSI) to develop a strategic policy document that offers practical tools and recommendations to resist disinformation and strengthen information integrity.[8] In line with the commitments of the Heads of State and Government of the Council of Europe affirmed in the Reykjavík Principles for Democracy,[9] this document is intended to support member states in addressing disinformation and related information disorders through comprehensive policies grounded in democratic principles, the rule of law and respect for human rights, particularly freedom of expression.

Measures recommended in this document are primarily aimed at governments and state institutions. Public authorities have a unique mandate and responsibility to safeguard democratic institutions, uphold the rule of law and protect the information environment through public policy, regulation, funding and co-ordination at the national level. Their role is essential in setting the legal and institutional framework within which other actors operate. That said, effectively tackling disinformation requires a whole-of-society response. Civil society organisations, media outlets, academic and other educational institutions, the private sector and the general public all play critical roles in building resilience to information disorder. Detailed guidance for these stakeholders can be found in the 2017 Report of the Council of Europe on information disorder,[10] which has pioneered international efforts in analysing and responding to threats to information integrity and remains an important point of reference, offering 35 recommendations for various actors including governments, technology companies, media and civil society.

In addition, while many policies to counter disinformation focus on the digital environment, and especially on large online platforms, disinformation and challenges to information integrity also manifest in traditional media environments, such as in the audiovisual sector and the press. These should not be left unattended. Thus, most recommendations put forward in this document equally apply in all communication contexts. Moreover, they are meant to balance immediate, operational measures with long-term, structural actions aimed at not just mitigating the negative effects of disinformation but also addressing its root causes.

In preparation of this document, a questionnaire was circulated among CDMSI members to gather the experiences and challenges of member states in tackling disinformation and other information disorders. The answers showed that disinformation and related challenges to information integrity require flexible responses that can easily adapt to the rapidly evolving information environment and related risks. According to answers provided by member states, deepfakes and AI-driven disinformation are some of the most pressing challenges for the

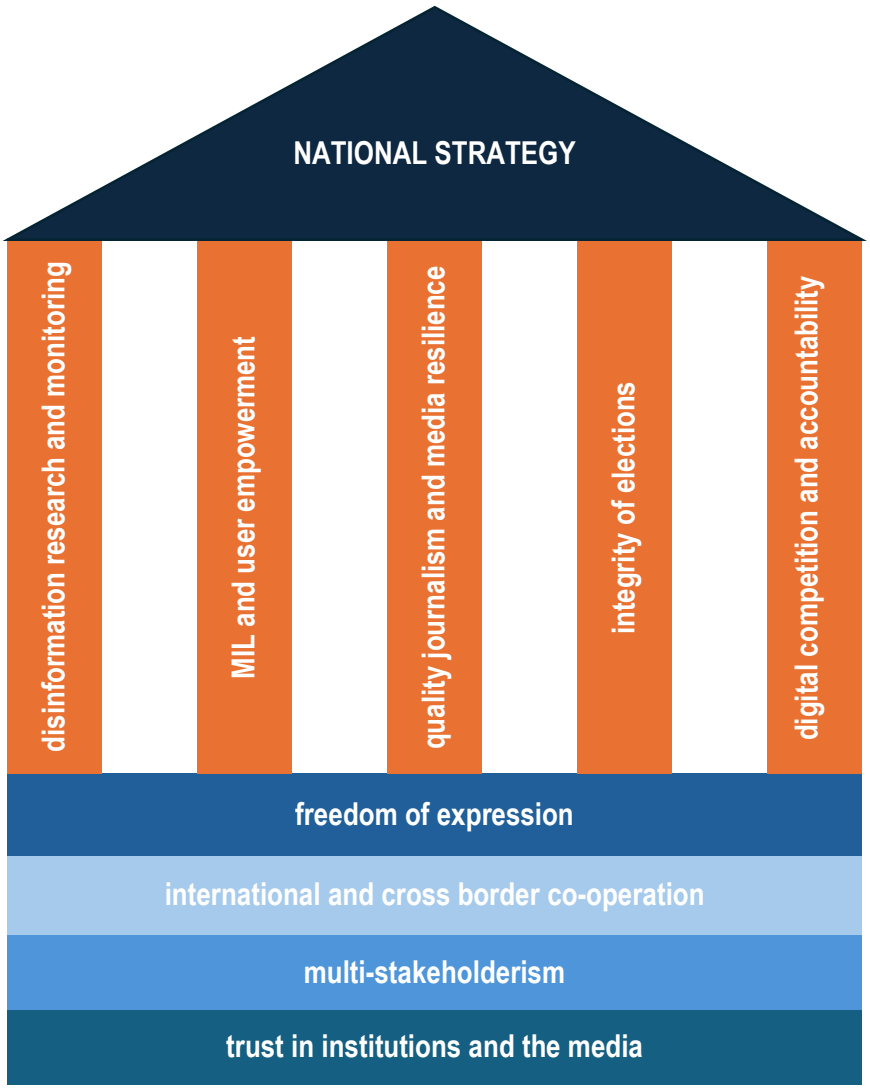
coming years.[11] At the same time, member states recognise that new threats are likely to emerge, requiring coherent and timely responses. Empowering individuals to recognise misleading narratives and attempts at information manipulation is essential to ensuring they can preserve and exercise their agency within the information environment.

In light of the variety of responses adopted across member states and the evolving nature of disinformation, the recommendations proposed here aim to offer a coherent framework to enhance national resilience to this challenge in line with human rights, the rule of law and democratic values. Moreover, states need to fully consider and respond to the various ways in which disinformation specifically affects women and girls, including through promoting gender-based violence and stereotyping, different age groups, such as children and seniors, as well as groups and individuals in situations of vulnerability or at risk of discrimination, including people with disabilities, national ethnic, linguistic and religious minorities, LGBTI communities and people with a migration background. The proposed framework should not be understood as a blueprint or a model strategy: information integrity faces common challenges, but these may take different intensity, shape and urgency in different local contexts. While there is no one-size-fits-all solution, human-rights-based, co-ordinated, multi-stakeholder and context-sensitive efforts, that are supported by evidence-based policy and international co-operation, can significantly improve the capacity to respond to disinformation in both the short and long term.

Fostering information integrity is crucial for strong democracies in which individuals make informed decisions about matters of public interest and contributes to societies' resilience towards harmful interferences of foreign state and non-state actors. This document aims to provide comprehensive guidance for policymakers to address one of today's major challenges in a holistic and co-ordinated manner, effectively leveraging available resources both domestically and internationally.

Building blocks at a glance

The recommendations proposed in this document are framed as 10 “building blocks” of a sound construction for resisting disinformation: the roof represents the overarching goal, consisting in the adoption of a comprehensive national strategy to counter disinformation and strengthen information integrity. It is supported by five pillars, each representing a key policy area of action, while the entire structure rests on a foundation of four core principles, which are essential for effective and human rights-compliant responses. Below there is an overview of all “building blocks” and their associated general recommendations, which are further detailed in the document.



Goal

Building block 1
Elaborate a structured national strategy

Develop and implement a robust national strategy to counter disinformation and promote information integrity that sets the basis for a clear legal framework, long-term planning and co-ordination between public institutions and other actors such as media, academia, civil society organisations and private actors, including digital platforms. This is fundamental to address the structural problems that undermine the information environment.

Pillars

Building block 2
Enhance disinformation research and monitoring

Prioritise the understanding and monitoring of how disinformation is generated and spreads, along with the factors that influence its impact, as this is essential to developing effective, evidence-based responses. This effort should encompass both real-time monitoring and long-term academic research.

Building block 3
Strengthen media and information literacy and user empowerment

Develop and implement a comprehensive, multidimensional media and information literacy (MIL) strategy that actively involves diverse stakeholders to empower to become informed media users and navigate increasingly complex and sometimes biased and/or manipulative content. MIL should be integrated in lifelong learning programs for sustainable, long-term success. In addition, promote the implementation by digital platforms of tools through which users can better control their informational experience online.

Building block 4
Support quality journalism and foster media resilience

Actively support the production of high quality, independent and pluralist journalism and foster its visibility and impact, including public interest content prominence. Quality journalism requires financial stability, protection from political and economic pressure or capture, safety, appropriate working conditions, as well as adherence to strong professional and ethical standards.

Building block 5
Safeguard the integrity of elections

Ensure the integrity of elections by setting clear rules for fair and balanced campaigning both online and offline. Take proactive measures to ensure that citizens are informed about the election process and the issues at stake.

Building block 6
Promote competition and accountability in the digital ecosystem

Work towards reducing the dependence from large tech monopolies by fostering “digital sovereignty” through the development of open-source technologies, likely to ensure that digital infrastructure, as well as its development and operation, comply with human rights and

other relevant legal provisions and standards, empower users and compete effectively with existing global platforms.

Foundational principles

Building block 7
Uphold freedom of expression

When adopting legislative or other measures to counter disinformation and protect information integrity, give priority to actions that do not interfere with freedom of expression. Ensure that any interference with the rights protected by Article 10 comply with its paragraph 2 and is applied within a rule of law framework. Promote independent public oversight of the measures taken by platforms to address risks to information integrity and their effects on freedom of expression.

Building block 8
Facilitate international and cross border co-operation

Foster structured and sustained international co-operation mechanisms to effectively co-ordinate responses and share best practices across borders.

Building block 9
Foster multi-stakeholder synergies

Seek and enable the effective participation and consultation of all relevant stakeholders including those that are often under-represented, such as the general public, civil society organisations, traditional and new media, platforms, academia and other actors.

Building block 10
Build long-term trust in institutions and the media

Work on comprehensive, long-term solutions to the existing information integrity challenges, with an emphasis on building trust in democratic institutions, quality journalism and news media.

Goal

Building block 1 – Elaborate a structured national strategy

Member states often lack structured responses to adequately address the harmful effects of disinformation and rely on scattered or reactive measures.[12] A well-designed national strategy, based on long-term planning and co-ordinated efforts between a diverse range of stakeholders, is essential to tackle the systemic issues that undermine the information environment. Without such a comprehensive national strategy, member states risk relying on fragmented and reactive measures that fail to address structural challenges and mitigate systemic threats. Such measures may even be counterproductive, inadvertently restricting freedom of expression or further eroding public trust in media and democratic institutions.

Against this background, **addressing disinformation and promoting information integrity requires a clear and harmonised legal framework, as well as comprehensive, whole-of-society approaches that prioritise proactive and positive measures** aimed at fostering a resilient information environment, on both the production and consumption sides. When measures to counter disinformation interfere with the exercise of the right to freedom of expression, they must strictly comply with the requirements of Article 10, paragraph 2, of the European Convention on Human Rights, namely they should be provided by the law and be necessary in a democratic society in pursuance of one of the legitimate aims indicated there. Hence, such restrictive measures should be considered with prudence, and criminal law provisions only be used as a last resort (see also below, Building block 7).

Furthermore, it is essential to keep in mind that disinformation is a complex and evolving "wicked problem",[13] affecting multiple areas of society and touching on several policy domains. **The challenges posed by it therefore demand co-ordinated responses across sectors** such as news production and dissemination, government communications, actions to ensure the integrity of elections, education and media and information literacy, national security and even equality and social cohesion policies.

Purveyors of disinformation often exploit existing societal vulnerabilities, discontents and divisions, targeting particular groups such as women and girls, LGBTI people, people with a migration background or minorities.[14] They also sow distrust in institutions,[15] the media and journalists, science and academia, as well as in critical sectors such as health[16] and environmental protection.[17] This not only increases the marginalisation and vulnerability of targeted groups but also hampers public understanding and trust in vital areas, ultimately weakening society's ability to respond effectively to critical challenges. Additionally, the erosion of trust in institutions and the media undermines democratic governance, weakens social cohesion, and makes it more difficult to build consensus around public policies and collective actions.

Furthermore, the nature of disinformation is constantly evolving, which requires constant and swift adaptation of both the recognition and definition of the challenge and the responses it demands.[18] For example, across countries, there is growing concern that emerging challenges from AI-driven disinformation, such as deepfakes or synthetic news, will further exacerbate the reactive and fragmented approaches currently taken by several member states.[19]

Given this background, it is essential to develop **a co-ordinated, cross-sectoral and regularly updated national strategy to counter disinformation and promote information integrity, supported with appropriate human, financial and technological resources**. To be effective, such a strategy should be grounded in the five pillars and four foundational principles identified in this document, which constitute the essential elements to support an effective strategy to resist disinformation.

Council of Europe standards

- Recommendation CM/Rec(2022)11 on principles for media and communication governance and Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression outline procedural and substantive principles that can serve as a foundation for national strategies. They also emphasise that there must be a clear legal framework of the online environment – an extremely efficient vehicle for disinformation – which defines the role to all actors involved, outlines their responsibilities and the limits to their actions. Such a legal framework should be an essential component of any effective national strategy on countering disinformation.
- The Parliamentary Assembly Resolution 2567 (2024) on propaganda and freedom of information in Europe calls on member states to develop holistic strategies to address both illegal propaganda and harmful but legal content.

Promising practices

Ireland provides a promising example on how to approach the design of a structured strategy on countering disinformation. The National Counter Disinformation Strategy, published in April 2025, was developed by a multi-stakeholder working group – including representatives from government departments, independent regulators, civil society, academia, research and industry – with input from the wider public.[20] The strategy emphasises that disinformation has a "corrosive influence across all spheres of life from public health to trust in democratic institutions" which makes it a "cross-policy issue" requiring co-ordinated action among many actors to ensure both effectiveness and the protection of fundamental rights. It also acknowledges that approaches to tackling disinformation may vary across countries, reflecting differences in the types and severity of threats. Norway's recent Strategy for Strengthening Resilience against Disinformation (2025-2030) is also a notable example.[21] Finally, Latvia's National Concept on Strategic Communication and Security of the Information Space 2023-2027, provides another example of a strategic framework for countering disinformation.[22]

Recommendation

Develop and implement a robust national strategy to counter disinformation and promote information integrity that sets the basis for a clear legal framework, long-term planning and co-ordination between public institutions and other actors such as media, academia, civil society organisations, private actors, including platforms. Prioritise:

- ✓ **Evidence-based approaches**: conduct research and launch initiatives to map key vulnerabilities and deeper structural problems – actors, geopolitical risks, media weaknesses, education gaps, divisions in society and susceptibility to manipulation.

- ✓ **Proactive and comprehensive approaches**: combine regulation, media and information literacy, and support for fact-checking.
- ✓ **Positive approaches**: prioritise education and capacity building over reactive legal restrictions.
- ✓ **Harmonisation of measures**: align national measures with European and international frameworks and standards to avoid a fragmented policy landscape.
- ✓ **Respect for human rights**: ensure that national strategies respect human rights and other relevant international standards, in particular those set by the Council of Europe.
- ✓ **Leveraging the experience of multiple institutions**: ensure close co-operation and co-ordination among governmental institutions as well as with non-governmental actors, the private sector and civil society to develop long-term, sustainable solutions.
- ✓ **Integrated approach**: mainstream actions related to countering disinformation and information integrity challenges in other relevant national strategies, such as those targeting discrimination and hate speech, especially when tackling identity-based disinformation.
- ✓ **Cross border and international dimensions**: integrate international co-operation and collaboration with other states and relevant actors as part of the national strategy to effectively address disinformation that transcends borders.
- ✓ **Appropriate funding and other resources**: allocate appropriate resources to effectively address disinformation while safeguarding the independence of non-state actors involved in these efforts; the long-term costs of information disorder far outweigh the benefits of investing in information resilience and integrity.

Pillars

Building block 2 – Enhance disinformation research and monitoring

Policymakers in member states often lack access to robust, timely and multidisciplinary research and data on disinformation, which could limit the effectiveness of national strategies and responses.[23] Despite growing global knowledge on disinformation, Europe still lacks sufficient context-specific research, in both academic inquiry and policy development, into how disinformation operates and how it actually impacts the formation of opinions and democratic processes.[24] Understanding and monitoring the spread of disinformation and its effects is fundamental for developing effective, evidence-based responses. While real-time monitoring can provide timely insights to guide short-term policy decisions, more in-depth and long-term research is needed to duly understand the root causes and nature of the associated threats as well as to identify sustainable solutions. In addition, disinformation is a complex, multidimensional phenomenon shaped by social, psychological, technological and geopolitical factors, making causality difficult to establish. Without robust, multidisciplinary and experimental research and monitoring, policies risk being misinformed, reactive, or even counterproductive. This challenge is often described as "misinformation about misinformation".[25] To stay ahead of evolving tactics and prevent further spread and impact of disinformation, research efforts must go beyond surface-level trends and support proactive, preventive and adaptive policymaking.

Research and monitoring should be conducted across both online and offline environments. In particular, it is important to keep in mind that the growing influence of social media and other platforms in shaping public opinion, as well as the ability to collect large-scale, granular data, makes the online space particularly valuable for advancing disinformation research and monitoring.[26] The online space provides unique opportunities to collect data about the volume, velocity and virality of false or misleading content, the network characteristics of disinformation spreaders, the reach and effectiveness of debunking efforts and how certain narratives gain traction and evolve.[27] The ever-changing and complex nature of digital platforms requires continuous monitoring, along with the capacity to test causal hypotheses about the impact of platform technologies on user behaviour. To ensure that findings are generalisable to real-world platform dynamics, researchers must be allowed to conduct experiments within platforms themselves.[28] Furthermore, there is significant untapped potential in enabling researchers to access data and findings from platforms' own experiments which could offer unique insights to develop targeted and effective solutions to the spread of disinformation.[29]

Council of Europe standards

- Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression stresses that effective policy on mis- and disinformation requires accurate, nuanced and comprehensive knowledge based on rigorous and independent research, including secure and privacy-compliant access to platform data for researchers. In implementing this Recommendation, states need to focus on:
    - ensuring that researchers can access data held by platforms in ways that are secure, legal and privacy-compliant;
    - the role of competent authorities to create secure environments that facilitate research;
    - accessing individual-level data available for independent research;

    - ensure that those granted access to individual data held by platforms have been subject to all necessary vetting procedures by independent institutions, aimed at ensuring that the approved researchers operate in an ethical framework to carry out significant research in the public interest and that they have the necessary expertise to process and protect such data;
    - liability; and data-sharing agreements between platforms and researchers.
- The Guidance note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner (2023, hereinafter "Guidance note on countering online mis- and disinformation") stresses the fundamental need for independent research on disinformation matters.
- The Venice Commission in its Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence (2024) emphasised the importance of sustained academic-industry partnerships to generate actionable insights, particularly in addressing challenges posed by generative Artificial Intelligence.
- The Draft Recommendation online safety and empowerment of users and content creators (approved by the CDMSI in December 2025 and to be considered for adoption by the Committee of Ministers in spring 2026) addresses the role of states in promoting and sustaining research on online platforms. Building on CM/Rec(2022)13, it emphasises both the need to allow independent researchers to be legally and technically allowed to access platform's data and to conduct experimental research on platform environments.

Promising practices

In the European Union's regulatory landscape, the Code of practice on disinformation[30] – now formalised as a Code of Conduct[31] under the EU Digital Services Act[32] – is one of the most advanced policy instruments aimed at improving knowledge and institutional responses to disinformation. A key innovation of the Code is the mandate to develop "structural indicators" that track the impact of policies and disinformation trends across platforms, providing a systematic and scalable framework for assessing the dynamics of disinformation.[33] This development lays the groundwork for long-term, evidence-based regulation and cross-country benchmarking. Article 40 of the Digital Services Act is the first legally binding EU provision granting researchers access to data from very large online platforms and search engines, under strict safeguards to protect privacy, confidentiality and platform security.[34] Though researchers must be based in an EU member state, or be under the jurisdiction of one of these, there are indirect or co-operative pathways through which researchers or institutions from Council of Europe member states outside the EU might benefit from this provision. Relevant research also needs to be supported on the national level. In Sweden, for example, the Psychological Defence Agency[35] promotes and disseminates relevant research, with the establishment of the Lund University Psychological Defence Research Institute in 2022 being one example of the Agency's work in this area.

Recommendation

Support research on disinformation and other priority risk areas and invest in the necessary capacities and resources to monitor the spread of harmful content at the national level. Prioritise:

✓ **Financial support**: provide financial support to university research programmes, civil society and other projects that aim to study the spread, prevalence and

characteristics, as well as the effects, of disinformation and other information disorders, with a focus on the relevant national context.

- ✓ **Experimental and longitudinal research frameworks**: support research that captures the evolving amplification mechanisms of disinformation, including algorithmic recommender systems and AI-generated content.
- ✓ **Appropriate legislation**: legally enable researchers, experts and the wider public to conduct research on online platforms, provided it is carried out in accordance with established principles of research integrity and ethics.
- ✓ **Capacity building**: empower independent public institutions, such as media regulators, national human rights institutions and ombudspersons, with the technological and methodological tools needed to monitor and analyse the spread of disinformation and other information disorders, as well as the impact of enabling measures.
- ✓ **Policy evaluation**: invest in systematic research to monitor and evaluate disinformation policies, assess their impact and ensure that responses are evidence-based, targeted and consistent with the rule of law and human rights standards; comprehensive evaluation frameworks should be used both *ex ante* and *ex post* to track measurable objectives, such as the reach of manipulative content, levels of public trust and behavioural outcomes, and to enable timely policy adjustments informed by empirical evidence.
- ✓ **Data access**: encourage technology providers to support researchers by granting access to relevant data, and empower authorities to facilitate this access, including to data already collected and analysed by online platforms over time.
- ✓ **Develop open and transparent metrics**: create and implement open and transparent metrics to monitor key aspects such as information diversity, algorithmic impacts and infrastructure resilience; these metrics should enable independent verification of how various systems influence the circulation of reliable versus manipulative content.
- ✓ **Introduce observability standards**: establish comprehensive observability standards including interoperable research APIs, audit protocols and shared taxonomies of manipulative content, to allow cross country comparability and co-ordinated response to emerging threats in the information ecosystem.
- ✓ **Partnership building**: foster the establishment of cross border dedicated strategic partnerships among universities and other research institutions to enhance collaborative research efforts, including to leverage access opportunities offered by existing legislative frameworks.
- ✓ **Be open and adaptive**: recognise that monitoring and research should encompass diverse topics – such as identity-based, climate, and health disinformation – and acknowledge that disinformation extends beyond the digital sphere.

Building block 3 – Strengthen media and information literacy and empower users

Many member states of the Council of Europe lack coherent and long-term media and information literacy (MIL) strategies.[36] While MIL alone cannot eliminate the harmful effects of disinformation on individuals and society, it remains key to empower individuals to critically assess sources, verify facts and recognise manipulative behaviours and narratives. The Media Literacy Index 2023 shows that many countries in Europe experience deficiencies in resilience to information challenges,[37] while surveys by Eurostat regularly find that the share of people without sufficient digital skills is still too high.[38] These insights are concerning, as a well-informed public is the best defence against disinformation and contributes to societal information resilience (see the Glossary).[39] Addressing this gap is complex and requires a broad and sustained approach. In particular, MIL is not simply the outcome of isolated interventions; it is deeply shaped by the overall quality of education – particularly in matters of digital literacy, digital citizenship, history and civic education – as well as by the levels of public trust in institutions and media.[40] Enhancing these interconnected fields demands long-term commitment and significant resources.

Moreover, the media and informational landscape is constantly evolving which means that disinformation tactics and technological tools are also always changing, requiring continuous learning rather than a one-time skill acquisition. Both experts and ordinary individuals must stay up to date to navigate this shifting environment effectively. Furthermore, MIL must extend beyond the basic ability to discern factual news from falsehoods. It should also prepare individuals to withstand the sophisticated tactics used by disinformation actors,[41] including the algorithmic and design-driven strategies that social media platforms deploy to capture attention.[42] Therefore, effective MIL programs need to draw on multiple educational disciplines, foster a diverse set of competencies and promote a deep understanding of human rights and responsibilities in the digital public sphere. This holistic approach requires co-ordinated efforts from actors at national, regional and local levels.

In addition, for MIL to become an effective tool against disinformation, the inequalities that leave vulnerable communities unprotected from online manipulation, particularly minorities, minors and the elderly, must be proactively addressed.[43] A strong political determination and appropriate capacity is also required to substantiate a meaningful right to receive information in the digital environment, which remains culturally, politically and technically challenging.[44] Embedding MIL within national education frameworks, with a particular emphasis on improving digital skills, is therefore crucial to fostering a more informed and resilient society.

Online content is increasingly shaped by opaque algorithmic systems that prioritise engagement and commercial interests over quality, user safety and the public good (see also below, Building block 6). Users of online services, particularly large platforms, have gradually lost control over their online experiences and the type and source of content they see and interact with. **Beyond being better equipped to critically engage with information, users should also benefit from digital environments that embed user empowerment by design**. Such environments would enable users to exercise their critical skills by granting them greater control over the lawful content they are exposed to – for example, by allowing them to flag unwanted material or report abusive behaviour, prioritise content from trusted information sources, or rely on third-party labelling to identify content that may pose a risk of disinformation. These tools should be integrated into platform design; however, in some

cases – such as alternative content curation that prioritises public interest content or information from trusted sources – they may also be developed and provided by third-party actors operating within existing platforms.

Council of Europe standards

- Recommendation CM/Rec(2022)11 on principles for media and communication governance identifies initiatives to strengthen MIL as key measures to mitigate the negative effects of disinformation and the lack of transparency in content dissemination. It further emphasises that implementing MIL measures serves as a means to empower users and promote the responsible use of media and online platforms.
- Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age attributes the media a critical role in collaborating with a range of other sectors to create and promote MIL initiatives to help citizens recognise and develop resilience to disinformation.
- The Parliamentary Assembly Resolution 2314 (2019) on media education in the new media environment calls on public service media organisations to teach children and teenagers how to spot disinformation and on internet intermediaries to actively co-operate with public, social and private entities to promote and support MIL, notably to counter disinformation.
- The Guidance note on countering online mis- and disinformation (2023) stresses the need for comprehensive MIL strategies (para. 40) and long-term reform of educational curricula (para. 41). It also addresses the issue of online user empowerment, by recommending measures that promote user rights (para. 35) and for the development of digital tools for user empowerment (para. 39).
- The Draft Recommendation on online safety and empowerment of users and content creators (approved by the CDMSI in December 2025 and to be considered for adoption by the Committee of Ministers in spring 2026), singles out a comprehensive set of measures that platforms could be required to take under domestic legal frameworks in order to empower users, gain control of their online experience, including to mitigate the risks to information integrity and pluralism.
- The policy document on National MIL strategies. Practical steps and indicators (2025), emphasise that effective national strategies on MIL should also focus on countering disinformation and strengthening information integrity. It also provides a comprehensive list of relevant Council of Europe MIL standards and other materials.

Promising practices

In Switzerland political and digital education are included in all curricula for compulsory education and the framework curricula for upper secondary education.[45] Similarly, Finland's emphasis on lifelong learning provides an inclusive model for engaging citizens of all ages in MIL initiatives. Furthermore, in Ukraine, specific MIL training targeting media professionals have been instrumental to support independent newsrooms in times of digital transformation and informational threats. However, education and access to information are not enough. In certain critical moments, such as crises when disinformation poses heightened risks, citizens require timely and authoritative information. To address this, some countries have implemented targeted governmental campaigns designed to quickly counter misleading narratives. For example, governmental information campaigns were launched during the COVID-19 pandemic to provide trustworthy information in a moment of high public vulnerability.

Recommendation

Adopt a comprehensive, multidimensional strategy to strengthen MIL, in line with the policy document on *National Media and Information Literacy Strategies*; develop and enforce regulatory and co-regulatory frameworks to empower users in shaping their online informational environment. Prioritise:

- ✓ **Formal education**: incorporate MIL in formal education curricula – ideally in a multidisciplinary manner, encouraging interaction and connecting with students' real life experiences. MIL education should also engage with aspects of information integrity, equipping learners with the skills to identify trustworthy sources and evaluate content critically.
- ✓ **Non-formal education and lifelong learning**: extend MIL initiatives beyond the school system through a lifelong learning approach that reaches all segments of society, including senior citizens and communities at risk of marginalisation.
- ✓ **Cross-sector co-operation**: ensure close co-operation with civil society, public service and private media organisations, national regulatory authorities and providers of formal and non-formal education.
- ✓ **Financing MIL**: ensure adequate funding for both private and public MIL activities.
- ✓ **Training of educators**: empower MIL educators through access to high-quality training, up-to-date resources and robust support systems so they can effectively guide learners in critically engaging with content both on and offline.
- ✓ **Digital learning**: invest in and support MIL digital learning platforms and open educational tools – such as interactive tutorials and adaptive modules – to promote lifelong learning and continuous capacity building across all age groups.
- ✓ **User empowerment**: adopt measures requiring online platforms to empower users with better access to trustworthy content, greater agency over the content they see, enhanced options for reporting harmful content and increased control over their social media feeds; promote and support the work of trusted flaggers, civil society organisations and other qualified experts to identify and report harmful content online.

Building block 4 – Support quality journalism and foster media resilience

Independent, quality media are essential to a healthy democracy and to safeguarding information integrity. By providing accurate, verified and contextualised information, journalism enables individuals to engage in public debate, make informed choices and resist manipulation and disinformation. However, quality journalism across Europe faces increasing structural challenges, including financial instability, political and economic pressure, limited resources and insufficient safeguards for editorial independence and professional standards. Since the late 1990s, the traditional business model of journalism has been undermined by the rise of the internet and the spread of free online content, which eroded advertising revenues that once subsidised affordable access to news.[46] Today, much of this revenue has shifted to digital intermediaries such as search engines and social media platforms that dominate the flow of information without producing original content.[47] As a result, many outlets struggle to sustain quality reporting, entering a cycle where reduced resources weaken journalism, erode public trust and further limit financial viability.[48]

Financial vulnerability and weakened institutional safeguards have also made media more susceptible to capture,[49] where powerful political or commercial interests exert influence over editorial decisions. Local outlets are particularly at risk, leading to news deserts in many regions where coverage of community issues has disappeared.[50] Even public service media, traditionally more stable, face budget cuts and political interference,[51] while journalists across Europe continue to encounter harassment, physical attacks and abusive lawsuits. At the same time, rapid advances in generative artificial intelligence, including conversational bots and AI-generated news summaries, are reshaping how audiences access and consume information, adding new complexities to an already fragile media environment.[52]

The rise of disinformation online has further highlighted the importance of independent media in maintaining information integrity. **Fact-checking** – once an invisible newsroom practice of responsible journalism – **has emerged as a new practice and profession with an increasingly important role in the modern information landscape**, serving as a powerful toolbox in countering the dissemination of misleading narratives and false claims, with the aim to enhance trust in news and public communication. Parallel efforts to improve the discoverability of quality journalism, through measures such as prioritising public interest content and developing trustworthiness indicators, have gained focus.[53] However, these measures must be carefully implemented to protect freedom of expression and individual choice. Clear safeguards, such as transparency requirements, robust standards, independent oversight and respect for journalistic copyright, are vital to supporting media freedom, pluralism and sustainability, while countering disinformation. Ensuring that digital platforms and AI technologies uphold these principles is also central to preserving public trust in news and strengthening the democratic role of quality journalism.

Council of Europe standards

- Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age encourages states to take proactive measures to promote quality journalism as a public good, including through financial and other forms of direct support to media actors, whether public, private, community-based, or local. It also addresses measures aimed at rebuilding and maintaining trust in quality journalism.
- Recommendation CM/Rec(2018)1 on media pluralism and transparency of media ownership calls for structural measures to promote both diversity among media sources and outlets. This includes ensuring adequate conditions for public service media to maintain its vital role in fostering public debate and political pluralism, as well as implementing strategies and mechanisms to support professional news organisations and high-quality independent and investigative journalism.
- Recommendation CM/Rec(2016)4 on the protection of journalism and safety of journalists and other media actors provides specific guidelines to member states in this area. It is complemented by Recommendation CM/Rec(2024)2 on countering the use of strategic lawsuits against public participation (SLAPPs) that provides detailed guidance of how to effectively protect journalists from abusive lawsuits. The Council of Europe Campaign for the Safety of Journalists and Platform to promote the protection of journalism and safety of journalists support the implementation of these recommendations.
- The Guidance note on the prioritisation of public interest content online (2021) recommends states to take action to make public interest content more prominent on online platforms and intermediaries.
- The Guidance note on countering online mis- and disinformation (2023) provides concrete recommendations on how to better foster independent fact-checking.
- The Guidelines on the responsible implementation of artificial intelligence (AI) systems in journalism (2023) provide practical guidance to news media organisations, but also states, technology providers and digital platforms, on how AI systems should be used to support the production of quality and responsible journalism.

Promising practices

Several member states have in place support schemes for news media, which often extend to online and non-traditional media as well. However, additional measures are needed to ensure that such funds are both sufficient and fairly distributed. In Romania, taxpayers can redirect 3.5% of their income tax to non-profit organisations – including news media that are registered as non-profits.[54] In Croatia, the Agency for Electronic Media issued public calls for activities and projects, including those related to fact-checking, through the tender on the "Establishment of verification of media facts and public data disclosure systems", which is part of the National Recovery and Resilience Plan.[55] In Italy, the state supports the news media publishing sector, including a wide range of outlets such as local, national, digital or printed, newspapers and periodicals. The criteria for accessing these funds are aimed at raising the standards of quality and reliability of information, promoting technological innovation, valuing the human capital of journalists and fostering a more sustainable and diverse media landscape.[56]

The European Fact-Checking Standards Network, which brings together fact-checking organisations across Europe, provides a good example of developing and enforcing high journalistic standards in fact-checking, as well as fostering co-operation across countries. Projects like the Journalism Trust Initiative[57] and NewsGuard[58] developed indicators that can determine to what extent news media outlets follow the rules of good journalistic practice,

thereby supporting audiences in assessing the trustworthiness of content. The Global Media Identifier[59] standard, meanwhile, aims to verify the identities of media publishers across platforms, an important step toward strengthening transparency and accountability in journalism.

Recommendation

Protect journalists and support the production of quality independent and pluralist journalism and foster its prominence. Prioritise:

- ✓ **Strong independent and pluralist public service media**: ensure that public service media are independent in law and practice, pluralistic, as well as adequately staffed and resourced to effectively fulfil their public-interest mandate in the digital age.
- ✓ **Support for quality media and journalism**: encourage and support quality journalism, including investigative journalism and not-for-profit community media, among other things through subsidies, financial and fiscal measures; provide citizens with vouchers or tax reliefs for expenditures in media; ensure that the state funding and advertising is transparent and non-discriminatory; foster the existence and effective implementation of safeguards for editorial independence and professional standards for all media actors.
- ✓ **Increased transparency**: enact and enforce robust legal frameworks on transparency of media ownership ensuring that information, including beneficial ownership, is collected and is publicly available; promote voluntary transparency of funding within self-regulation.
- ✓ **Prominence of public interest and trustworthy content**: ensure that online platforms do not impose unfair conditions in the digital media market and promote proportionate prominence mechanisms so that quality journalism reaches wider audiences; use established standards and media identifiers to help recognise trustworthy content and guide decisions on visibility.
- ✓ **Strong self-regulation**: support the development of ethical codes and self-regulatory regimes for all media actors, including codes related to the use of AI in journalism and for journalism, in accordance with the Guidelines on the responsible implementation of AI systems in journalism.
- ✓ **Support fact-checking**: empower independent fact-checking organisations in accordance with the Guidance note on countering online mis- and disinformation.
- ✓ **Protection of journalists**: protect journalists from intimidation, pressure and attacks and interferences, including physical violence and harassment and SLAPPs; refrain from using such measures against domestic and foreign journalists, both in times of peace and war; promote fair working conditions for journalists.

Building block 5 – Safeguard the integrity of elections

The effects of disinformation on electoral processes are a growing concern across Council of Europe member states. Attempts at influencing electoral processes through disinformation campaigns, often in the context of **foreign information manipulation and interference (FIMI) operations** have been widely documented.[60] The Parliamentary Assembly of the Council of Europe has clearly indicated that foreign interference constitutes a threat to democratic security in Europe and, in this context, it has condemned the escalation of hostile interference, including through disinformation and propaganda, particularly originating from the Russian Federation.[61]

While this phenomenon affects the media landscape, online **platforms and new technologies enable new and more impactful** avenues for malign actors to propagate false or misleading narratives and to manipulate public information with a rapidity and breadth not previously possible,[62] including through the sophisticated targeting of manipulative political communication and advertising.

As electoral coverage and advertising is generally relatively well-regulated and safeguarded in print and broadcast media, there is a concerning lack of oversight and regulation in the digital environment, especially on social media.[63] As such, **often neither politicians, nor other interest groups are bound to follow clear rules or to be sufficiently transparent on their online spending and their tactics**.

In addition, other emerging technologies pose growing threats to election integrity. For example, AI enables malicious actors to deceive audiences more effectively, while targeting and microtargeting makes it possible to provide individuals and different demographic groups with tailor-made messaging.[64] Disinformation campaigns and malign foreign actors frequently use these opportunities.[65] The EU's European External Action Service (EEAS) has identified signs of AI-aided foreign information attacks in the electoral processes of several Council of Europe member states,[66] underscoring that information manipulation remains a serious and ongoing threat. As technology evolves rapidly, these challenges will likely continue to change, requiring policymakers to adapt constantly.

Council of Europe standards

- In *Bradshaw and others v. the United Kingdom* (2025), the European Court of Human Rights addressed states' obligations under Article 3 of Protocol No. 1 to the Convention (right to free elections) on countering systematic large-scale foreign interference in elections. Recognising that disinformation may pose a serious threat to electoral integrity, it held that, where hostile foreign interference creates a real risk of undermining the very essence of the right to vote, states may be under a positive obligation to adopt and regularly review appropriate measures (para. 136), including investigating credible allegations of electoral interference when failure to do so may impedes its ability to take such measures (para. 138). While the difficulty of assessing foreign influence should not prevent states from acting to defend democracy, there is a lack of clear consensus on the specific measures that states should take (para. 159), within the limits of respect for freedom of expression (para. 160-161). Therefore, States enjoy a wide margin of appreciation in the choice of means to be adopted to counter credible threats to their democratic processes (para. 162).
- Recommendation CM/Rec(2022)12 on electoral communication and media coverage of election campaigns provides a comprehensive framework to safeguard fairness, transparency and integrity in electoral communication in the digital age. It calls for co-regulatory governance and strengthened oversight bodies, clear rules for online political

advertising, as well as detailed transparency obligations for parties, candidates, service providers and platforms. It promotes algorithmic accountability, measures to counter manipulation and disinformation and strong privacy protections.

- Recommendation CM/Rec(2007)15 on measures concerning media coverage of election campaigns provides a set of general principles to ensure the fairness of media coverage of elections and specific measures concerning broadcast media; it calls on member states to respect and uphold the independence of media in election periods.
- Parliamentary Assembly Resolution 2593 (2025) on Foreign interference: a threat to democratic security in Europe highlights the significant threat posed by foreign interference to democratic security in Europe. It condemns such interference, particularly from the Russian Federation, noting efforts to manipulate political campaigns, elections and referendums across the continent. The resolution urges member states to secure democratic institutions, enhance co-ordination to counter these threats and strengthen legal frameworks to address foreign interference.
- Parliamentary Assembly Resolution 2254 (2019) on Media freedom as a condition for democratic elections highlights the growing threat posed by disinformation and foreign interference to democratic processes. It urges governments to recognise the transnational nature of these challenges, strengthen co-operation with internet intermediaries, ensure that voters have access to trustworthy information and address the concentration of informational power in major technology companies.
- The Urgent Report on the cancellation of election results by Constitutional Courts (2025), of the Venice Commission examined the conditions under which a constitutional court may annul election results, following the cancellation by the Romanian Constitutional Court of the 2024 presidential election due to findings of digital manipulation and opaque campaign financing (paras. 80-82). It stressed that external influence, whether from foreign actors, NGOs or media, can be as damaging as the violation of election rules, though its impact is harder to measure. It highlighted major challenges posed by online campaigning, AI and disinformation, calling for clearer rules on campaign messaging, transparency and finance, and emphasised the need for robust procedural safeguards and well-reasoned, evidence-based decisions in any annulment process.
- In the Interpretative declaration of the Code of good practice in electoral matters as concerns digital technologies and artificial intelligence (2024), the Venice Commission emphasised that the freedom of voters to form an opinion includes the right to have access to all kinds of information enabling them to be correctly informed before making a decision, which can be affected by online information disorders.

Promising practices

Several Council of Europe member states have developed good practices that seek to find an appropriate balance between safeguarding electoral integrity and protecting the wide freedom of expression that is inherent to political debate and campaigning. In France, the *2018 Law on the fight against manipulation of information* addresses the dissemination of deliberately misleading information, with particular focus on online media and digital platforms. The law imposes transparency and co-operation obligations on platforms under the oversight of the audiovisual regulatory authority (Autorité de Régulation de la Communication Audiovisuelle et Numérique, ARCOM). It aims to enhance transparency regarding the financing, distribution and promotion of online content, address propaganda from foreign state-funded broadcasters and strengthen media and information literacy. The law also establishes a fast-track civil procedure for the three months preceding key elections and referenda, whereby a judge may order the removal, within 48 hours of reporting, of content that is manifestly false, intentionally and widely disseminated through artificial or automated means, where such content could cause public disturbance or compromise the

integrity of elections.[67] Likewise, in Ireland, the 2022 Electoral Act has been passed with the stated aim of "protect[ing] the integrity of [its] … electoral and democratic processes against the spread of disinformation and misinformation in the online sphere during electoral periods".[68]

Recommendation

Strengthen the governance of election integrity in the digital age by setting clear rules for fair, transparent and balanced campaigning and establishing co-regulatory frameworks for online political advertising and campaigning, with stricter oversight of large platforms. Prioritise:

- ✓ **An independent mechanism of democratic oversight**: Provide independent electoral authorities, or other relevant national networks and bodies, with the powers, resources and tools necessary to fulfil their mandates effectively—including the ability to impose sanctions and to ensure neutral platform content curation and moderation—supported by multistakeholder advisory bodies.
- ✓ **Regulation of online political advertising**: Introduce clear rules on political advertising, particularly when it takes place online, including spending limits, requirements governing microtargeting, the use of artificial intelligence and full transparency regarding the sources and scale of funding. Provide effective and proportionate sanctions for violations. Key measures should include mandatory labelling and the creation of public archives.
- ✓ **Monitoring and countering disinformation**: Independent authorities in the electoral field should monitor disinformation campaigns prior to elections and pro-actively counter messages and activities that threaten the integrity of elections; they should develop tools to assess platforms' ability to detect political ads, as well as inauthentic co-ordinated behaviour.
- ✓ **Information campaigns**: Ensure that citizens have easy access to all relevant official information about the election process and the key electoral topics. Such information should be proactively disseminated through media and relevant online platforms, including social media, with targeted outreach at national, regional and local levels.
- ✓ **Ethical codes of political campaigns**: Ensure that political parties and candidates adopt and abide by ethical codes on campaign communications, ensuring that their messaging is proactive, transparent and accessible to the electorate and do not use microtargeting in ways that mislead or manipulate the electorate.

Building block 6 – Promote competition and accountability in the digital ecosystem

Council of Europe member states have a dependency on non-European digital infrastructures, limiting their capacity to ensure media pluralism, human rights compliance and democratic control over the information ecosystem. Research shows that Europe faces an infrastructural gap, with most of its digital technologies being imported.[69] The current dependency on a handful of non-European dominant tech companies weakens the capacity of Europe to control the digital infrastructure and, by extension, its information ecosystem. In particular, large online platforms, which play a central role in shaping public opinion and influencing the rights of users, creators, influencers and businesses, are still not fully aligned with the expectations deriving from the Council of Europe values and standards on protecting human rights and fundamental freedoms, democracy and the rule of law in the media and communication environment.[70] Despite efforts to regulate the digital space with ambitious frameworks, their influence continues to be a subtle yet pervasive force. They increasingly exercise a form of privatised governance through the terms and conditions they impose on users, creating a contractual relationship marked by structural information asymmetries where platforms are in a significantly better position than users.[71] Due to their dominant positions and network effects, the large online platforms undermine consumer choice.[72] Moreover, platforms' business models that prioritise user engagement and assume that controversial content generates more user activity gives prominence to low quality and potentially harmful content.[73] These challenges remain largely unaddressed by current regulations.[74] In parallel, fostering competition faces substantial hurdles,[75] including regulatory fragmentation, bureaucratic complexity and limited ability to attract talent. This highlights the need for deep and structural interventions.

A key strategy is to make it easier for people to switch between platforms by promoting interoperability, allowing different services to work together and supporting a greater variety of digital infrastructures. A paradigm shift is being advocated through the rise of what is referred to as "Open Network Economy": a decentralised, interoperable system where users can build their own digital experience rather than relying on what a few dominant platforms offer.[76] This approach also supports "algorithmic pluralism," meaning that users could choose between different algorithms to shape how information is shown to them.[77]

In addition, Council of Europe member states should promote new ways of managing data to reduce power imbalances. These include data trusts (independent bodies that manage data for people), data cooperatives (member-run groups that oversee shared data) and data unions (groups that allow users to negotiate collectively over the use and value of their data).[78]

By encouraging open-source, interoperable and alternative digital infrastructures, Council of Europe member states, as appropriate, can decrease reliance on a few dominant companies and create a fairer competition environment. Building and maintaining its own digital infrastructure would not only secure essential services but also help protect information integrity. A diverse digital ecosystem that reflects the values of the Council of Europe will be crucial for ensuring both security and trustworthy information in the digital age.

Council of Europe standards

- Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age invites member states to introduce frameworks that ensure "the fair treatment of content producers and the media by online platforms". Moreover, member states should create enabling conditions for open-source solutions, access to training data, open data approaches and to ensure competition among technology providers, including European and specialised start-ups, while respecting the rights of others.
- Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries calls online platforms to respect individuals' right to access information and ideas.
- The Guidelines on the responsible implementation of artificial intelligence (AI) systems in journalism (2023) emphasise that member states have a positive obligation to protect and create favourable conditions for the realisation of human rights and media pluralism. They should foster access and choice between technology providers that respect and promote the realisation of journalistic values and human rights. To this end, there is a need for the diversification of funding schemes to support short- and long-term projects on the development of responsible journalistic AI systems, as well as, more broadly, alternative digital tools and communication infrastructures, particularly for smaller and local media organisations.

Promising practices

At the infrastructure level, holistic and scalable solutions are still lacking at the European level, while several promising initiatives are emerging. One of the most significant is EuroStack,[79] a recent initiative – mainly targeting the European Union and its member states – that sets out a comprehensive plan for achieving "European digital sovereignty". EuroStack aims to rebuild Europe's technological independence by connecting all the essential layers of the digital ecosystem – ranging from raw materials and semiconductor production to cloud services, AI, networks and cybersecurity – into one co-ordinated and competitive system. By recognising how tightly these layers depend on one another, the EuroStack vision is to give Europe strategic control over its entire technological backbone. To support this goal, states should assess how their industries and research sectors can contribute to building such an integrated ecosystem.

Recommendation

Support the promotion and development of a digital infrastructure that serves the public interest by upholding human rights and environmental standards, using open-source technologies where possible, empowering users, effectively competing with dominant global platforms and delivering clear economic, social and user benefits. Prioritise:

- ✓ **Interoperability**: adopt regulation that require online platforms to be interoperable, thereby enabling users to freely move between services and easily transfer their data, contacts and settings, which is essential for ensuring genuine user choice and fostering a competitive market; explore options for allowing users of large platforms to choose tools for content recommendation and moderation developed by third parties; ensure that interoperability fully complies with international standards and domestic legal frameworks on data protection and user privacy.

- ✓ **Resilience-oriented infrastructure**: promote infrastructure planning and design focused on resilience, encouraging the development and adoption of decentralised and open-source alternatives where appropriate.
- ✓ **Start-up capital**: Consider providing targeted financial support to new platforms based in Council of Europe member states, independent public–private partnerships and existing social media services that commit to interoperability, recognising the potential strategic importance of a local digital ecosystem; this support could take the form of competitive grants awarded to companies that demonstrate transparency, respect for human rights and active promotion of interoperability, with the programme potentially funded, in part, by fines imposed on companies that fail to comply with relevant regulations.
- ✓ **Invest**: consider investing in independent infrastructure for artificial intelligence, encompassing cloud and computing resources, to reinforce resilience and competitiveness and to promote open, safe, sustainable and human-rights-respecting AI.
- ✓ **Responsible and value-based technology**: Establish frameworks to ensure that digital infrastructures and services, including cloud and artificial intelligence systems, are designed and operated in a transparent, responsible and value-based way, respecting human rights and limiting environmental degradation; open-source technologies should be supported.

Foundational principles

Building block 7 – Uphold freedom of expression

The protection of democracy and of the right to receive information require states to address the challenges of disinformation. However, responses to disinformation may involve **measures that restrict freedom of expression**, such as sanctioning individuals or media outlets, or requiring online service providers to limit the visibility or accessibility of certain types of content. In such cases, strict compliance with Article 10 of the European Convention on Human Rights is essential. As the European Court of Human Rights has cautioned, *"*there is a very fine line between addressing the dangers of disinformation and outright censorship*".*[80]

Narratives that may pose risks to information integrity or democratic processes, presented as alternative to mainstream viewpoints, often concern questions of public interest and form part of political discourse. Accordingly, the margin for justifying restrictions solely on the grounds that content may contribute to information disorder is necessarily narrow.[81]

A non-exhaustive survey of legal frameworks in Council of Europe member states[82] shows that the dissemination of false or misleading information may be criminally relevant where it is linked to other offences,[83] while in some jurisdictions broader provisions criminalise the dissemination of false information as such, where it is intended, or has the effect, to disturb public order or provoke social alarm.[84] However, **relying on criminal law to counter disinformation carries significant risks: prosecutions may be misused**, particularly where offences are vaguely defined or lack adequate safeguards. Such an approach has been widely criticised and may be incompatible with international human rights standards.[85]

The enforcement of **rules for audiovisual media services**, such as statutory duties concerning accuracy, objectivity and pluralism of information, as well as restrictions on harmful content, may apply to disinformation. Most audiovisual regulators, however, lack a direct mandate to address disinformation *per se*, with the Republic of Moldova being an exception.[86] Specific measures affecting media actors have been adopted in the context of sanctions regimes targeting the Russian Federation, both by the EU[87] and individual Council of Europe member states.[88]

Disinformation disseminated through digital platforms is addressed through a dual regulatory approach. When content is restricted by the law, it is subject to removal orders or notice-and-action mechanisms, in which platform liability arises only where they fail to act expeditiously upon knowledge of the illegal content concerned. In addition, systemic risks arising from platform design are increasingly addressed through platform accountability frameworks that place platforms' risk management processes under public oversight. In this context, risks for information integrity are primarily addressed through measures concerning the dissemination of illegal content.[89] In certain cases, notably under the Digital Services Act, very large online platforms and search engines must also assess and mitigate risks from content that, while lawful, may harm civic discourse, as well as risks linked to intentional manipulation of their services, including inauthentic or automated activity.[90]

Measures restricting content on grounds of alleged falsehood carry clear risks for freedom of expression, including freedom and editorial independence of media. Such interventions may fuel conspiracy narratives and claims of victimisation by disinformation actors, deepening

polarisation and eroding trust in democratic institutions.[91] Overly strict or vaguely framed rules can be misused to suppress minority views or legitimate criticism, thus having a chilling effect. Likewise, insufficient accountability and public oversight of content curation and moderation can lead to under- or over-enforcement, as well as discriminatory or arbitrary practices by private actors that undermine the integrity of the information environment.

These considerations suggest the **need to prioritise resilience-building measures that counter disinformation without unduly interfering with freedom of expression**.[92] Effective **self-regulatory and co-regulatory mechanisms** for professional communicators, including journalists and advertisers, but also new media actors, such as citizen journalists and influencers, can also support information integrity and pre-empt state interference with media freedom.

Council of Europe Standards

- In *Bradshaw and others v. the United Kingdom* (2025), the European Court of Human Rights recognised that states may have positive obligations to counter disinformation, in particular in the context of foreign election interference. However, it has emphasised the need to balance them against the right to freedom of expression under Article 10 of the Convention (para. 160-161). Similarly, the case of *Google LLC and Others v. Russia* (2025), shows how regulation of online platforms that require excessive moderation also impacts on their Article 10 rights and the need to design and apply legislative interventions within the limits of its paragraph 2.

  According to Article 10 of the Convention, as interpreted by the case-law of the Court, restrictions to freedom of expression must have a proper legal basis that is accessible and foreseeable: they must be formulated with sufficient precision to enable a person to regulate their conduct. Criminal law provisions must clearly and precisely define the scope of relevant offences, in order to avoid excessive state's discretion to prosecute potentially leading to abuse through selective enforcement (*Savva Terentyev v. Russia*, 2018, para 85; *Altuğ Taner Akçam v. Turkey*, 2011, paras 93-94). Predictability is particularly important in an electoral context (*Magyar Kétfarkú Kutya Párt v. Hungary* [GC], 2020, para. 99).

  Restrictions must genuinely pursue one of the legitimate aims listed in paragraph 2 (*Bielau v. Austria*, 2024, para. 30, protection of health; *Salov v. Ukraine*, 2005, para. 113, the free formation of political opinion of voters - rights of others; *Gaponenko v. Latvia*, 2023, para. 41, the prevention of disorder or crime). Exceptions to freedom of expression must be construed strictly and the need for restrictions must be established convincingly (*Magyar Helsinki Bizottság v. Hungary* [GC], 2016, para. 187). In particular, Article 10 affords a high level of protection to political speech and debates matters of public interest (*Sürek v. Turkey (no. 1)* [GC], 1999, para. 61), especially in the context of elections.

  In this context, statements of fact must be distinguished from the expression of value judgments, the truthfulness of which is not susceptible of proof. In drawing such distinction and assessing whether an opinion has sufficient factual basis, the context is essential (*Mortensen v. Denmark*, 2025, paras 40-42).

  The falsity of a statement of fact does not in itself justify restrictions, especially in the form of criminal or other sanctions to individuals that disseminate them (*Salov v. Ukraine*, 2005, para. 113). The intention to cause harm to a protected interest (*Salov v. Ukraine*, 2005, para. 113) the concrete capacity to do so (*Avagyan v. Russia*, 2025, para. 35) must be shown as part of the necessity and proportionality test. In this context, the status of the person making the statements, including any associated professional obligations to provide accurate information, may have some relevance (*Bielau v. Austria*, 2024, concerning a medical doctor who had categorically denied vaccine benefits, contradicting medical consensus). While "public watchdogs", and particularly the press, enjoy increased protection, provided that they comply with the duties and responsibilities connected with the function of journalist and the consequent obligation of "responsible journalism" (see Guide on Article 10, 2025, para. 318 ss.).

- Recommendation CM/Rec(2022)11 on principles for media and communication governance stresses the need for promoting human rights and fundamental freedoms in communication (Principle 6); the Explanatory Memorandum further articulates this principle, by stressing the limits faced by states, the importance of aligned rules for offline and online environments, as well as the need for self-regulation, subject to public oversight when appropriate. It also stresses the need for a graduated approach and proportionality in the regulation of duties and responsibilities of different types of media actors.
- Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression is designed to assist states and relevant private actors in their independent and collaborative efforts to protect and promote freedom of expression in the digital age. The Guidelines appended to the Recommendation formulate principles aimed at ensuring that digital technologies serve rather than curtail such freedom and provide recommendations on how to address the adverse impacts and enhance the positive implications of the widespread use of digital technologies on freedom of expression in human rights compliant ways.
- The Guidance note on countering online mis- and disinformation (2023), indicates that co-regulatory frameworks for platform accountability should focus on the governance of content prioritisation and moderation processes rather than on individual items of content, ensuring that restrictions, whether grounded in law or in contractual terms, are compatible with freedom of expression and applied in a consistent, non-discriminatory and transparent manner.
- The Draft Recommendation on online safety and empowerment of users and content creators (approved by the CDMSI in December 2025 and to be considered for adoption by the Committee of Ministers in spring 2026) provides a comprehensive set of principles to promote an approach to the management of online risks related to freedom of expression, including in relation to information integrity.
- The Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe Urgent joint opinion on the draft amendments to the Penal Code regarding the provision on “false or misleading information” in Türkiye, concluded that it did not conform to the requirements of Article 10.2 of the Convention. It found that it lacked the required clarity and precision. Moreover, it was not necessary in a democratic society, since it did not respond to a pressing social need, nor was proportionate. While recognising that information disorder poses serious challenges, the Opinion warns about the need to limit the use of criminal provisions in this area, giving the chilling effect that they may have and the risk of abuse.
- Parliamentary Assembly's Resolution 2590 (2025) on Regulating content moderation on social media to safeguard freedom of expression emphasises the need for balanced content moderation on social media to protect freedom of expression while addressing the challenges posed by harmful content. It calls for member states to establish clear regulations that safeguard user’s rights, ensure fair working conditions for human moderators and promote independent dispute resolution mechanisms. Additionally, it urges social media platforms to incorporate fundamental rights into their policies, provide clear communication regarding content moderation actions and collaborate with journalists and fact-checkers to combat disinformation effectively.
- Parliamentary Assembly Resolution 2567 (2024) on propaganda and freedom of information in Europe emphasises the need for member states to combat illegal propaganda while respecting freedom of expression and the rule of law. It calls for comprehensive strategies to address both illegal and legal propaganda, highlighting the importance of independent media, public trust and collaboration between public authorities and the private sector. It urges States to implement targeted sanctions against specific propagandists and to promote media literacy, transparency and quality journalism.

Promising practices

Faced with exceptional exposure to Russian propaganda and interference after the full-scale invasion of Ukraine, the Republic of Moldova has confronted the challenge of taking appropriate measures to safeguard its democratic security and the integrity of the information space, while upholding human rights and the rule of law. Mindful of the implications of such measures for fundamental rights, in particular freedom of expression, it has submitted notifications of derogation under Article 15 of the European Convention on Human Rights, thereby subjecting its actions to transparent scrutiny. At the same time, it has consistently sought co-operation and expert advice from international organisations and partners, including the Council of Europe, to strengthen human rights compliance. Legislative reforms affecting the media have, in particular, been submitted to the Venice Commission for opinion.[93] Meanwhile, the Audiovisual Council, as the competent regulatory authority for disinformation-related provisions of the Audiovisual Media Services Code, has developed with the assistance of international experts in a Council of Europe co-operation project, a methodology for assessing cases of disinformation in accordance with legal requirements and within the limits of Article 10. While areas for improvement may remain,[94] this shows how concerns relating to the respect of freedom of expression in the fight against disinformation may be embedded from the outset in law- policy-making process.

Recommendation

While prioritising measures that do not interfere with freedom of expression, when adopting legislative or other measures to counter disinformation and safeguard information integrity: ensure that any restriction to the rights protected by Article 10 comply with its paragraph 2, and is applied within a rule-of-law framework; and promote independent public oversight of measures taken by platforms to address risks to information integrity and their impact on freedom of expression. Prioritise:

- ✓ **A bill of digital rights**: consider establishing a bill of human rights in the digital environment that upholds, among others the right to freedom of expression, including in the context of measures addressing disinformation.
- ✓ **Regulatory and human rights impact assessments**: constantly assess the adequacy and impact of legislative and regulatory measures potentially affecting the free flow of information in society, to better understand or prevent any potential negative impact – direct or indirect – on freedom of expression and other human rights, including issues of gender equality.
- ✓ **Respect of Article 10 of the Convention**: ensure that any measure to counter disinformation or safeguard information integrity that interferes with freedom of expression complies with the requirements of:
  - **legality and legal certainty** – any content or behaviour that is subject to restrictions is clearly defined by the law, ensuring foreseeability, predictability and protection against arbitrariness;
  - **legitimate aim** – measures genuinely pursue one or more aims listed in Article 10, paragraph 2 of the Convention;
  - **necessity and proportionality** – restrictions are limited to what is necessary in a democratic society and proportionate to the legitimate aim pursued; competent authorities should be able, when appropriate, to assess proportionality in

individual cases, with particular regard to the need of safeguarding freedom of media and the press.

- ✓ **Restraint in the use of criminal law**: reserve criminal sanctions, where used at all, for the most harmful forms of disinformation that pose clear and serious risks to the rights of others or to a protected public interest, in line with the Convention and related case-law and as provided by applicable international instruments.
- ✓ **Adequate and proportionate regulatory and co-regulatory frameworks** for internet intermediaries and platforms:
  - refrain from imposing disproportionate liability on intermediaries for user-generated content and avoid excessive moderation obligations that may lead to over-removal of lawful material;
  - clearly distinguish between responses to the dissemination of illegal or otherwise regulated content and those relating to lawful content; states should not directly or indirectly require platforms to restrict access to specific pieces of lawful material;
  - ensure independent public oversight of design solutions adopted by platforms, as identified in the Guidance note on countering online mis- and disinformation, to address systemic risks to information integrity;
  - support accessible, transparent, timely and effective alternative dispute resolution mechanisms, such as social media councils or out-of-court settlement bodies, for users affected by platforms' content moderation decisions.
- ✓ **Rule of law essential safeguards:**
  - **Independence and impartiality** – ensure that judicial, regulatory and other authorities responsible for enforcing restrictions on freedom of expression to counter disinformation or maintain information integrity operate independently and impartially in law and practice;
  - **Access to an effective remedy** – ensure that any natural or legal person whose freedom of expression is affected by decisions of public authorities or intermediaries have access to judicial or otherwise effective remedies consistent with Articles 6 and 13 of the Convention;
- ✓ **Strengthened professional communication standards**: strengthen and promote self- and co-regulatory frameworks for professional communicators, taking account of new communication tactics and technologies – including the growing use of AI – and the expanding range of actors able to reach large audiences, including journalists, advertisers, influencers, citizen journalists and other new media actors.

Building block 8 – Facilitate international and cross border co-operation

Disinformation is a border-crossing phenomenon that no member state can effectively tackle alone. In today's digital age, misleading content and narratives can easily spread across borders, particularly where linguistic, cultural, or historical ties exist – creating a significant spillover effect in the spread of disinformation. Moreover, malign content creators, familiar with multiple cultural contexts, can tailor these narratives to local populations, amplifying their impact and resonance. For this reason, disinformation as a global and transnational challenge has risen high on the agenda of many international organisations. Beyond the Council of Europe, for example, international organisations such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO) and the World Health Organisation (WHO) have increasingly developed programmes aimed at addressing specific disinformation-related risks.

Given the scope and complexity of the challenge, co-operation among Council of Europe member states is also critical to effectively tackling disinformation and build information integrity. Despite some progress, the responses across member states remain fragmented, with insufficient co-ordination to align efforts and secure a healthy information environment. Effective responses must go beyond carefully tailored domestic policies and focus on the coherence of national measures, the sharing of data and expertise and the development of common standards grounded in human rights and the rule of law. Multilateral co-operation and structured mechanisms for exchange between member states are essential to strengthen resilience to informational threats, enable joint responses and ensure a coherent European approach to safeguarding the integrity of information.

Council of Europe standards

- The Reykjavík Declaration "United around our values" (2023) adopted at the Fourth Summit of Heads of State and Government of the Council of Europe, reaffirms the importance of international co-operation, including to counter mis- and dis-information.
- In Resolution 2567 (2024) on propaganda and freedom of information in Europe, the Parliamentary Assembly calls on states to "strengthen collaboration and look within the framework of the Council of Europe for co-ordinated responses, making better use of the co-operation mechanisms and tools provided by the Organisation" (point 12.18).
- Parliamentary Assembly Resolution 2254 (2019) on media freedom as a condition for democratic elections calls for the adoption of co-ordinated European and global strategies, promoting shared responsibility and a mix of regulatory and dispute resolution approaches to safeguard democratic integrity.
- The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law establishes a Conference of the Parties, a follow-up mechanism enabling monitoring, reporting and co-operation among states and stakeholders to ensure consistent implementation and long-term compliance – offering a model for structured transnational co-operation (Article 23).
- The Guidance note on countering online mis- and disinformation (2023) stresses the need for collaborative, multistakeholder responses and highlights the importance of shared standards and international dialogue to address cross border disinformation while upholding freedom of expression.

Promising practices

The European Union has been at the forefront of developing policies to tackle cross border disinformation, aiming to create a coherent and co-ordinated approach across member states.[95] The European Council has established a Horizontal Working Party on enhancing resilience and countering hybrid threats to support coherence and co-operation among the European Union and its member states.[96] In parallel, NATO's Strategic Communications Centre of Excellence facilitates the exchange of expertise, resources and best practices among NATO member states, enhancing collective capacity to counter disinformation.[97] At the Council of Europe level, the project RESIST: Strengthening Societal Resilience to Disinformation in Europe, funded by EEA and Norway Grants and running from 2025 to 2030, aims to support member states in developing comprehensive, collaborative approaches and deepening cross border co-ordination to improve resilience against disinformation.[98] Member states such as Republic of Moldova, Romania and Ukraine are also exploring co-operation mechanisms, by for example looking into creating a coalition in the field of cybersecurity with the view "to build on Ukraine's experience gained in recent years [and] strengthen a common operational framework for prevention, detection and co-ordinated response to cyber threats". [99]

Recommendation

Foster structured and sustained interstate and international co-operation mechanisms to effectively co-ordinate responses to disinformation, facilitate the exchange of best practices and strengthen efforts to safeguard information integrity. Prioritise:

- ✓ **Recognising cross border threats**: acknowledge both domestic and foreign disinformation, information interference and hybrid threats as critical challenges to national and international security. Ensure responses account for the spillover effects of these threats across borders and remain in alignment with human rights standards.
- ✓ **Identifying synergies**: proactively identify areas of synergy with other countries, assess how measures implemented by other states can complement domestic efforts and seek shared solutions to address cross border threats.
- ✓ **Multilateral approaches**: leverage the resources of European and international organisations and forums to strengthen co-operation and co-ordination in addressing the threat of disinformation and support multilateral initiatives that foster collaborative cross border efforts in building information integrity.

Building block 9 – Foster multi-stakeholder synergies

The growing challenge of disinformation, particularly in the digital space, requires co-ordinated and cross-sectoral efforts to ensure long-term, inclusive and effective responses that respect human rights. Disinformation spreads rapidly across media channels and borders, impacting public discourse and trust. For disinformation responses to be robust and sustainable, it is essential that governments, tech platforms, civil society, academics and other stakeholders collaborate in designing and implementing policies. A multi-stakeholder approach allows for a more comprehensive understanding of the problem and facilitates the adoption of measures that are human rights compliant and more effective. By working together, these diverse actors can help design and implement responses to disinformation that are better informed, context-appropriate, gender-mainstreamed and responsive to the needs of the public, including groups that are particularly targeted by or exposed to disinformation. Overall, it contributes to transparency, accountability and alignment with democratic principles.

While the involvement of multiple stakeholders is crucial, the process often faces challenges that hinder meaningful participation and effective co-ordination. **Many Council of Europe member states still lack structured, inclusive mechanisms for stakeholder engagement, leading to gaps in accountability and uneven responses to disinformation**. Platforms, for example, often retain significant discretion over when and how they engage with stakeholders, resulting in consultations that may be non-binding or insufficiently impactful. Furthermore, the varying levels of resources and representation across stakeholders can lead to unequal participation, where groups in situations of vulnerability and at risk of discrimination are excluded from critical discussions. To address these gaps, it is necessary to implement binding and transparent processes for consultation, participation and follow-up. Ensuring that all relevant parties – especially those most affected by disinformation – are involved at every stage of policy design, implementation and evaluation has the potential to enhance the effectiveness of responses to disinformation and improve overall accountability.

Council of Europe Standards

- Recommendation CM/Rec(2011)7 on a new notion of media calls for engagement with "all actors in the media ecosystem in order for them to be properly apprised of the applicable legal framework; invite traditional and new media to exchange good practice and, if appropriate, consult each other in order to develop self-regulatory tools, including codes of conduct, which take account of, or incorporate in a suitable form, generally accepted media and journalistic standards" (point 7).
- Recommendation CM/Rec(2022)11 on principles for media and communication governance singles out "openness and inclusiveness" as two of the fundamental procedural principles, whereby "media and communication governance should be open and inclusive to satisfy the right to be heard of various groups and interests in society and to democratise decision making about communication in the public sphere" (principle 2). Its Explanatory Memorandum further develops these principles, by calling on states (para. 2.2) and other media actors (para. 2.3) to engage in regular, open and inclusive consultation, co-operation, and dialogue with all relevant stakeholders with a view to ensuring that an appropriate balance is struck between the public interest, interests of users and affected parties and industry interests" and "pay particular attention to the needs and voices of vulnerable subjects and minorities as well as to gender and ethnic diversity" (para. 2.4).

- Parliamentary Assembly Resolution 2255(2019) on public service media in the context of disinformation and propaganda specifically recommends that online platforms co-operate with public and private European news outlets to improve the "visibility of reliable, trustworthy news and facilitate users' access to it" (para. 8.2).
- The Guidance note on countering online mis- and disinformation (2023) stresses that "[s]tates, civil society, platforms, public service media, news organisations, fact-checkers … user communities and researchers should collaborate to develop and implement wide-ranging measures to enhance user empowerment"(point 38). It also points out that the development of criteria for prioritising reliable news and public interest content on platforms should be done through a transparent, multi-stakeholder process, ensuring broad collaboration to establish fair and credible standards (Explanatory report, point 3.d).
- The Guidance note on content moderation (2021) mentions co-regulation as a form of *ad hoc* co-operative framework between public and private actors. It also highlights that such frameworks need to be set up by the state, to prevent arbitrary decisions by private actors.

Promising practices

In recent years, several new bodies have been created at both EU and global levels to strengthen co-ordination and build synergies among a wide range of stakeholders, including civil society, the media, technology companies and policymakers. At EU level, these include the European Board for Media Services,[100] the European Board for Digital Services[101] and the European Artificial Intelligence Board.[102] The European Digital Media Observatory (EDMO)[103] – an EU-funded initiative designed to support a co-ordinated response to disinformation across Europe – brought together experts from academia, fact-checking organisations, media literacy communities and policy research. It has played a crucial role in shaping data access, promoting research infrastructures as well as expanding media literacy measures and fact-checking. In the private sector, Meta's Oversight Board provides another notable example bringing together academics, policy makers and other experts.[104]

At national level, in February 2023, Ireland set up a multi-stakeholder working group to develop a National Counter Disinformation Strategy.[105] Italy's National Cybersecurity Strategy 2022-2026 provides another example, establishing co-ordination mechanisms among government institutions and agencies to prevent and counter online disinformation. It also includes multi-stakeholder initiatives and campaigns aimed at raising public awareness about online and cybersecurity risks.[106] Likewise, Latvia has set up inter-institutional mechanisms to enhance awareness and counter information threats, including the National Information Space Security Co-ordination Group.[107] Various member states also participate on the Steering Group of the OECD Hub on Information and Integrity, and have contributed to the development of the 2024 OECD Recommendation on Information Integrity.[108]

Recommendation

Allow and enable the meaningful participation of all stakeholders, including civil society, media and the private sector, when developing and enforcing legislation, policies and regulation, by actively involving them in meaningful consultations, taking into account their specific roles and responsibilities; establish inclusive and stable multi-stakeholder frameworks that foster collaboration and shared decision making. Prioritise:

- ✓ **Regular and inclusive consultations:** Organise regular, transparent exchanges on disinformation policies with a wide range of stakeholders, ensuring that all interested parties have access to relevant information and can contribute meaningfully.
- ✓ **Involvement in policy implementation:** Ensure that all relevant stakeholders, including public authorities, platforms, civil society, academia and the public, are involved in the implementation of policies to counter disinformation by engaging in inclusive consultations.
- ✓ **Follow-up and monitoring:** Introduce binding follow-up mechanisms to assess the impact of multi-stakeholder consultations, support monitoring and audits and require intermediaries and platforms to give due consideration to stakeholder input and transparently explain the reasons for not implementing them.
- ✓ **Inclusive processes:** Guarantee inclusive and equitable participation by providing funding or representation mechanisms for underrepresented or under-resourced groups and ensure their participation is meaningful. Potential targets or victims of disinformation should participate at all stages of policy design, implementation, evaluation and follow-up.
- ✓ **Scientific committees**: Establish independent scientific committees composed of experts and researchers from academia, public institutions, civil society and industry. These committees could continuously provide evidence-based advice to inform decision making by public authorities and platforms, contributing to legitimacy and accountability in cross-sector responses to disinformation.

Building block 10 – Foster long-term trust in institutions and the media

In many Council of Europe member states, declining public trust in media and institutions undermines societal resilience and democratic legitimacy. Trust in the media is generally low across Europe, with only a few high trust environments.[109] Confidence in government, healthcare systems and law enforcement has also steadily declined in recent years.[110] This erosion of trust affects all segments of society, from the financially vulnerable to the more affluent.[111] Disinformation and information manipulation exacerbate the problem, further undermining trust, driving polarisation and weakening societal resilience. The COVID-19 pandemic provides a striking example of how mistrust can hinder governments' ability to respond effectively to crises, while amplifying the harmful effects of disinformation and propaganda. Restoring trust in democratic institutions, the media and science requires addressing the underlying social, economic and political factors that fuel scepticism and disengagement. This calls for holistic, evidence-based strategies that reduce structural inequalities, address cultural drivers of mistrust, foster transparency and promote inclusive and reliable information ecosystems.

Council of Europe member states should **adopt long-term approaches that go beyond regulatory measures and consider the broader societal dynamics that drive distrust**. This includes understanding why communities disengage from institutional discourse and how digital environments shape these dynamics. Lessons can also be drawn from societies where trust in institutions, media and fellow citizens remains high, to assess whether certain practices can be adapted elsewhere.

High-quality empirical research is essential to identify the root causes of declining or increasing trust, evaluate the effectiveness of interventions and inform evidence-based strategies to counter disinformation. Data-driven approaches can help policymakers identify at-risk communities, understand the impact of social and economic inequalities on trust and tailor responses accordingly.

Furthermore, **social media and other online platforms can be leveraged as tools to rebuild trust**, for example through "prosocial design"[112] and "bridging algorithms"[113] that encourage positive engagement and exposure to diverse perspectives to foster societal cohesion. Promoting transparency, accountability and participatory engagement in digital spaces can help create an information ecosystem where trust is actively reinforced rather than eroded.

Council of Europe Standards

- Council of Europe Convention on access to official documents (CETS No. 205, the Tromsø Convention) aims to ensure transparency of governmental activities through proactive and responsive measures for those seeking official information.
- Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age provides examples of practices, involving a range of stakeholders, such as journalists, publishers and policymakers, that can contribute to a more trustworthy media environment, including ethical policies, transparency of financing and ownership, as well as legal frameworks to support independence.
- Parliamentary Assembly Resolution 2567 (2024) on propaganda and freedom of information in Europe and the Guidelines of the Committee of Ministers on protecting freedom of expression and information in times of crisis stress that maintaining the right of

access to information during states of emergency, is fundamental to build trust around governmental information processes (point 12.10, Resolution 2567 (2024)).

- The Guidance note on countering online mis- and disinformation (2023) highlights how fact-checking can strengthen journalistic integrity and build trust, urging public support to promote the independence and sustainability of fact-checking organisations.

Promising practices

Positive and proactive communication, as well as media and information literacy measures, can play an important role in increasing trust in institutions and the media. In Ireland, campaigns such as "Be Election Smart" and voter registration efforts help citizens identify reliable information during election periods. In Ukraine, NGO coalitions monitor media during elections, debunk disinformation and implement educational programmes like "Filter" to boost voter awareness and critical thinking. Enhancing public awareness and strategic communication can also be a crucial component of an "early warning system" for disinformation. These are mechanisms designed to detect, assess and respond to emerging disinformation threats in a timely manner. During high-risk times, such as ahead of elections, during political unrest, or geopolitical tensions, it is critical to have an established, rapid-response communication strategy. The EU, for example, has set up the European External Action Service (EEAS) Strategic Communication Task Forces "to work with partners and support the EU's message in different parts of the world" in a way that responds effectively to FIMI and disinformation".[114] Official government channels and public broadcasters also play a central role in delivering fact-based, timely updates that counter the noise of mis- and disinformation, guiding public opinion in a constructive direction. Norway, for example, was praised for its open governmental communication during the COVID-19 pandemic, that empowered citizens to understand data, engaged with criticism and objections to proposed measures and involved society in a dialogue.[115]

Recommendation

Adopt a holistic, long-term national strategy to rebuild trust in democratic institutions and quality news media. To be effective, the strategy should:

- ✓ **Monitor levels of public trust regularly**: Use national/regional surveys and qualitative tools to track trust levels and inform policy. Data should identify trust gaps and guide adjustments in institutional communication and media policies.
- ✓ **Build on transparent communication**: Ensure transparent, inclusive and participatory institutional communication, in line with the recommendations of the Tromsø Convention. This entails adopting proactive disclosure policies, maintaining access to official information during emergencies and embedding procedural fairness.
- ✓ **Proactively detect and mitigate information voids**: Identify areas where the absence of reliable, professional information allows manipulative narratives to take hold by establishing early-warning systems and mobilising trustworthy media service providers.
- ✓ **Encourage participatory decision making**: Involve citizens and residents through open consultations and collaboration with trusted local actors (e.g., teachers, doctors, journalists) to bring them closer to state institutions and ensure meaningful scrutiny of public policies.
- ✓ **Collaborate with trusted partners**: Collaborate with trusted intermediaries to enhance public credibility and information outreach. These intermediaries include

local journalists, educators, healthcare professionals, community leaders and civil society organisations, who have established trust within their communities and can effectively communicate reliable information, especially where institutional trust is low. Social media platforms could also contribute as particularly influential trusted partners.

- ✓ **Adress trust in a wide range of policies**: Integrate trust-building into social and economic policies, focusing on reducing inequalities to tackle the possible root causes of mistrust.

Glossary

For the purpose of this document

Artificial intelligence (AI): an "artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments.[116]

Deepfake: manipulated or synthetic audio or visual media that seem authentic, and which feature (a) person(s) that appear(s) to say or do something they have never said or done, produced using artificial intelligence techniques, including machine learning and deep learning.[117]

Disinformation: verifiably false, inaccurate or misleading information *deliberately* created and disseminated to cause harm or pursue economic or political gain by deceiving the public.[118]

Foreign information manipulation and interference (FIMI): a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processed. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory.[119]

Identity-based disinformation: the spreading misleading or false claims related to gender, sexuality, race, ethnicity, religion and other identity markers that aim at adversely impacting marginalised communities.[120]

Influence operation: refers to co-ordinated efforts to influence a target audience, relying on a range of deceptive tactics, including suppressing independent information sources in combination with spreading fabricated content (also: co-ordinated inauthentic activity).[121]

Information disorder: an umbrella term for harmful content that can have an impact on individuals or society.[122]

Information integrity: the product of an information environment that promotes access to accurate, reliable, evidence-based and plural information sources and that enables individuals to be exposed to plural and diverse ideas, make informed choices and better exercise their rights.[123]

Societal information resilience: a society's ability to create systems of trustworthy information provision, its readiness to support knowledge institutions and its investment in measure of media and information literacy (MIL) that would help citizens identify trustworthy sources and content.

Malinformation: genuine information shared to cause harm, often by moving information designed to stay private into the public sphere.[124]

Misinformation: refers to verifiably false, inaccurate or misleading information disseminated *without an intention* to mislead, cause harm, or pursue economic or political gain.[125]

Media and information literacy (MIL): a set of cognitive, technical and social skills and capacities that empower citizens to effectively access, critically analyse, evaluate, create,

reflect on and act using various forms of media content and information across all channels of communication, including in the context of widespread use of AI.[126]

User empowerment: it refers to the means through which users expand their understanding, informed choice and control of their online experience to fully benefit from its opportunities and address its risks without becoming overburdened.[127]

Whole-of-society approach: a concept based on the engagement of diverse groups, including citizens, to achieve common policy goals, among other things, through increasing social and political trust, highlighting the culture of democratic participation and emphasising the need to increase critical media literacy.

Endnotes

[1] Council of Europe (2025), *Towards a new Democratic Pact for Europe*, Report of the Secretary General, available at https://go.coe.int/GOaxe, p. 13.
[2] See United Nations, Development Coordination Office (2025), *Disinformation is a global risk. So why are we still treating it like a tech problem?*, Blog post, available at https://un-dco.org/stories/disinformation-global-risk-so-why-are-we-still-treating-it-tech-problem.
[3] More details at www.coe.int/en/web/new-democratic-pact-for-europe/home.
[4] See e.g. Council of Europe, Steering Committee for Media and Information Society (CDMSI) (2023), *Guidance note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner*, CM(2024)9-add1, emphasis added. The concept of disinformation is part of the broader framework of "information disorder", a term which also includes related and interconnected phenomena such as harmful misinformation and malinformation, see Wardle C. and Derakhshan H. (2017), *Information disorder. Toward an interdisciplinary framework for research and policymaking*, Strasbourg, Council of Europe, available at https://go.coe.int/lmtTh.
[5] See, for example: European Commission (2025), *Code of conduct on disinformation – As amended in October 2024*, available at https://data.europa.eu/doi/10.2759/5029213;, UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression (2020), *Joint Declaration on Freedom of Expression and elections in the digital age*, adopted on 30 April 2020, available at https://www.osce.org/representative-on-freedom-of-media/451150, as well as and the three reports on *Foreign information manipulation and interference threats* by the European External Action Service (EEAS): Strategic Communication and Foresight (SG.STRAT), respectively (2023) *Towards a framework for networked defence*, (2024) *A framework for networked defence* and (2025) *Exposing the architecture of FIMI operations*, available at www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.
[6] Organisation for Economic Co-operation and Development (OECD), Council on Information Integrity (2024), *Recommendation on Information Integrity*, adopted on 17 December 2024, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505.
[7] United Nations (2024), *Global Principles for Information Integrity. Recommendations for Multi-stakeholder Action*, available at https://doi.org/10.18356/9789211065756.
[8] Terms of reference of the Steering Committee on Media and Information Society (CDMSI), in *Programme and Budget 2024-2027 - Terms of Reference of Intergovernmental Structures*, CM(2023)131-addfinal.
[9] *Reykjavík Principles for Democracy*, in *Reykjavík Declaration "United around our values"*, Appendix III, adopted at the Fourth Summit of Heads of State and Government of the Council of Europe, 16-17 April 2023, available at https://go.coe.int/1l5MN.
[10] Wardle C. and Derakhshan H, 2017, cited above, note 4.
[11] Bontridder N. and Poullet Y. (2021), "The role of artificial intelligence in disinformation", *Data & Policy*, vol. 3, issue e32, available at https://doi.org/10.1017/dap.2021.20.
[12] See Blagojev T. et al. (2025), *Monitoring media pluralism in the European Union: results of the MPM2025*, European University Institute, available at https://hdl.handle.net/1814/92916; and Bleyer-Simon K. (ed.) (2025), *How is disinformation addressed in the member states of the European Union? : 27 country cases*, European University Institute, available at https://hdl.handle.net/1814/92834.
[13] See Jack C. (2019), "Wicked content", *Communication, Culture & Critique*, vo. 12, issue 4, pp. 435-454.
[14] Grambo K. (2019), "Fake news and racial, ethnic, and religious minorities: A precarious quest for truth", *University of Pennsylvania journal of constitutional law*, available at https://scholarship.law.upenn.edu/jcl/vol21/iss5/4.
[15] Bennett W.L. and Livingston S. (2018), "The disinformation order: Disruptive communication and the decline of democratic institutions", *European journal of communication*, vol. 33, issue 2.
[16] Suarez-Lledo V. and Alvarez-Galvez J. (2021), "Prevalence of health misinformation on social media: systematic review", *Journal of medical Internet research*, vol. 23, issue 1, available at https://doi.org/10.2196/17187.
[17] Lewandowsky S. (2021), "Climate change disinformation and how to combat it", *Annual review of public health*, vol. 42, issue 1, available at https://doi.org/10.1146/annurev-publhealth-090419-102409.
[18] Bleyer-Simon K. and Reviglio U. (2024), *Defining disinformation across EU and VLOP policies*, European Digital Media Observatory (EDMO) Policy Report, European University Institute, available at https://hdl.handle.net/1814/77435.
[19] See Knott A. at al. (2024), "AI content detection in the emerging information ecosystem: new obligations for media and tech companies", *Ethics and Information Technology*, vol. 26, issue 4, p. 63, available at https://doi.org/10.1007/s10676-024-09795-1; Khachaturov D., Schnyder R. and Mullins R. (2025), "Governments should mandate tiered anonymity on social-media platforms to counter deepfakes and LLM-driven mass misinformation", *arXiv* (preprint), available at https://doi.org/10.48550/arXiv.2506.12814.
[20] Ireland, Department of Culture, Communications and Sport (2025), *National counter disinformation strategy*, available at www.gov.ie/en/department-of-culture-communications-and-sport/publications/national-counter-disinformation-strategy-working-group/

[21] Norway (2025), *Strategi for å styrkje motstandskrafta mot desinformasjon (2025-2030)* available only in Norwegian at www.regjeringen.no/no/aktuelt/regjeringen-legger-frem-en-strategi-for-a-styrke-motstandskraften-mot-desinformasjon/id3109197/.
[22] Latvia (2023), *The National Concept on Strategic Communication and Security of the Information Space 2023–2027*, available at www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija.
[23] Bleyer-Simon K. (ed.) (2025), *How is disinformation addressed in the member states of the European Union? : 27 country cases*, European University Institute, available at https://hdl.handle.net/1814/92834.
[24] Baqir A., Galeazzi A. and Zollo F. (2024), "News and misinformation consumption: A temporal comparison across European countries", *Plos.one*, vol. 19, issue 5, available at https://doi.org/10.1371/journal.pone.0302473.
[25] See Altay S., Berriche M. and Acerbi, A. (2023), "Misinformation on misinformation: Conceptual and methodological challenges", *Social media+ society*, vol. 9, issue 1, available at https://doi.org/10.1177/20563051221150412.
[26] Terenzi M. and Giglietto F. (2025), "Cracking the code: social data access and the DSA's impact on disinformation research", *European journalism observatory*, available at https://en.ejo.ch/recent/cracking-the-code-social-data-access-and-the-dsas-impact-on-disinformation-research.
[27] Aïmeur E., Amri S. and Brassard G. (2023), "Fake news, disinformation and misinformation in social media: a review", *Social network analysis and mining*, vol. 13, issue 1, p. 30, available at https://doi.org/10.1007/s13278-023-01028-5.
[28] Rieder B. and Hofmann J. (2020), "Towards platform observability", *Internet policy review*, vol. 9, issue 4; Thorburn L. (2022), "How to measure the effects of recommenders", *Medium*, available at https://medium.com/understanding-recommenders/how-to-measure-the-causal-effects-of-recommenders-5e89b7363d57.
[29] Knott A. et al. (2024), "The EU's Digital Services Act must provide researchers access to VLOPs' experimental protocols", *Forum for information and democracy*, available at https://informationdemocracy.org/2024/06/14/the-forum-members-of-its-working-group-and-researchers-call-for-the-dsa-to-provide-researchers-access-to-conduct-experimental-evaluations-of-vlops/ .
[30] European Commission (2022), *The strengthened Code of practice on disinformation 2022*, available at https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.
[31] European Commission (2025), *Code of conduct on disinformation – As amended in October 2024*, available at https://data.europa.eu/doi/10.2759/5029213.
[32] European Union, *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)*, available at http://data.europa.eu/eli/reg/2022/2065/oj, hereinafter "EU Digital Services Act".
[33] See Nenadic I., Brogi E. and Bleyer-Simon K (2023), *Structural indicators to assess effectiveness of the EU's Code of Practice on Disinformation*, RSC Working Paper 2023/34, European University Institute, available at https://hdl.handle.net/1814/75558.
[34] European Digital Media Observatory (EDMO) (2022), *Report of the European Digital Media Observatory's Working Group on platform-to-researcher data access*, available at https://edmo.eu/edmo-news/edmo-releases-report-on-researcher-access-to-platform-data/.
[35] See the official website of the Agency: https://mpf.se/psychological-defence-agency.
[36] Blagojev T. et al. (2025), *Monitoring media pluralism in the European Union: results of the MPM2025*, European University Institute, available at https://hdl.handle.net/1814/92916.
[37] Open Society Institute Sofia (2023), *The Media Literacy Index 2023*, available https://osis.bg/?p=4450&lang=en.
[38] Eurostat (2024), *Skills for the digital age*, at https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Skills_for_the_digital_age.
[39] See Dame Adjin-Tettey T. (2022), "Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education", *Cogent arts & humanities*, vol. 9, issue 1.
[40] On the components of resilience, see Humprecht E., Esser F. and Van Aelst P. (2020), "Resilience to online disinformation: A framework for cross-national comparative research", *The international journal of press/politics*, vol. 25, issue 3.
[41] Fasching M. and Schubatzky T. (2022), "Beyond truth: Teaching digital competences in secondary school against disinformation: Experts' views on practical teaching frameworks for basic digital education in Austria", *Medienimpulse*, vol. 60, issue 3, available at https://doi.org/10.21243/mi-03-22-19.
[42] Diaz Ruiz C. (2025), "Disinformation on digital media platforms: A market-shaping approach", *New media & society*, vol. 27, issue 4, available at https://doi.org/10.1177/14614448231207644.
[43] Kimani R. (2024), "Digital media literacy for adults over 60: Five insights", *DW Akademie*, available at https://akademie.dw.com/en. See also Hermans A. (2022), *The digital era? Also my era! Media and information*

literacy: a key to ensure seniors' rights to participate in the digital era, Council of Europe, available at https://go.coe.int/WyA0C.

[44] See Eskens S., Helberger N., and Moeller J. (2017), "Challenged by news personalisation: Five perspectives on the right to receive information", *Journal of media law*, vol. 9, issue 2, available at https://doi.org/10.1080/17577632.2017.1387353. See also Knight-Georgetown Institute (KGI), Expert Working Group on Recommender Systems (2025), *Better Feeds: Algorithms That Put People First: A How-To Guide for Platforms and Policymakers*, available at https://kgi.georgetown.edu/research-and-commentary/better-feeds/.

[45] See Kuenzi R. (2019), "Teaching students how to live democratically", *Swissinfo*, available at www.swissinfo.ch/eng/democracy/political-education_teaching-students-how-to-live-democratically/44859236.

[46] See Cagé J. (2016), Saving the media: Capitalism, crowdfunding, and democracy, Belknap. See also, United Kingdom, Ofcom (2025), Transmission Critical. The future of Public Service Media, Report, available at www.ofcom.org.uk/tv-radio-and-on-demand/public-service-broadcasting/public-service-media-review ; Argentesi E. and Filistrucchi L. (2007), "Estimating market power in a two-sided market: The case of newspapers", Journal of applied econometrics, vol. 22, issue 7; Pickard V. (2020), Democracy without Journalism?: Confronting the Misinformation Society, Oxford University Press.

[47] See Parcu P.L. (2020), "New digital threats to media pluralism in the information age", *Competition and Regulation in Network Industries*, vol. 21, issue 2.

[48] Kępa-Figura D., Szkudlarek-Śmiechowicz E. and Belovodskaja A. (2025), "Clickbaitism and trust in media outlets", in Paliszkiewicz at al. (eds.) *Trust, media and the economy*, Routledge.

[49] See Schiffrin A. (ed.). (2021), *Media capture: How money, digital platforms, and governments control the news*, Columbia University Press.

[50] Blagojev T. et al. (2023). *News deserts in Europe: Assessing risks for local and community media in the 27 EU member states*; *Preliminary report*, European University Institute, available at https://hdl.handle.net/1814/75762; and Verza S. et al (eds) (2024), *Uncovering news deserts in Europe: risks and opportunities for local and community media in the EU*, *Research project report*, European University Institute, available at https://hdl.handle.net/1814/76652.

[51] Blagojev T. et al. (2025), *Monitoring media pluralism in the European Union: results of the MPM2025*, European University Institute, available at https://hdl.handle.net/1814/92916.

[52] Newman N. (2025), *Overview and key findings of the 2025 Digital News Report*, Reuters Institute for the Study of Journalism, available at https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2025/dnr-executive-summary.

[53] Mazzoli E.M. and Tambini D. (2020), *Prioritisation uncovered. The discoverability of public interest content online*, Study DGI(2020)19, Council of Europe, available at https://go.coe.int/5JXJ0.

[54] Council on Foundations (2021), *Nonprofit law in Romania*, available at https://cof.org/country-notes/nonprofit-law-romania, see also Starkman D. and Chittum R. (2021), "The Hamster wheel, triumphant: Commercial models for journalism are not working; Let's try something else", in Schiffrin A. (ed.) (2021), *Media capture: How money, digital platforms, and governments control the news*, Columbia University Press, 232-258.

[55] Grbeša Zenzerović M. and Nenadic I. (2022), *Strengthening resilience to disinformation: the state of affairs and guidelines for action*, 2nd edn., Agency for Electronic Media, available at https://aem.hr/blog/2010/02/18/publikacije/?lang=en.

[56] See more information at https://informazioneeditoria.gov.it/it/misure-di-sostegno-alleditoria/fondi-per-leditoria/fondo-unico-per-il-pluralismo-e-l-innovazione-digitale-dell-informazione-e-dell-editoria/.

[57] Journalism Trust Initiative. https://rsf.org/en/journalism-trust-initiative.

[58] NewsGuard. News Reliability Ratings, available at www.newsguardtech.com/solutions/news-reliability-ratings/.

[59] ISO (2025). IWA 44:2025. Global Media Identifier (GMI) for distribution channels and brands, available at www.iso.org/standard/88469.html.

[60] Among numerous sources, see Panizio E. (ed.) (2024), Disinformation narratives during the 2023 elections in Europe, European Digital Media Observatory (EDMO) Report, 2nd edn, available at https://edmo.eu/publications/second-edition-march-2024-disinformation-narratives-during-the-2023-elections-in-europe/; and the three reports on *Foreign information manipulation and interference threats* by the European External Action Service (EEAS): Strategic Communication and Foresight (SG.STRAT), respectively (2023) *Towards a framework for networked defence*, (2024) *A framework for networked defence* and (2025) *Exposing the architecture of FIMI operations*, available at www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.

[61] Parliamentary Assembly, Resolution 2593 (2025) on Foreign interference: a threat to democratic security in Europe. See also European Union, *Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine*, available at http://data.europa.eu/eli/reg/2022/350/oj, and *Council Decision (CFSP) 2022/351 of 1 March*

2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, available at http://data.europa.eu/eli/dec/2022/351/oj, respective Preambular paragraphs 6.

[62] *Bradshaw and others v. the United Kingdom*, No. 15653/22, Judgement of 22 July 2025, para. 134.

[63] Blagojev T. et al. (2025), *Monitoring media pluralism in the European Union: results of the MPM2025*, European University Institute, available at https://hdl.handle.net/1814/92916.

[64] Dawson J. (2021), "Microtargeting as information warfare", *The Cyber Defense Review*, vol. 6, issue 1, 63–80, available at www.jstor.org/stable/26994113.

[65] Prysiazhniuk M. (2025), "Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact", *Culture. Society. Economy. Politics*, vol. 5, issue 1, 88-108, available at https://doi.org/10.2478/csep-2025-0007.

[66] See the EEAS Reports on FIMI threats, cited above, available at www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.

[67] France, *Law No. 2018-1202 of 22 December 2018 on the fight against the manipulation of information*, available at www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559. On the compatibility of the law with the right to freedom of expression, see France, Constitutional Council, *Decision No. 2018-773 DC of 20 December 2018*, available at www.conseil-constitutionnel.fr/en/decision/2018/2018773DC.htm. See also Craufurd Smith R. (2019), "Fake news, French Law and democratic legitimacy: lessons for the United Kingdom?", *Journal of media law*, vol. 11, issue 1, available at https://doi.org/10.1080/17577632.2019.1679424.

[68] Ireland, *Electoral Reform Act 2022*, available at www.irishstatutebook.ie/eli/2022/act/30/enacted/en/html. Note however the academic commentary questioning the balance between election integrity and freedom of expression in Shattock E. (2024), "Knowledge, deception, and freedom of expression: a critical examination of Ireland's approach to disinformation under the Electoral Reform Act 2022", *International review of law, computers & technology*, vol. 39, issue 3, available at https://doi.org/10.1080/13600869.2024.2428145.

[69] See European Commission: European Political Strategy Centre (2025), *The future of European competitiveness. Part A, A competitiveness strategy for Europe*, Publications Office of the European Union, available at https://data.europa.eu/doi/10.2872/9356120.

[70] See, also, Botero Arcilia B. and Griffin R. (2023), *Social media platforms and challenges for democracy, rule of law and fundamental rights*, European Parliament, available at https://data.europa.eu/doi/10.2861/672578.

[71] Lukovic V. (2021), "Information asymmetries in algorithms at digital platforms: motivations to participate and EU regulatory approach", *EMAN 2021 Conference Proceedings*, available at https://doi.org/10.31410/EMAN.2021.167.

[72] Veltri G.A. et al. (2023), "The impact of online platform transparency of information on consumers' choices", *Behavioural public policy*, vol. 7, issue 1, available at https://doi.org/10.1017/bpp.2020.11.

[73] Diaz Ruiz C. (2025), "Disinformation on digital media platforms: A market-shaping approach", *New media & society*, vol. 27, issue 4, available at https://doi.org/10.1177/14614448231207644; Cunningham T. et al. (2025), "Ranking by engagement and non-engagement signals: Learnings from industry", *Annals of the New York Academy of Sciences*, available at https://doi.org/10.1111/nyas.15399.

[74] See European Commission, European Political Strategy Centre (2025), *The future of European competitiveness. Part A, A competitiveness strategy for Europe*. Publications Office of the European Union, available at https://data.europa.eu/doi/10.2872/9356120.

[75] See, European Commission (2023), *Report on the state of the Digital Decade 2023, Communication from the to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM/2023/570 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2023:570:FIN.

[76] This approach is exemplified by the Fediverse, a decentralised ecosystem for social media, see *About Fediverse*, available at https://fediverse.party/en/fediverse/.

[77] Reviglio U. (2025), "Making Media Pluralism Work in the Age of Algorithms", *Tech policy press*, available at www.techpolicy.press/making-media-pluralism-work-in-the-age-of-algorithms/.

[78] Micheli M. et al (2023), *Mapping the landscape of data intermediaries*, Publications Office of the European Union, Luxembourg, available at https://dx.doi.org/10.2760/261724.

[79] See Bria F., Timmers P. and Gernone F. (2025), *EuroStack – A European Alternative for Digital Sovereignty*, Bertelsmann Stiftung, available at https://eurostack.eu/.

[80] *Bradshaw and others v. the United Kingdom*, No. 15653/22, Judgment of 22 July 2025, para. 160.

[81] *Castells v. Spain*, No. 11798/85, Judgment of 23 May 1992, para. 43; *Wingrove v. the United Kingdom*, No. 17419/90, Judgment of 25 November 1996, para. 58.

[82] The examples are drawn from answers received by CDMSI Members. See also, Venice Commission (2022), *Urgent joint opinion No. 1102/2022 of Venice Commission and the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft amendments to the Penal Code regarding the provision on*

"false or misleading information" (Türkiye), CDL-PI(2022)032, available at https://go.coe.int/Zx5k5, paras 5-30; European Regulators Group for Audiovisual Media Services (ERGA) (2020), *Notions of disinformation and related concepts*, ERGA report, available at https://erga-online.eu/wpcontent/uploads/2021/01/ERGA-SG2-Report-2020-Notions-of-disinformation-and-relatedconcepts.pdf; Ó Fathaigh R., Helberger N. and Appelman N. (2021), "The perils of legally defining disinformation", *Internet policy review*, vol. 10, issue 4, available at https://doi.org/10.14763/2021.4.1584; Bleyer-Simon K. (ed.) (2025), *How is disinformation addressed in the member states of the European Union? : 27 country cases*, European University Institute, available at https://hdl.handle.net/1814/92834.

[83] See, for example: Republic of Moldova, *Criminal Code, Article 140*, and *Contravention Code, Article 365.5* (war propaganda); the Netherlands, *Criminal Code, Articles 131 and 132* (incitement to violence or crime); Norway, *Criminal Code, paras 130 and 130a* (national security concerns, including instances involving cooperation with foreign intelligence services).

[84] See, for example: Türkiye, *Penal Code, Article 217/A*; Italy, Penal Code, *Articles 656 and 658*; France, *Law of 29 July 1881 on freedom of the press*, Article 27.

[85] UN Special Rapporteur on Freedom of Opinion and Expression, OSCE Representative on Freedom of the Media, and OAS Special Rapporteur on Freedom of Expression (2020), *Joint Declaration on Freedom of Expression and elections in the digital age*, adopted on 30 April 2020, available at www.osce.org/representative-on-freedom-of-media/451150; European Commission and High Representative of the Union for Foreign Affairs and Security Policy (2020), *Tackling COVID-19 disinformation - Getting the facts right*, Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2020) 8 final, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0008; Commissioner for Human Rights (2020), *Press freedom must not be undermined by measures to counter disinformation about COVID-19*, statement of 4 July 2020, available at https://go.coe.int/zMOkd; United Nations, Human Rights Council (2021), *Disinformation and freedom of opinion and expression*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Irene Khan, UN doc. A/HRC/47/25, 12 April 2021, para. 85, available at www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report; Ó Fathaigh R., Helberger N. and Appelman N. (2021), "The perils of legally defining disinformation", *Internet policy review*, vol. 10, issue 4, available at https://doi.org/10.14763/2021.4.1584; Noorlander P. (2025), *Limiting the use of criminal law to restrict freedom of expression: a guide to Council of Europe standards*, Council of Europe, available at https://go.coe.int/z3hon, pp. 28-30.

[86] Republic of Moldova, *Code of audiovisual media services, as amended by law no. 143 of 2 June 2022*.

[87] Cabrera Blázquez F.J. (2022), *The implementation of EU sanctions against RT and Sputnik*, European Audiovisual Observatory, Strasbourg, available at https://go.coe.int/pj9vi.

[88] Richter A. (2022), *Sanction law against Russian and Belarusian audiovisual media*, European Audiovisual Observatory, Strasbourg, available at https://go.coe.int/PKmIu.

[89] See, for example, EU Digital Services Act, Article 34.1.a (which is applicable only to very large online platforms and search engines); and United Kingdom, *Online Safety Act 2023*, c. 50, available at www.legislation.gov.uk/ukpga/2023/50, hereinafter "United Kingdom Online Safety Act", Sections 9-10 and 26-27 (applicable to regulated user-to-user services and search services respectively, independently of their size or reach).

[90] EU Digital Services Act, Article 34, paras 1.c.and 2.

[91] United Nations, Human Rights Council (2021), *Disinformation and freedom of opinion and expression*, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression Irene Khan, UN doc. A/HRC/47/25, 12 April 2021, para. 85, available at www.ohchr.org/en/documents/thematic-reports/ahrc4725-disinformation-and-freedom-opinion-and-expression-report.

[92] Venice Commission and Directorate of Information Society and Action against Crime of the Directorate General of Human Rights and Rule of Law (DGI) (2019), *Joint Report on Digital Technologies and Elections*, CDL-AD(2019)016, para. 138, available at https://go.coe.int/bD3HD.

[93] Venice Commission (2022), *Opinion No. 1090/2022 on amendments to the Audiovisual Media Services Code and to some normative acts including the ban on symbols associated with and used in military aggression actions (Republic of Moldova)*, CDL-AD(2022)026, available at https://go.coe.int/UXgps; and (2025) *Opinion No. 1240/2025 on the legislative reforms on mass media regulation: the draft law on mass media, the draft law amending the audiovisual media services code, and the draft law amending the law on advertising (Republic of Moldova)*, CDL-AD(2025)027, available at https://go.coe.int/MpWdK.

[94] *Ibidem*.

[95] Nenadić I. (2019), "Unpacking the 'European approach' to tackling challenges of disinformation and political manipulation", *Internet policy review*, vol. 8, issue 4, available at https://doi.org/10.14763/2019.4.1436.

[96] See more at www.consilium.europa.eu/en/council-eu/preparatory-bodies/horizontal-working-party-on-enhancing-resilience-and-countering-hybrid-threats/
[97] See more at https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5.
[98] See more at www.coe.int/en/web/freedom-expression/resist-strengthening-societal-resilience-to-disinformation-in-europe.
[99] See Agerpress (2025), *Coalition in cybersecurity could be formed between Romania, Republic of Moldova and Ukraine (DNSC)*, available at https://agerpres.ro/english/2025/08/04/coalition-in-cybersecurity-could-be-formed-between-romania-republic-of-moldova-and-ukraine-dnsc--1473604.
[100] "An independent advisory body created by the European Media Freedom Act. It gathers independent national media regulators and works closely with the European Commission to support media regulation at EU level". See more at https://media-board.europa.eu/index_en.
[101] "An independent advisory group that has been established by the Digital Services Act, with effect from 17 February 2024". See more at https://digital-strategy.ec.europa.eu/en/policies/dsa-board.
[102] A key EU "advisory body that was created by the AI Act, which took effect on 1 August 2024". See more at https://digital-strategy.ec.europa.eu/en/policies/ai-board
[103] See more at https://edmo.eu/.
[104] The applies "Facebook, Instagram and Threads' content standards in a way that protects freedom of expression and other global human rights standards". See more at www.oversightboard.com/.
[105] See more at www.gov.ie/en/department-of-culture-communications-and-sport/publications/national-counter-disinformation-strategy-working-group/.
[106] See more at www.acn.gov.it/portale/en/strategia-nazionale-di-cybersicurezza.
[107] Latvia, Cabinet Regulation No. 236, *By-laws of the National Information Space Security Coordination Group*, adopted 9 May 2023, available at https://likumi.lv/ta/en/en/id/341811.
[108] Organisation for Economic Co-operation and Development (OECD), Council on Information Integrity (2024), *Recommendation on Information Integrity*, adopted on 17 December 2024, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505.
[109] Newman N. at al (2025), *Digital News Report 2025*, Reuters Institute for the Study of Journalism, available at https://dx.doi.org/10.60625/risj-8qqf-jt36.
[110] Eurofound (2022), *Fifth round of the Living, working and COVID-19 e-survey: Living in a new era of uncertainty*, Publications Office of the European Union, Luxembourg, available at http://eurofound.link/ef22042.
[111] Prats M., Smid S. and Ferrin M. (2024), "Lack of trust in institutions and political engagement: An analysis based on the 2021 OECD Trust Survey", *OECD Working Papers on Public Governance*, No. 75, OECD Publishing, Paris, available at https://doi.org/10.1787/83351a47-en.
[112] See Prosocial Design Network, available at www.prosocialdesign.org/ .
[113] See Bridging Systems, available at https://bridging.systems/.
[114] EEAS Strategic Communication Task Forces, see www.eeas.europa.eu/eeas/eeas-strategic-communication-task-forces_en?s=2803.
[115] See Pileberg S. (2021), "Norwegian authorities have earned the public's trust through openness about their COVID-19 strategy", University of Oslo - Department of Media and Communication, available at https://www.hf.uio.no/imk/english/research/news-and-events/news/2021/norwegian-authorities-have-earned-the-publics-trust.
[116] Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law (CETS no. 225), Article 2.
[117] As defined in European Parliament, Directorate-General for Parliamentary Research Services (2021), *Tackling deepfakes in European policy*, European Parliament, available at https://data.europa.eu/doi/10.2861/325063, p. 2.
[118] As defined in Recommendation CM/Rec(2022)12 on electoral communication and media coverage of election campaigns, and Recommendation CM/Rec(2022)11 on principles for media and communication governance and in the Guidance note on countering online mis- and disinformation, emphasis added, point 3.a. The concept of disinformation is part of the broader framework of "information disorder," a term coined by Wardle C. and Derakhshan H, 2017, cited above, note 4, which also includes related and interconnected phenomena such as harmful misinformation and malinformation.
[119] As defined in European External Action Service (EEAS), Strategic Communication and Foresight (SG.STRAT) (2023), *Foreign information manipulation and interference threats. Towards a framework for networked defence*, available at www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.
[120] European External Action Service (EEAS), Strategic Communication and Foresight (SG.STRAT) (2024), *Foreign information manipulation and interference threats. A framework for networked defence*, available at

www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en#104639.

[121] European Commission (2025), *Code of conduct on disinformation – As amended in October 2024*, available at https://data.europa.eu/doi/10.2759/5029213.

[122] Wardle C. and Derakhshan H, 2017, cited above, note 4, p. 5.

[123] Organisation for Economic Co-operation and Development (OECD), Council on Information Integrity (2024), *Recommendation on Information Integrity*, adopted on 17 December 2024, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505, part II.

[124] Wardle C. and Derakhshan H, 2017, cited above, note 4, p. 5.

[125] Council of Europe (2023), *Guidance note on countering online mis- and disinformation*, point 3.b, emphasis added. See also Wardle C. and Derakhshan H, 2017, cited above, note 4, p. 5.

[126] As defined in Council of Europe (2025), *National media and information literacy (MIL) strategies: Practical steps and indicators*.

[127] As defined in the Draft Recommendation on online safety and empowerment of users and content creators, approved by the CDMSI in December 2025 and to be considered for adoption by the Committee of Ministers in spring 2026, para. 11.