COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES Recommendations **CM/Rec(2022)13** 6 April 2022

Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression

(Adopted by the Committee of Ministers on 6 April 2022 at the 1431st meeting of the Ministers' Deputies)

Preamble

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe (ETS No. 1),

Committed to the shared values of human rights, democracy and the rule of law;

Recalling that Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, "the Convention") confers on everyone the right to freedom of expression, including freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers, and that Article 10.2, as interpreted by the European Court of Human Rights, specifies that these rights can only be limited when such interference is prescribed by law, pursues a legitimate aim and is necessary in a democratic society;

Mindful of the negative obligation of member States not to interfere with freedom of expression and other human rights in the digital environment and of their positive obligation to actively protect human rights and create a safe and enabling environment for everyone to participate in public debate and freely express opinions and ideas;

Noting that private companies should not cause or contribute to adverse human rights impacts through their activities and that they should prevent or mitigate adverse human rights impacts linked to their operations, products or services;

Reiterating that freedom of expression is essential for democratic societies and that digital technologies have become indispensable for this freedom;

Emphasising that digital technologies have expanded individuals' and groups' ability to receive and impart information and that they have increased the range and diversity of information individuals can access;

Conscious that digital technologies can create and strengthen social bonds, help citizens express grievances and promote alliances across borders and cultures, enable marginalised communities to build networks of solidarity and foster more open, inclusive and diverse public spheres;

Recognising the pivotal role played by privately owned providers of digital infrastructures that enable freedom of expression online and shape the conditions under which this right can be exercised, but are not directly subject to the obligations to provide the guarantees and observe the limitations outlined in Article 10 of the Convention;

Recalling that media pluralism is a prerequisite for secure, widespread and unlimited access to information on issues of public interest;

Acknowledging that professional news organisations play a crucial role in the production and distribution of high-quality information, but that new advertising and data exploitation models have jeopardised their business models, thus weakening their financial sustainability and, as a result, their independence;

Recognising that well-funded and independent public-service media can enhance democratic debate;

Noting that effective policy making on the implications of digital technologies for freedom of expression requires accurate, nuanced and comprehensive knowledge derived from rigorous and independent research, but that most such knowledge and the data required to generate it are held by internet intermediaries who, for the most part, do not share them in full;

Conscious of the need to protect children and all those whose human rights, in particular freedom of expression, may be disproportionally harmed by certain types of content that are widely available online, and mindful that any measures to protect them need to respect freedom of expression and other human rights;

Determined to safeguard the rights enshrined in the Convention and committed to follow up on the Declaration by the Committee of Ministers on the occasion of the 70th anniversary of the Council of Europe (17 May 2019), which demanded strong action to reverse the persistent deterioration of freedom of expression in Europe in recent decades,

Recommends that the governments of member States:

1. fully implement the guidelines attached to this recommendation, in effective co-operation with all relevant stakeholders;

2. in implementing the guidelines, take account of the standards enshrined in Article 10 of the Convention, the relevant case law of the European Court of Human Rights, previous recommendations of the Committee of Ministers to member States and its declarations dealing with different aspects of freedom of expression, internet freedom and digital technologies, notably Recommendation CM/Rec(2021)8 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2020)1 on the human rights impacts of algorithmic systems, Recommendation CM/Rec(2018)2 on the roles and responsibilities of internet intermediaries, Recommendation CM/Rec(2016)5 on Internet freedom, Recommendation CM/Rec(2016)1 on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, Recommendation CM/Rec(2015)6 on the free, transboundary flow of information on the Internet, Recommendation CM/Rec(2014)6 on a Guide to human rights for Internet users, Recommendation CM/Rec(2013)1 on gender equality and media, Recommendation CM/Rec(2012)4 on the protection of human rights with regard to social networking services, Recommendation CM/Rec(2012)3 on the protection of human rights with regard to search engines, Recommendation CM/Rec(2011)7 on a new notion of media, and Recommendation CM/Rec(2007)16 on measures to promote the public service value of the Internet;

3. assess and review their legislative, regulatory and supervisory frameworks and policies as well as their practices with respect to the impact of digital technologies on freedom of expression to ensure that they are in line with the guidelines, with a view to avoiding hasty and fragmented measures that may have further adverse effects on the larger information environment;

4. ensure that this recommendation, including the guidelines, is translated and disseminated as widely as possible and through all accessible means among competent authorities and stakeholders, including parliaments, independent authorities, specialised public agencies, civil society organisations, users and the private sector;

5. endow their competent regulatory authorities and institutions with the necessary resources and authority to investigate, oversee and co-ordinate compliance with their relevant legislative and regulatory framework, in line with this recommendation;

6. engage in regular, inclusive, meaningful and transparent consultation, co-operation and dialogue with all stakeholders (including the media, internet intermediaries, civil society, human rights organisations, the research and professional community and educational institutions), paying particular attention to vulnerable individuals and groups, with a view to ensuring that the impacts of digital technologies on freedom of expression are comprehensively monitored, debated and addressed;

7. encourage and promote the implementation of effective and tailored digital literacy programmes, in co-operation with all relevant stakeholders, to enable all individuals and groups to benefit from digital technologies for their enhanced exercise and enjoyment of freedom of expression;

8. fund and promote rigorous and independent research on the individual and societal implications of digital technologies for freedom of expression and take meaningful steps to ensure that independent researchers, free from commercial and political interests, can access the necessary data held by internet intermediaries within an appropriate, human rights-compliant legal framework and especially in accordance with the conditions set out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as updated by its amending Protocol (CETS No. 223);

9. review regularly, in consultation with all relevant actors, and report domestically and within the Committee of Ministers on the measures taken to implement this recommendation and its guidelines with a view to enhancing their effectiveness and adapting them to evolving challenges.

Appendix to Recommendation CM/Rec(2022)13

Guidelines on the impacts of digital technologies on freedom of expression

Scope and definitions

Freedom of expression, as protected by Article 10 of the European Convention on Human Rights (ETS No. 5, “the Convention”), is not only a fundamental individual right. It is also a means to protect and enhance democracy through open and public debate. Digital technologies can, and indeed should, support this right and serve this purpose.

These guidelines are designed to assist States and public and private actors, in particular internet intermediaries, as well as the media, civil society organisations, researchers, educational institutions and other relevant actors in their independent and collaborative efforts to protect and promote freedom of expression in the digital age. The guidelines set out principles aimed at ensuring that digital technologies serve rather than curtail such freedom. They also provide recommendations on how to reduce the adverse impacts and enhance the positive impacts of the widespread use of digital technologies on freedom of expression in human rights-compliant ways.

“Internet intermediaries” are understood here as defined in Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. Bearing in mind that internet intermediaries offer a variety of functions and services and may carry out several functions in parallel, where appropriate, reference is made here to specific functions they perform.

“Privacy”, when referred to in these guidelines, should be understood in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), as updated by its amending Protocol (CETS No. 223) (hereinafter “Convention 108”), as well as with the case law of the European Court of Human Rights, as encompassing any information relating to an identified or identifiable individual, regardless of whether such information is publicly available or not and irrespective of whether it is generated on digital platforms or by other means.

Whenever the provisions of these guidelines imply personal data processing, including when such processing involves data sharing and cross-border data transfers, Convention 108 applies, in particular as regards enhanced requirements for the processing of sensitive data and other safeguards and guarantees.

The guidelines are organised into six sections: foundations for human rights-enhancing rule-making; digital infrastructure design; transparency; accountability and redress; education and empowerment; and independent research for evidence-based rule-making. Each section offers guidance to States and other stakeholders on how to fulfil their human rights obligations and responsibilities with regard to freedom of expression, combining legal, regulatory, administrative and practical measures.

1. Foundations for human rights-enhancing rule-making

1.1. **Clear and unambiguous objectives**. Any self-regulation, co-regulation or regulation of digital technologies that potentially restricts freedom of expression should clearly distinguish between responses to illegal forms of expression and responses to forms of expression that are legal and protected by Article 10 of the Convention but that may potentially infringe other human rights enshrined in the Convention. State regulation should only restrict the dissemination of content that is illegal, and any such restrictions should comply with Article 10.2 of the Convention. For content that is legal but may potentially infringe other human rights enshrined in the Convention, alternative responses should be sought that prioritise safeguards rather than restrictions on freedom of expression, in line with point 1.5 of these guidelines. Consistent with their obligation to protect human rights, States should ensure that all regulatory frameworks, including self- or co-regulatory approaches, comply with the Convention.

1.2. **Legality, necessity and predictability**. Any State policies or actions interfering with the right to freedom of expression should be prescribed by law, pursue one of the legitimate aims listed in Article 10.2 of the Convention, employ proportionate means and fulfil the requirements of legal certainty, necessity and predictability.

1.3. **Precision**. States should only regulate forms of expression and types of content that they have clearly defined. Definitions that are vague and lend themselves to subjective interpretations should be avoided in regulatory practice, as they cannot provide sufficient clarity and predictability to all parties involved and can result in disproportionate and unjustified hindrances to freedom of expression.

1.4. **Proportionality**. Any regulation, compliance requirement and administrative process put in place to achieve the goals highlighted in these guidelines should be proportionate to the risk level, size and capacity of different internet intermediaries. States should only impose substantial obligations on very large internet intermediaries, defined on the basis of their reach and ability to affect the exercise of freedom of expression, and on companies that enable or perform activities that pose a credibly high risk to freedom of expression. The criteria upon which the size, capacity and risk level of different internet intermediaries are assessed should be specified clearly, reviewed periodically, measured precisely and communicated transparently by the regulator.

1.5. **Graduated response**. In their regulatory and co-regulatory initiatives, States should acknowledge that internet intermediaries can employ various content moderation techniques beyond removal. These techniques include prioritisation and de-prioritisation, promotion and demotion, monetisation and demonetisation (where applicable) and the provision of supplementary information to users, including trigger warnings, alerts and additional content from official and independent authoritative sources. In employing these techniques, internet intermediaries should ensure due transparency, predictability, oversight and safeguards for freedom of expression.

1.6. **Focus on processes**. Regulation and co-regulation should focus primarily on the processes through which internet intermediaries rank, moderate and remove content, rather than on the content itself.

1.7. **User empowerment**. Regulatory, co-regulatory and self-regulatory initiatives should aim to expand users' understanding, choice and control of the impact of digital technologies on their freedom of expression without overburdening them with excessive requirements to safeguard their rights.

1.8. **Protection**. Individuals targeted by potentially damaging types of online expression – for example harassment, bullying and stalking – can suffer substantial harm because of the mass scale, high speed and co-ordination made possible by digital technologies. The victims of these activities should have ample and effective opportunities to report perpetrators and obtain remedies.

1.9. **Human rights impact assessments**. As digital technologies and their uses change constantly, their impacts on freedom of expression should be reviewed regularly. When public and private actors consider intervention that may affect freedom of expression, they should first conduct and publish a human rights impact assessment. If that impact assessment concludes that the proposed intervention poses risks to human rights, it should also include concrete measures to prevent or mitigate such risks.

1.10. **Privacy**. Private actors and States can curtail individuals' right to privacy and informational self-determination by employing sophisticated surveillance and algorithmic persuasion strategies. Any activities by public and private actors should conform with Article 8 of the Convention and the existing legal frameworks for privacy and data protection, including Convention 108. States and private actors should furthermore comply with the privacy provisions laid down in Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems and the Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (13 February 2019).

1.11. **Multistakeholder collaboration**. The definition of policies, guidelines and regulations applicable to digital technologies that can have an impact on freedom of expression requires the full participation of governments, parliaments, international organisations, internet intermediaries, the media, civil society, the research community, the expert community and users, taking into account their specific roles and responsibilities. These collaborative processes should be based on a scope and competences that are clearly defined and mutually agreed, on adequate funding, provision of the necessary data by all stakeholders involved, streamlined procedures to close feedback loops and clear recognition of who is responsible for implementing the outcomes. The development of international public policies and governance arrangements should enable the full and equal participation of all stakeholders from all countries, as provided for in the Declaration by the Committee of Ministers on Internet governance principles (21 September 2011).

2. Digital infrastructure design

2.1. The digital infrastructure of communication in democratic societies should be designed to promote human rights, openness, interoperability, transparency and fair competition.

2.2. States and internet intermediaries should enable access to and use of the digital infrastructure under fair, reasonable and non-discriminatory conditions to promote effective competition.

2.3. Internet intermediaries should enable third-party use and access to users under non-discriminatory and fair conditions, including support for data portability and interoperability. The conditions for access and use should not result in user lock-ins.

2.4. State regulation should strengthen competition across all relevant media and communication markets. In addition to enforcing and amending competition law, where necessary, in order to limit concentration in media and communication markets, States should also modernise media concentration policies to take into account the conditions under which the attention of mass audiences is channelled and commercialised and how these processes can shape the opinions of individuals and groups in the public sphere, with a view to enhancing pluralism as a counterbalance to the increasingly concentrated power to shape public opinion.

2.5. States should not use their powers and policies related to competition and media concentration to interfere with the activities of internet intermediaries in ways that restrict freedom of expression and other human rights.

2.6. States should invest in public-service media and maintain regulatory and governance frameworks that ensure that public-service media are independent from political interference, have a clear role and remit, avoid crowding out private competitors and serve all audiences, including younger generations, across all available digital technologies and without discrimination. States should also support private media that demonstrably achieve the same goals without interfering with their editorial independence. This holds particularly true for local and regional media that tend to enjoy a high level of trust and play a vital role in community building and democratic governance.

2.7. States should stimulate the digital transformation of news organisations and promote investment in and development of digital technologies that enhance their capabilities, for example through public support for free and open-source software and infrastructure development.

3. Transparency

3.1. States and regulators should ensure that internet intermediaries generate and publish all necessary data to enable any analyses necessary to guarantee meaningful transparency on how internet intermediaries' policies and their implementation affect freedom of expression among the general public and vulnerable individuals and groups.

3.2. States should assist private actors and civil society organisations in the development of independent institutional mechanisms that ensure impartial and comprehensive verification of the completeness and accuracy of any data made available by internet intermediaries in their transparency measures.

3.3. Internet intermediaries should publish the necessary information in machine-readable format to ensure transparency of their policies at different levels and to pursue different goals, including empowering users, enabling third-party auditing and oversight, and informing independent efforts to counter problematic content online. These transparency requirements should be proportionate to the size, capacity, function and risk level of different internet intermediaries.

3.4. Internet intermediaries should provide adequate transparency in the design and implementation of their terms of service and their key policies, such as information regarding content removal, recommendation, amplification, promotion, "downranking", monetisation and distribution, particularly with respect to their consequences for freedom of expression.

3.5. When internet intermediaries create or significantly update their key policies or terms of service, they should engage in open, transparent and meaningful consultations with relevant public and private stakeholders. This process should explore the ways in which policies and terms of service affect freedom of expression and other human rights. Internet intermediaries should provide full information on the process, content and outcome of these consultations, disclosing all the feedback they receive and explaining whether and how it is taken into account.

3.6. When there are legitimate concerns that their policies may lead to discrimination, internet intermediaries should provide information that allows independent third parties to evaluate whether their policies are implemented in a non-discriminatory way, including by disclosing the datasets upon which automated systems are trained in order to identify and correct sources of algorithmic bias.

4. Accountability and redress

4.1. States should ensure that any person whose freedom of expression is limited as a result of regulation can access effective redress mechanisms against these restrictions in a simple, accessible and affordable way before the courts.

4.2. States should ensure that any news provider whose editorial freedom is threatened as a result of internet intermediaries' application of their terms of service or content moderation policies is able to seek timely and effective remedies, including being able to access redress mechanisms.

4.3. States should strengthen all relevant regulatory authorities and equip them with adequate resources and expertise so they can effectively monitor the impact of digital technologies on freedom of expression. States should also ensure that internet intermediaries provide the necessary information for these monitoring activities in a timely manner.

4.4. States may, where necessary and particularly in time of public emergency, in accordance with Article 15 of the Convention as interpreted by the European Court of Human Rights in its case law, introduce appropriate and proportionate obligations for internet intermediaries to promote public interest content. Internet intermediaries should offer a higher level of protection for public interest content in ways that should be clear, non-discriminatory and transparently defined.

4.5. When internet intermediaries enforce any restrictions on freedom of expression, they should provide users directly or indirectly affected by such restrictions with clear information on the regulation under which their rights have been limited. Internet intermediaries should also provide timely and effective redress mechanisms that allow the affected individuals to submit an appeal without undue costs, delays or difficulties. To this end, internet intermediaries should offer users clear guidelines on how they can appeal and information on how and when such an appeal would be adjudicated. Internet intermediaries should implement this provision in accordance with the Council of Europe Guidance note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation.

4.6. Internet intermediaries should set up processes and procedures to ensure that information collected from their users' appeals is used to identify and implement necessary improvements of key policies, thus preventing future grievances and harm.

4.7. Within the principles outlined in point 1.1 of these guidelines, in situations where the public is likely to suffer substantial harm from content circulating online, internet intermediaries should remove this content if they have made clear that it is not allowed on their platform. They should also distribute corrections or alerts issued by authoritative institutions as soon as possible and in a manner that ensures that the remedy is commensurate with the likely harm caused, for instance by targeting an audience similar to the one originally affected by the harmful content.

5. Education and empowerment

5.1. States should enhance protection of the privacy and informational self-determination of individuals by enabling users to exercise greater control over the data they generate, the inferences derived from such data and the resulting implications for their user experience. States should require internet intermediaries to clearly inform individuals in advance about the data their algorithmic systems will process, including the purposes and possible outcomes of these operations, and to ensure appropriate interoperability. States should empower users to control their data, including whether and how they are being targeted and profiled. States should ensure that internet intermediaries enable users to easily and quickly modify the parameters of the service to ensure that they are not subject to profiling. This option should be presented prominently and in a neutral manner.

5.2. States should enable all individuals to have access to digital literacy education that helps them to understand the conditions under which digital technologies affect freedom of expression, how information of varying quality is produced, distributed and processed, and the ways in which individuals can protect their rights. States should also support joint educational initiatives by public institutions, international organisations, the media, universities, user groups, civil society actors, internet intermediaries and other stakeholders. Particular emphasis should be placed on the empowerment of vulnerable individuals and groups and those with limited access to quality information.

5.3. Digital literacy programmes should enhance awareness of the kinds of personal data that are processed and/or generated by digital devices, software and applications, the processes and user behaviour that generate them, the ways in which algorithms draw inferences from them, and the purposes for which different public and private organisations employ these inferences to influence the attitudes and behaviour of individuals and groups. Such programmes should also highlight any opportunities users have to exercise control over the ways in which their data are used.

5.4. Digital literacy programmes should be inclusive and informed by rigorous, independent research; they should empower individuals by making them aware of the available redress mechanisms against harm they may suffer as a result of other users' expressions and against any infringement of their freedom of expression.

5.5. Considering the novelty and complexity of many forms of communication enabled by digital technologies, States should promote public debate and empower expert and scientific communities to provide evidence-based guidance on how to distinguish between uses of digital technologies that enable permissible persuasion and uses that entail unacceptable manipulation that encroaches on freedom of expression, particularly as regards self-determination and the ability to hold opinions. The results of these debates should inform public policies and digital literacy programmes.

6. Independent research for evidence-based rule-making

6.1. States should provide adequate funding for rigorous, independent research in the public interest that highlights the individual and societal impacts of digital technologies on human rights, particularly freedom of expression, in different social, political, legal and cultural contexts, with a view to enabling evidence-based analysis, debate and rule-making on these issues.

6.2. While protecting the rights enshrined in Article 8 of the Convention, States should ensure that researchers can access data held by internet intermediaries in ways that are secure, legal and privacy-compliant. Where personal data are necessary for the purpose of research, the principles of proportionality and necessity need to be strictly observed. Research should always respect the right of users to privacy and relevant data protection legislation, have an appropriate legal basis for processing personal data and be conducted in an ethical and responsible way. States should clearly establish what data held by internet intermediaries can be shared with independent researchers. Where this is not specified in statutory frameworks, regulatory authorities should interpret them in a way that safeguards both the right to privacy of users and rigorous, independent research in the public interest.

6.3. Data lawfully collected for other purposes by internet intermediaries may be processed, in compliance with all due data protection safeguards, for the purposes of conducting rigorous, independent research aimed at understanding and addressing the implications of digital technologies for human rights and, in particular, freedom of expression. In accordance with Convention 108, such research, conducted for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, should be understood as fulfilling the public interest requirement when there is no recognisable risk of infringing the rights and fundamental freedoms of data subjects.

6.4. National competent authorities should, in collaboration with researchers and internet intermediaries, create secure environments that facilitate research into the societal and individual implications of the use of digital technology for human rights and, in particular, freedom of expression. National legislation can further specify the processes and conditions for the setting up, maintenance and monitoring of such secure environments. The creation of these environments should be preceded by wide-ranging discussions on how to distinguish between personal and non-personal data; what personal data are to be made available, from what platforms and in what ways; what systems and technologies need to be adopted to protect the integrity of the data shared by internet intermediaries; and how to ensure effective independent oversight of all processing activities, including through enforcement by supervisory and judicial authorities. Researchers operating in these environments are fully responsible for compliance with data protection and other relevant regulations.

6.5. Internet intermediaries should make accurate and representative individual-level data available for independent research on the effects of digital technologies on human rights and, in particular, freedom of expression. Personal data should be shared in compliance with personal data protection laws and the principles of proportionality and necessity, independently of commercial and political influence and based on the principles and safeguards stipulated in Convention 108. Personal data shared for research purposes should be anonymised or, if necessary, pseudonymised using state-of-the-art techniques.

6.6. Researchers should only be allowed to access individual-level data held by internet intermediaries if they have been vetted by an independent scientific institution based on their qualifications and the merits of their projects, are affiliated with a university, have received approval by their university's ethical review board, hold the necessary expertise to analyse and safeguard the data and do not have commercial or political interests that conflict with the research they wish to pursue. Public institutions may set up processes whereby independent research organisations can be periodically accredited so that researchers operating within them can also be granted access to data held by internet intermediaries under the same conditions and with the same safeguards. Public and private actors should incentivise collaboration between researchers affiliated with universities and those working in research institutions, news media and civil society organisations.

6.7. Researchers and their institutions should be jointly and severally liable if they process data shared by internet intermediaries in violation of users' privacy or other provisions of the law. When such joint liability is incompatible with national legislation, States should consider revising their statutes to establish such liability as an additional guarantee of researchers' ethical conduct and institutional accountability.

6.8. To protect researchers' independence, data-sharing agreements between internet intermediaries and researchers should clarify that internet intermediaries cannot interfere with the design, analysis and publication of research based on the data they make available. Where personal data are concerned, such data-sharing agreements shall be in line with Convention 108 and other applicable international data protection standards. Independent scientific institutions and data protection authorities should monitor the implementation of these agreements and adjudicate any disputes.

6.9. Internet intermediaries that provide researchers with access to the data they hold should retain the right to object to any uses of the data they shared that may compromise users' privacy or data protection rights or otherwise violate the law. When they share data with researchers in accordance with applicable law and provide adequate safeguards to protect users' privacy, including additional safeguards for special data categories, internet intermediaries should be immune from liability resulting directly and solely from the sharing of such data.

6.10. States should ensure that internet intermediaries' terms of service do not discriminate against research into the impacts of their services on human rights and, in particular, freedom of expression, at the societal and individual levels, and that researchers who have received approval from an ethical review board or equivalent body cannot be held liable on the grounds that they breached the internet intermediaries' terms of service while conducting their research.