UNDER 35 AND UNDER SIEGE

How Young European Citizens Propose to Combat Disinformation in Democratic Societies

Beatriz Botero Arcila

Assistant Professor of Law at Sciences Po

Florent Parmentier

Secretary-General at CEVIPOF – Sciences Po

Beatriz Botero Arcila is an Assistant Professor of Law at Sciences Po Law School and a Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard University. She holds a master and a doctorate from Harvard Law School where she defended a dissertation on the governance of smart cities and urban platforms and the data they collect. Beatriz's current work focuses on the governance of data and artificial intelligence.

Florent Parmentier, Ph.D, is Secretary-General at CEVIPOF-Sciences Po. He teaches at Sciences Po (foresight and geopolitics) in Paris and University Mohammed VI Politechnics (Rabat, Morocco). He is a research associate at Institut Jacques Delors, Center of Geopolitics of HEC Paris and GMF Paris. Founder of the website Eurasia Prospective, Florent's current works include European geopolitics in various fields.

INTRODUCTION

Disinformation has become a pervasive and critical threat to the integrity of democratic processes worldwide, particularly elections. Disinformation is generally defined as "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."[1] Note that this definition excludes forms of speech that are already illegal and can be acted against, such as hate speech or defamation.[2] As the deliberate spread of false or misleading information, disinformation is often weaponized to destabilize political systems by undermining trust in electoral outcomes, deepening polarization, and exacerbating social divisions. Recent research emphasizes how electoral disinformation is strategically deployed to delegitimize the democratic process, creating fertile ground for political and social instability.[3]

*A growing trend in the disinformation landscape is the transformative role of artificial intelligence (AI), which has the potential to enhance the scale, speed, and sophistication of disinformation campaigns while lowering their cost. The evolving use of AI requires careful analysis to understand its potential to manipulate public discourse. A growing body of literature is dedicated to the risks associated with AI-powered disinformation and potential control and mitigation mechanisms.[4] However, **while disinformation poses a global challenge, its manifestations are shaped by local political, informational, and cultural contexts.** In countries with varying levels of democratic consolidation, such as France, Germany, Romania, and Moldova, the specific nature of disinformation and the corresponding policy solutions differ significantly.*

This paper builds on a broad consultation carried out by Make.org and the SciencesPo Tech & Global Affairs Innovation Hub, with support from NATO and Microsoft, between May 15 and June 20, 2024, during which 7,865 participants from France, Germany, Moldova, and Romania responded to the question: "What are your ideas for protecting democracies from disinformation (e.g., fake news, AI, influence attempts)?"[5]

Beyond the [high-level summary of the results](#), the data collected through this consultation offers valuable insights on the different perceptions of the negative impacts of disinformation across various countries. Putting these results in perspective with the most current research in law and political science, this policy brief highlights how tailored strategies can be developed to address disinformation within distinct democratic settings.

1. DISINFORMATION: A GLOBAL CHALLENGE WITH LOCAL VARIATIONS

Disinformation has emerged as a global challenge, threatening democratic systems by undermining trust in institutions, amplifying political polarization, and influencing public debates and electoral processes. However, while disinformation is a global issue, its manifestations differ significantly depending on the local political, social, and informational ecosystems. The varying media landscapes, historical contexts, and levels of public trust in institutions across countries like France, Germany, Romania, and Moldova contribute to these distinct patterns.

All four countries face specific challenges related to **external influence, political polarization, and public mistrust**. They are frequently targeted by disinformation campaigns driven by internal actors and political forces with illiberal ideologies. The latest sometimes work closely with external actors, particularly Russia, which seeks to destabilize political systems and weaken European Union (EU) and Western solidarity. Russia's influence is particularly prominent in disinformation campaigns aimed at eroding support for EU integration, NATO, and Western alliances, a trend seen across multiple electoral cycles in these countries.
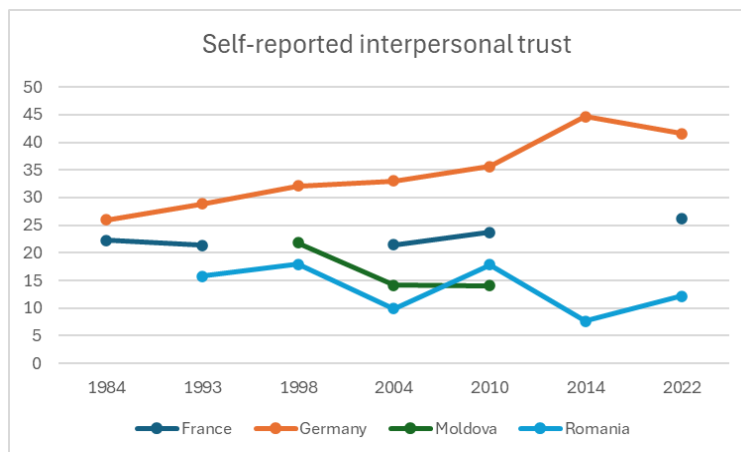

Table 1: Self-reported interpersonal trust (Share of people agreeing with the statement "most people can be trusted")
Data source: Integrated Values Surveys (2022), from Esteban Ortiz-Ospina, Max Roser and Pablo Arriagada (2016) - "Trust", OurWorldinData.org | CC BY

2024: A Pivotal Year for Elections

2024 has been a defining year for elections worldwide, with significant disinformation campaigns targeting several critical electoral events in Europe. In **June 2024**, France, Germany, and Romania participated in the **European parliamentary elections**, and **October/November 2024** marked the **Moldovan presidential elections** and a referendum on **EU integration**. During these elections and the campaigns leading up to them, disinformation focused heavily on divisive topics such as **immigration** and **national identity**, particularly in France[6] and Germany.[7] In both countries, national and international security as well as immigration have been a polarizing issue, and disinformation has sought to amplify these divisions by portraying migrants as threats to national security and identity

or by spreading false information on the involvement of each country in the war between Russia and Ukraine.

In **Romania**, disinformation campaigns took a different form, focusing on **undermining public trust** in political institutions such as the government, judiciary, and media. These campaigns often play on narratives of corruption and dysfunction, aiming to weaken citizens' belief in democratic governance. According to the EU Disinfo Lab, for at least 5-7 years, there has been a growing 'sovereigntist' movement (bridging nationalism and populism) that is the main drive behind disinformation, pushing mostly anti-Western narratives.[8] In this perspective, Romania is overly influenced by Western powers, suggesting it acts more as a subordinate rather than an independent nation, implying that Romania's political and economic decisions are heavily guided by EU and NATO policies, potentially at the expense of its national interests. As Romania heads toward its **November/December 2024 presidential elections**, the impact of these narratives is likely to intensify, further challenging the integrity of its political landscape.

Meanwhile, **Moldova,** according to the RSF ranking**, has shown notable improvement** in recent years due to efforts to increase media independence**.** However, it presents a unique case where **linguistic and ethnic divisions** between the Romanian-speaking majority and the Russian-speaking minority are exploited. Disinformation campaigns have often targeted **President Sandu's pro-European stance**, portraying it as a threat to Moldova's sovereignty and cultural identity. In **Gagauzia**, a Russian-speaking autonomous region, disinformation amplifies ethnic and linguistic divisions, promoting pro-Russian sentiment and opposition to EU integration.[9] Meanwhile, **Ilan Shor**, a fugitive politician and businessman with close ties to Russia, has been accused of orchestrating disinformation campaigns to undermine the government, often using media and social networks to mobilize anti-government protests and challenge democratic reforms.[10] Russia has been particularly active in promoting disinformation to undermine Moldova's pro-EU movements, especially in the lead-up to the **presidential election and EU referendum**. Russian-backed narratives emphasize the risks of EU integration, often framing it as a loss of national sovereignty or a threat to the Russian-speaking minority, thereby deepening the country's internal divisions in the context of the war in Ukraine.[11]

Media Landscapes and Disinformation Channels

A country's media environment plays a critical role in how disinformation spreads and is countered. France and Germany both benefit from relatively **strong and diverse media landscapes**, where traditional media outlets still enjoy a credible level of independence and pluralism, retaining significant influence. However, despite the strength of these media ecosystems, political polarization and the rise of social media platforms have allowed disinformation to flourish. In these countries, disinformation spreads not only through mainstream media but also through **public social networks** and **private messaging channels**, which, until now, have largely escaped regulatory scrutiny.

World Press Freedom Index
Score & Global Ranking 2024

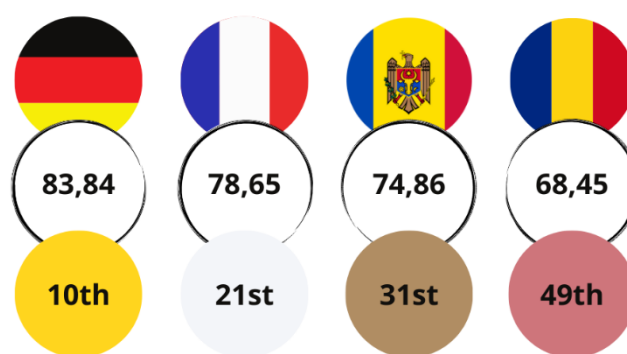|			
🇩🇪	🇫🇷	🇲🇩	🇷🇴
83,84	78,65	74,86	68,45
10th	21st	31st	49th

Table 2: World Press Freedom Index scores and global rankings for Germany, France, Moldova and Romania in 2024.

Data source: Reporters Without Borders World Press Freedom Index

In contrast, despite the absence of strong cultural, historical, or economic relations to Russia, the **Romanian media landscape** is more vulnerable to both domestic and foreign disinformation. Local oligarchs and external actors wield significant influence, creating an information ecosystem where disinformation thrives. Romania is ranked 34th in the European Media Literacy Index 2023, falling within the 4th cluster, which includes countries with problematic performance in media literacy.[12] This has made Romania particularly susceptible to both **internally-generated disinformation** (focused on corruption and political disillusionment) and **externally-driven narratives** aimed at weakening ties with the EU and NATO.

Moldova's media environment is the most **fragmented** of the four, heavily influenced by **external sources**, particularly **Russian-language media**. Russian media channels are widely consumed by Moldova's Russian-speaking population, making it challenging for local media to counteract disinformation narratives that promote anti-Western sentiment. Moreover, the weakness of Moldova's domestic media infrastructure leaves it highly vulnerable to **foreign disinformation**, which is disseminated not only through traditional media but also through **private communication platforms**, including encrypted messaging apps, which are difficult to regulate.[13]

Beyond Media Landscapes: The Role of Social Networks, Messaging Apps and AI

In all four countries, disinformation is increasingly spread via **public social networks** and **private messaging channels**. These platforms help in forming niche communities where people with similar language and interests can interact, share ideas, and support each other. But it also provides a fertile ground for the rapid and unregulated spread of disinformation.

While social media platforms like Facebook and Twitter allow for mass dissemination, **private messaging services** such as WhatsApp and Telegram pose a unique challenge because they operate outside the purview of traditional content moderation systems. This shift toward more private communication spaces has also made disinformation harder for

governments and organizations to track and counter disinformation effectively, highlighting the need for new regulatory approaches. Young Europeans, who tend to use digital platforms tailored to their preferences, could be particularly vulnerable to echo chambers and biased information. The Make.org consultation emphasizes the importance of early education to combat disinformation, advocating for programs that teach young people to recognize and verify fake news. This includes integrating media literacy into school curricula, focusing on foundational concepts of information, critical thinking, and political awareness to equip students with the skills to navigate and assess information independently. Additionally, the consultation underscores the need to educate young citizens on identifying AI-generated content, encourage clear labelling of AI-produced media, and promote a more inclusive, transparent vision of AI in society to help audiences understand both its potential and risks.

In this context, AI plays a dual role in shaping the spread of disinformation on social networks and messaging apps.[14] On the one hand, it amplifies and refines the spread of false information by lowering the cost of mass-creation of convincing synthetic content, including new disinformation vectors such as deepfakes, facilitating the deployment of both networks and micro-targeting.[15] On the other hand, AI offers potential solutions in detecting and mitigating disinformation, although the ever-evolving sophistication of AI-driven disinformation techniques continually challenges these defenses.

AI technologies continue to pose significant risks in 2024, particularly through AI-generated text, which many platforms still fail to address in their policies. In the lead-up to Moldova's October referendum, President Maia Sandu has faced an unprecedented wave of Russian AI-driven disinformation, aiming to sway public opinion through strategically tailored narratives.[16] This negligence is highlighted by recent disclosures from companies like OpenAI about the use of their tools in influence operations.[17] Platforms often rely on vague statements and place the burden of responsibility on users or the AI industry, rather than implementing robust self-detection measures.[18]

2. COMBINING COORDINATED LEGAL APPROACHES AND TAILORED POLICY RESPONSES TO FACE DISINFORMATION ACROSS CONTEXTS

Over the past years, different actors ranging from tech companies to national governments and international organisations have started adopting new strategies to address the challenges of the spread of disinformation on social media. This section mainly discusses the main regulatory and policy approaches used now to address disinformation, to then move to the discussion of recommendations.

Legal and policy responses to face disinformation online cut across two main regulatory frameworks: the guarantee of freedom of expression online and the regulation of social media.

Content moderation and intermediary liability

The baseline regime of content regulation online is known as intermediary liability, which at its core establishes that intermediary services, such as social media, have an immunity for liability for hosting illegal content, under the condition that they do not participate in its production and that they remove illegal content when they are made aware of it. This regime was first introduced by the E-Commerce Directive (ECD) in 2000 and was fully replaced in 2022 by the Digital Services Act (DSA) which came into force in 2024. With this partial immunity, intermediary liability law aims to foster the development of the online ecosystem while enabling companies to go beyond legal minimums. These intermediaries can shape their online environments by setting their own content standards through their terms of service and community guidelines, extending beyond basic legal requirements.[19]

The DSA, as the ECD did before, defers to national law and other EU regulations to define what is illegal content - which platforms must remove expeditiously when made aware of it. Under EU law, illegal content includes child sexual abuse material, hate speech, terrorist content and intellectual property infringement.[20] At the national level, criminal codes and other rules often forbid additional kinds of speech and content. In fact, the definition of disinformation as information that is disseminated to intentionally cause harm or for profit, overlaps with existing legal categories of forbidden speech, such as defamation or false advertising. Nevertheless, several countries in Europe have recently passed broader legislation that criminalises the dissemination of false information, with complicated implications for freedom of expressions, as we discussed in the next section.[21]

Freedom of expression as a limit to the direct regulation of disinformation

Because disinformation necessarily implies speech, laws and policies that aim to tackle disinformation directly implicate the right to freedom of speech and information, protected in Europe by Article 11 of the European Charter of Fundamental Rights. Different countries and legal cultures have more tolerance to the limitation of freedom of expression to safeguard other public interests - such safety. In general, however, limitations on freedom of expression are always examined with care and are narrowly defined.

Particularly important for the purposes of regulating disinformation is the fact that, under European fundamental rights law, information that is misleading or false - thus, the type of content that characterises misinformation[22] - is by definition not illegal content. In *Salov v. Ukraine*, for example, the European Court of Human Rights explained: 'Article 10 of the Convention as such does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful. [This] would deprive persons of the right to express their views and opinions about statements made in the mass media, and would thus place an unreasonable restriction on the freedom of expression.'[23]

Nevertheless, countries have started passing regulations to prohibit disinformation. France, for example, has passed regulation that penalises the dissemination of information that "threatens public order."[24] Somewhat similarly, Germany's Network Enforcement Act, or NetzDG, did not adopt new criminal offences but increased the platform's liability for not removing hateful content swiftly enough.[25] Poland has passed regulation that allows political

candidates to apply for an expeditious judicial order that restrains the publication of information that contains "untrue data or information" and to prohibit its further distribution.[26]

Moldova and Romania are also not exempt from this trend: a 2023 cybersecurity law issued in Romania includes as a list of threats to national security "disinformation and propaganda campaigns that might affect the constitutional order."[27] Because these regulations are rather vague and broad, civil society organisations have raised concerns about their inevitably overinclusive nature and their potential impact on freedom of expression. Indeed, there is no definition offered for the threats listed in the law, which broadly enables intelligence services to take discretionary actions.[28]

Similar concerns have been raised in Moldova, where, in 2023, an amendment to the Code of Audiovisual Media Services introduced disinformation as "the intentional dissemination of verifiably false or misleading information created to harm national security" and forbade media providers from distributing such content. The rule has also been criticised by civil society for potentially disproportionately limiting freedom of expression.[29]

There is, indeed, a tricky conundrum in the question on how to regulate and address the real risks and challenges of disinformation without curtailing legal and legitimate speech. At the same time, it is legitimate to combat content that undermines democratic processes. The key challenge, however, may be to identify the second element of the definition of disinformation, mainly the intent to harm or profit so that others' rights and interests are not disproportionately undermined. At the European and regulatory level, however, some new approaches focus more on understanding and addressing how this "how information is produced, how it is distributed, and how people engage with it in the public sphere."[30]

A turn towards risk regulation

The DSA introduced new obligations, especially for the largest platforms, to conduct risk assessments on several systemic risks and to take measures to mitigate them.[31] In particular, some of the systemic risks mentioned in the regulation are "'(a) the dissemination of illegal content through their services; (b) any actual or foreseeable negative effects for the exercise of fundamental rights, in particular the fundamental rights [...] to freedom of expression and information [...]; (c) any actual or foreseeable negative effects on civic discourse and electoral processes, and public security [...].'"[32] The DSA, however, does not apply to private messaging, as they are not information society services as defined by European law, though it may apply to public channels such as Telegram or WhatsApp channels.[33]

Though it is still early in the days of DSA enforcement, these measures will in principle make major platforms less free to determine what their content moderation policies are and how they tackle disinformation, as they will have to consider more holistically how their policies and systems create or contribute to create risks associated with this phenomenon. In doing so, it will make other, previously self-regulatory and co-regulatory experiences and practices mandatory.

Co-regulation

In 2022, for example, major platforms signed a Code of Practice of Disinformation, where they made a series of voluntary commitments to tackle disinformation on several fronts. These commitments included were not limited to content moderation, and rather focused more on actions oriented at addressing 'manipulative behaviour', such as the strategic dissemination of disinformation by, for example, deleting fake accounts, demonetising disinformation, and adopting safe design practices that decrease the viral spread of this type of content.[34] Under the DSA, this type of Code will now have official status, which means that they will be used as a factor to evaluate the risk mitigation obligations under Article 35.

Self-regulation

Similarly, most of the main online platforms have implemented policies to combat disinformation and misinformation by banning and demoting specific activities and content types.[35] However, these efforts have been less effective than desired, not only because policy enforcement is incomplete in practice but also because trust and safety teams have been reported to be insufficiently funded.[36] Additionally, platforms prioritise English-language content and wealthier markets, which raises concerns about moderation in linguistically and culturally minoritarian regions of Europe like Moldova and Romania. The DSA does not address the size or funding of trust and safety teams - and it raises the question on whether increased investment in moderation staff, tools would be an important measure to implement - but still it is expected that the enforcement of the DSA may contribute to address some of these issues.

Disinformation governance, trust and safety and media literacy

In parallel to these different regulatory interventions, it is important to notice that increasingly the governance of disinformation at the platform level is treated less as the management of individual cases that focus on specific types of content, and rather on the systems that underlie it. This approach, known as trust and safety, emphasises the need for *ex ante* regulation of system design rather than *ex post* accountability for individual outcomes. This includes, for example, focusing on the dynamics of the spread of disinformation and the technological features that enable them on a given platform.

Along these lines, thus, transnational policies that emphasised the need of strengthening trust and safety teams and adopting context specific design practices may be amongst the best efforts to prevent, but specifically identify on time and address disinformation in countries like Moldova and Romania.

Similarly, media literacy has become an important policy lever to combat the spread of disinformation and strengthen trust in the media ecosystem. This was, also, one of the main findings of the consultation, as the proposals submitted by Moldovan and Romanian citizens are predominantly focused on media education.

It is important to note, however, that these policies are important but not a silver bullet. In France, for example, media literacy education has a strong tradition, and it is part of school curriculums. Media literacy in France is seen as essential for democracy, but also as an element of broader social policy. The European Digital Media Observatory's data shows that

France is slightly above the European average in internet usage. However, the relationship between media literacy and trust in news is complex. In some studies, researchers have found that increased media literacy leads to lower levels of trust, especially news from search engines and social media.[37] French citizens have a low level of trust in news, which has been related by some actors as related to a rise in conspiracy theories.[38]

Indeed, media literacy programs are not a silver bullet and seem to work best when considered as an element of a broader holistic approach to addressing disinformation. Strategies favoured to enhance trust in the media, for example, are related to enhancing transparency, reduced bias, and improvement alignment of coverage with people's everyday concerns.[39] Similarly, independent fact-checking efforts play an important role, as the visible presence of fact-checking labels and resources on social media can increase public awareness and discourage prominent figures from making false claims. Studies suggest, however, that users are more receptive to fact-checking in countries with strong, non-partisan media institutions. These echoes the findings of the consultation where the respondents from Moldavia and Romania signalled that they would be skeptical of government institutions in charge of fact-checking.

POLICY RECOMMENDATIONS

This brief and the following policy recommendations are inspired by the contributions to the previously mentioned open consultation on disinformation, carried out in France, Germany, Moldova, and Romania.

- **Enhance national media literacy programs prioritising early and continuous media education as a foundational response to disinformation.**

Develop curricula that not only build individual critical thinking and verification skills but also address the underlying distrust in public institutions. Integrating media literacy into educational systems will empower citizens with tools to navigate information independently, fostering a more resilient and informed democratic society. This is true across all of the countries addressed in this paper.

- **Adopt policies and programs that strengthen the independent media ecosystem.**

Support for independent and pluralistic media and civil society organisations can strengthen the local and national media ecosystem, which in turn may strengthen trust and local capacity to counteract disinformation campaigns.

- **Develop frameworks which take into account different national contexts by balancing effective oversight with robust privacy protections.**

Implement **privacy-preserving, decentralised platforms** and transparent mechanisms where governments collaborate with civil society organisations for fact-checking rather than state-determined truth labelling. This approach respects citizens' privacy preferences, especially in countries sensitive to state control, while promoting trusted information ecosystems.

- **Focus policy efforts on identifying the dissemination channels and act on the underlying infrastructures of disinformation.**

Relevant measures may be collaborating with platforms to strengthen content moderation in national languages, and work with the European Commission to address national needs in the framework of the Digital Services Act. In all cases, measures should be designed with national needs and interests in mind, while not infringing disproportionately on freedom of expression rights.

- **Collectively build technical and legal capacity for early detection and moderation of harmful disinformation content**

Building shared innovative, standardised sets of tools (e.g. AI-assisted detection), business practices, and legal remedies could maximise impact while effectively acting as a transfer to countries with more limited resources (financial, technical, ability to pressure Big Tech platforms…). With proper adaptation to local contexts, the common elaboration of tech and legal tools could be a promising mechanism to reinforce democratic societies and enhance regional and global stability.

- **Any measure to counter disinformation must be part of a broader strategy to enhance political communication and public trust**.

In a systemic approach, policies improving trust in governments, media and the scientific community contribute to strengthening resilience to disinformation. This may include the development and adoption of technological tools, including AI-based ones, supporting democratic debate and pluralistic public spaces, even in multi-linguistic settings.

1 De Cock Bunning, M., *A Multi-Dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation*, Publications Office of the European Union, 2018

2 This paper does not explicitly include other forms of information disorders, such as misinformation (false or misleading that is spread without the intent to harm or profit) or malinformation (information that is "based on reality" but taken out of context or exaggerated in a misleading and/or harmful way) either, although AI technologies may impact them (Wardle, C., and Derakhshan, H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe, Strasbourg, 2017).

3 See for instance Shelley Boulianne, Edda Humprecht, "Perceived Exposure to Misinformation and Trust in Institutions in Four Countries Before and During a Pandemic", *International Journal of Communication* 17, 2023, pp.2024–2047

4 Steven M. Williamson, Victor Prybutok, "The Era of Artificial Intelligence Deception: Unraveling the Complexities of False Realities and Emerging Threats of Misinformation", *Information*, 15(6), 2024, pp.1-43

5 Open consultation co-organized by Make.org and SciencesPo Tech & Global Affairs Innovation Hub, with support from NATO and Microsoft. Aggregated results are available here.

6 Chavalarias, David. *Minuit Moins Dix à l'horloge de Poutine*. June 2024. HAL Archives Ouvertes.

7 O'Carroll, Lisa. "Disinformation Networks 'Flooded' X before EU Elections, Report Says" *The Guardian*, July 12, 2024.

8 Dr. Cucu, Ciprian. Disinformation Landscape In Romania. National factsheet for the EU Disinfo Lab, September 2023

9 Ion Cristea, "Republic of Moldova. Presidential elections and Referendum 2024", *New Strategy Center*, October 2024.

10 Necsutu, Madalin. "Fugitive Moldovan Oligarchs Exploit Online Weaknesses to Spread Disinformation Before Elections" *Balkan Insight*, September 10, 2024

11 Denis Cenusa, "Russia's disinformation in Eastern Europe: revealing the geopolitical narratives and communication proxies in Moldova", *Eastern Europe Studies Center*, 2 April 2024

12 Lessenski, Marin. *The Media Literacy Index 2023*. European Policies Initiative (EuPI) of Open Society Institute – Sofia Foundation (OSIS), June 2023

13 Tobias Lemke, Michael W Habegger, "Foreign Interference and Social Media Networks: A Relational Approach to Studying Contemporary Russian Disinformation", *Journal of Global Security Studies*, 7(2), June 2022

14 Bontcheva, Kalina. Generative AI and Disinformation: Recent Advances, Challenges, and Opportunities. Vera.ai Whitepaper, February 2024

15 Kertysova, Katarina. "Artificial Intelligence and Disinformation," *Security and Human Rights*, 29(1-4), 55-81. December 12, 2018.

16 Mark Scott, "Moldova fights to free itself from Russia's AI-powered disinformation machine", *Politico*, 7 May 2024

17 Todd C. Helmus, "Artificial Intelligence, Deepfakes, and Disinformation: A Primer", *RAND Corporation*, 1 July 2022

18 Miguel, Raquel. "Platforms' AI Policy Updates in 2024: Labelling as the Silver Bullet?", *EU DisinfoLab*, July 2024

19 Botero Arcila, Beatriz, and Griffin Rachel, Social Media Platforms and Challenges for Democracy, Rule of Law and Fundamental Rights, study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, April 12, 2023

20 Ibid

21 Ó Fathaigh, R., et al., 'The Perils of Legally Defining Disinformation', *Internet Policy Review*, Vol. 10, No. 4, November 4, 2021

22 False or misleading information that is shared without malicious intent, as opposed to disinformation.

23 Judgement of 27 April 2004 of the European Court of Human Rights, *Salov v. Ukraine*, application no. 65518/01

24 Law n° 2018-1202 of December 22 2018 relative to the prevention of false information

25 Heldt, Amélie. "Germany is amending its online speech act NetzDG… but not only that." *Internet Policy Review*. April 6, 2020.

26 The European Court of Human Rights has since then ruled that a fine issued under the Polish provision, regarding the distribution of a handout that included criticism to members of an outgoing local government, violated Article 10 of the European Convention on Human Rights. See Ronan Ó Fathaigh, Brzeziński V. Poland: Fine Over 'false' Information During Election Campaign Violated Article 10, Strasbourg Observers (August 8, 2019).

27 Asociația pentru Tehnologie și Internet (ApTI), "New Romanian cybersecurity law in force despite heavy criticism", contribution to EDRi (European Digital Rights), May 3, 2023

28 Ibid

29 "Moldova Adopts New Anti-Disinformation Law". *CSO METER*. June 7, 2022 & "Moldova to establish new state body to combat disinformation". *CSO METER*. July 20, 2023

30 European Commission: Directorate-General for Communications Networks, Content and Technology, *A multi-dimensional approach to disinformation – Report of the independent High level Group on fake news and online disinformation*, Publications Office, 2018

31 DSA, Art. 34 and 35

32 DSA, Art. 34

33 *See* DSA, recital 14. "The concept of 'dissemination to the public', as used in this Regulation, should entail the making available of information to a potentially unlimited number of persons (...) such as emails or private messaging services, fall outside the scope of the definition of online platforms as they are used for interpersonal communication between a finite number of persons determined by the sender of the communication. However, the obligations set out in this Regulation for providers of online platforms may apply to services that allow the making available of information to a potentially unlimited number of recipients, not determined by the sender of the communication, such as through public groups or open channels."

34 European Commission, '2022 Strengthened Code of Practice on Disinformation', Policy and Legislation, June 16, 2022. See also Botero & Griffin

35 Keller, T., et al., ''Coordinated Inauthentic Behaviour' And Other Online Influence Operations In Social Media Spaces', *AoIR Selected Papers of Internet Research*, October 5, 2020; Krishnan, N., et al., 'Research Note: Examining How Various Social Media Platforms Have Responded to COVID-19 Misinformation', *Harvard Kennedy School Misinformation Review*, December 15, 2021

36 Silverman, C., Mac, R., Dixit, P., "'I Have Blood On My Hands': A Whistleblower Says Facebook Ignored Global Political Manipulation", *BuzzFeed News*, September 14, 2020
Scheck, J., Purnell, N., Horwitz, J., "Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak, Documents Show", *Wall Street Journal*, September 16, 2021
Dwoskin, E., Menn, J., and Zakrzewski, C., "Twitter can't afford to be one of the world's most influential websites", *Washington Post*, 4 September 2022

37 Fletcher, Richard. "The Impact of Greater News Literacy" *Reuters Institute Digital News Report*, 30 May 2018

38 See the European Digital Media Observatory (EDMO) page dedicated to media literacy in France

39 Banerjee, Sayan, et al. *Strategies for Building Trust in News: What the Public Say They Want across Four Countries*. Reuters Institute for the Study of Journalism, 2023.