CELE
Centro de Estudios en Libertad de Expresión

Documento de posición

26

Submission in response to the Call for Evidence in connection with the development of the European Democracy Shield

CELE

May 25, 2025

CELE, "Submission in response to the Call for Evidence in connection with the development of the European Democracy Shield", Documento de posición No. 26 (ESP), Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2025).

Facultad de Derecho

Centro de Estudios en Libertad de Expresión

UP
Universidad de Palermo

CELE's Submission in response to the Call for Evidence in connection with the development of the European Democracy Shield

Nicolás Zara

CELE/UP

cele@palermo.edu

May 25, 2025

Introduction

The Center for Studies on Freedom of Expression and Access to Information (CELE) is an academic research center affiliated with Universidad de Palermo in Argentina. The Center provides technical and legal analysis on issues affecting this fundamental right, and since 2012 has been studying freedom of expression on the Internet as a specific research area. The Center is a leading voice on the promotion and protection of freedom of expression nationally, regionally, and internationally.

This submission was prepared in response to the Call for Evidence for the development of the European Democracy Shield. It aims to provide a critical assessment of the initiative, with an analysis that emphasizes freedom of expression.

The Call for Evidence

The Call for Evidence for the establishment of a European Democracy Shield contains a diagnosis on the current status of democracy in the European Union. It expresses the need, based upon such a diagnosis, to take action against some threats that purportedly threaten its existence. However, it is worded in significantly vague terms, and it offers few hints of what the next steps could be concerning the concrete policies that could be implemented in the framework of the Democracy Shield.

The Call for Evidence starts by underscoring the centrality of free expression and the free flow of information in healthy democracies. It states that European democracies face significant challenges, including "a rise in the number of threats from internal and foreign actors taking various forms, including foreign information manipulation and interference and disinformation, as well as threats to the integrity of elections and democratic processes, such as cyber-attacks, covert political funding or manipulated boosting of specific political content, actors or parties online"[1].

The proposal indicates that it is aimed to tackle "the increasing threats to democratic institutions, systems and processes within the EU and the context in which they operate, both at national and EU level, which, compounded, contribute to the overall decrease of citizens' trust in democracy"[2]. It refers to a context of "changes in the global information ecosystem"[3], which gives rise to new ways of "fostering new freedoms and opportunities" and "makes it easier for hostile actors, both internal and foreign, to manipulate information and step up information warfare"[4]. This threats acquire a hybrid form which includes, as per the same document, "cyber, disinformation, online and offline influence campaigns"[5].

The European Commission proposes four axis to address the problematics referred to: (a) countering disinformation and foreign information manipulation and interference, (b) ensuring the fairness and integrity of electoral processes and the strengthening of democratic frameworks and checks and balances, including free, plural and independent media and civil society organisations, (c) strengthening societal resilience and preparedness (including digital and media literacy, critical thinking, etc.), and (d) fostering citizens' participation and engagement. This response will focus on the first of those.

Filling the gaps

Given the lack of precision in the text of the consultation, context is of the essence to predict the content of the policies that could potentially be adopted under the proposed framework. The idea of a "Democracy Shield" for Europe was first introduced by the President of the European Commission, Ursula Von der Leyen, at the Democracy Summit of

[1] Call for Evidence for the establishment of an European Decmocracy Shield, Section "A. Political context, problem definition and subsidiarity check".

[2] Id.

[3] Id.

[4] Id.

[5] Id.

May 2024 in Copenhagen, Denmark. In her speech in such occassion[6], she emphasized about the need for Europe to set up "its own dedicated structure on countering foreign interference", in the face of "the rise of foreign interference and manipulation in our societies, our democracies and our elections", including "swarms of negative disinformation targeting different issues and individual candidates" in the weeks before her speech. This includes not only "fakes or fabricated content" but also "buying influence and causing chaos", politicians "selling their souls on Russian propaganda outlets and videos" and "malicious cyber-attacks". All of the above with the intent of "divide [European] societies from within".

In her Political Guidelines for the European Commission, President Von Der Leyen stated that the goal of this project would be to "increase situational awareness, by detecting, analysing and proactively countering disinformation and information manipulation", to counter "foreign information manipulation and interference online".[7]

Speaking to the European Parliament on July 2024, Von der Leyen further addressed the Democracy Shield. She highlighted the "urgent need to provide the European Union with powerful cyber-defence tools, to impose transparency on foreign funding of our public life as a common rule, but also to guarantee a reliable information framework". In that occasion, she added that this new structure would need to have the ability to "act and impose sanctions"[8]. She added that "for this, the EU must support an independent press, continue to ensure rules are observed by digital giants, and further encourage media literacy programmes"[9].

A note on FIMI and "information warfare"

Countering the threat of foreign information manipulation and interference (FIMI) seems to be the main goal of the European Democracy Shield. According to the European External Action Service (EEAS), FIMI "describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and

[6] Speech by Ursula Von der Leyen at the Democracy Summit 2024, video recording available here.

[7] Von der Leyen, "Europe's Choice: Political Guidelines for the Next European Commission (2024-2029)", Strasbourg,

[8] Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024-2029, available here

[9] Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024-2029, available here

coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory"[10].

In the foreword to the 3rd EEAS report on FIMI, Kaja Kallas, the European Union High Representative for Foreign Affairs and Security Policy, referred to the European information space as "a geopolitical battleground".[11] She described how "foreign actors use FIMI to manipulate public opinion, fuel polarisation, and interfere with democratic processes within the EU and worldwide. The aim is to destabilise our societies, damage our democracies, drive wedges between us and our partners and undermine the EU's global standing". Relevantly, she distinguished FIMI operations from the mere dissemination of deceptive narratives by foreign governments, as she considers the former as "an integral part of military operations used by foreign states to lay the way for kinetic action on the ground".

The definition of FIMI used by the EEAS encompasses both expressive and non-expressive activity, legal and illegal activity or expression, and both State action (or action by privates ultimately attributable to a State) and non-State action. The definition is no more specific when referring to the substance of these actions: it includes any action that threatens and can negatively impact values, procedures, or political processes. Under this conceptualization, virtually anything could be considered Foreign Information Manipulation & Interference.

This is aggravated by the utilization of war metaphors in the public discourse in support of State-led and State-mandated interventions in the public sphere. For instance, in a 2023 document intended to guide VLOPs/VLOSEs on how to comply with their risk mitigations under the Digital Services Act, the European Commission expressed their worries about the increase of "Kremlin-aligned social media accounts" and referred to those as part of

[10] European External Action Service, 1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked Defence, February 2023, available at https://docs.google.com/document/d/1UmhUU7sL22iaVyOGTKu2g6XMt9QmL4Sd7xLgEe_C-jA/edit?tab=t.0, page 4

[11] Kaja Kallas, Preface, in European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference: Exposing the Architecture of FIMI operations, March 2025, available at https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf, page 2

"Russia's information warfare" [12][13]. The Commission observed that "disinformation is only one weapon in the Kremlin's information warfare arsenal. The Kremlin's operations on online platforms often build on other inflammatory or deceptive content, and a range of malign behaviours designed to silence opponents and suppress the truth about the war in Ukraine"[14]. Likewise, Vice-President Kaja Kallas referred to the "weaponisation of information by autocratic governments"[15] and argued that "the novelty of this years' report is the exposure of massive digital arsenals put in place specifically by Russia and China to conduct their FIMI operations"[16].

Article 11.1 of the European Charter of Fundamental Rights and Article 10.1 of the European Convention on Human Rights define Freedom of expression in identical terms, as "the freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers"[17]. Likewise, Article 19(2) of the ICCPR protects the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers"[18]. Accordingly, the State cannot make any difference in the treatment

[12] European Commission - Directorate-General for Communications Networks, Content and Technology, "Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns", 2023.

[13] It was called to our attention that Barata and Calvet Bademunt noted that, even though this document is attributed to DG CNECT in the EuCom website, according to the New York Times, it was "prepared" by the nonprofit Reset. See Joan Barata and Jordi Calvet Bademunt, The European Commission's Approach to DSA Systemic Risk is Concerning for Freedom of Expression, Tech Policy Press, October 2023, available at https://www.techpolicy.press/the-european-commissions-approach-to-dsa-systemic-risk-is-concerning-for-freedom-of-expression/ and Steven Lee Myers, E.U. Law Sets the Stage for a Clash Over Disinformation, The New York Times, September 2023, available at https://www.nytimes.com/2023/09/27/technology/disinformation-law-european-union.html?smid=nytcore-android-share.

[14] European Commission - Directorate-General for Communications Networks, Content and Technology, "Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns", 2023.

[15] Kaja Kallas, Preface, in European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference: Exposing the Architecture of FIMI operations, March 2025, available at https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf, page 2

[16] Kaja Kallas, Preface, in European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference: Exposing the Architecture of FIMI operations, March 2025, available at https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf, page 2

[17] European Charter on Fundamental Rights, Art. 11.1, European Convention on Human Rights, Art. 10.1. Underlining added by the author.

[18] International Covenant on Civil and Political Rights, Article 19 (2). Underlining added by the author.

it gives to a speaker of a piece of information depending on its origin. Therefore, mandating platforms to "mitigate" expressions of certain speakers because they are "Kremlin-aligned" (not even affiliated) or "supress the truth about the war in Ukraine" should be considered off-limits. European citizens have the right to decide for themselves what the truth is in matters of public concern, a process that can only happen if the State lets information flow freely. This includes not only refraining from curtailing the spread of legal expression by itself, but also not using third parties as proxies to do so—for instance, internet platforms through the Digital Services Act, which is a part of the European "FIMI Toolbox"[19]-. Paternalistic interventions in the public sphere lead to a less informed citizenry, more vulnerable to falling for disinformation operations.

The utilization of war metaphors does not make restrictions on the free flow of information any more legitimate, and raises substantial risks of abuse. While using metaphors "allows us to understand one aspect of a concept in terms of another, it also "hides" other aspects of the concept that are inconsistent with them"[20]. In this case, the mere fact that a piece of expression or campaign can be traced back to an authoritarian regime or to the government of a country that is at war with a European Union ally does not automatically render any action associated with it as illegal or a direct attack on democracy.

On top of that, the mere invocation of the protection of national security does not give the state carte blanche to limit access to information under Article 10 (2) of the European Convention on Human Rights[21] or Article 19 (3) of the ICCPR[22]. This is not to say that

---

[19] European Union External Action Service, Second EEAS Report on Foreign Information Manipulation and Interference (FIMI) threats, January 2024, p. 13, available at https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

[20] Matías Gonzalez Mama, On the Metaphor of Social Media as a Public Forum in the United States (July 01, 2024). CELE Research Paper No. 60, Available at SSRN: https://ssrn.com/abstract=5158664 or http://dx.doi.org/10.2139/ssrn.5158664

[21] The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

[22] The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by

there could be no legitimate restrictions, but rather that under both instruments, any measure imposed on European citizens that impairs in any way their ability to access information must be legal, necessary, and proportionate.

For the European Court of Human Rights, under the legality test, any restriction to freedom of expression must be "formulated with sufcient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail"[23]. The ICCPR adopts a similar standard[24]. The imprecise definition of FIMI used by the EEAS does not withstand the legality test and, as a result, cannot be used as a basis for any restriction on freedom of expression or the free flow of information.

Even when a given restriction can be traced to the persecution of a legitimate end, International and European Human Rights law require that it is proven necessary. At the same time, it must be the least restrictive means possible, and commensurate with its purported aim[25]. In a case regarding expression by the leader of a proscribed organization, the European Court of Human Rights held that the identity of the speaker does not justify interfering with their freedom of expression[26].

A note on information integrity

According to a briefing by the European Parliamentary Research Service, "the broad concept of information integrity falls within the scope of the evolving European democracy shield idea"[27]. This project "links existing work to counter foreign information manipulation and interference (FIMI) with the implementation of key legislation and initiatives to boost the health of the information sphere. This includes regulation of online platforms and search

---

law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

[23]European Cout of Human Rights, The Sunday Times v the United Kingdom (no 1) [1979] ECtHR 6538/74, par. 49.

[24] Human Rights Council, 'General Comment No. 34 on Article 19 of the ICCPR' (2011) CCPR/C/GC/34, par. 25

[25] European External Action Services, EU Guidelines on Freedom of Expression Online and Offline, p. 6, available at https://www.eeas.europa.eu/sites/default/files/09_hr_guidelines_expression_en.pdf

[26] European Court of Human Rights, Sürek and Ozdemir v. Turkey, [nos. 23927/94 and 24277/94], par. 61.

[27] EPRS | European Parliamentary Research Service, Information integrity online and the European democracy shield, December 2024, p. 2., available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767153/EPRS_BRI(2024)767153_EN.pdf

engines in the Digital Services Act (DSA), including the 2022 strengthened code of practice to make online platforms do more to curb information manipulation and hate speech, and the work of the European Digital Media Observatory (EDMO) and its regional hubs. It also includes the AI Act, with its risk-based approach to regulating AI, including generative AI-facilitated information manipulation such as deepfakes, the European Media Freedom Act, and the Regulation on Transparency and Targeting of Political Advertising"[28].

As the document acknowledges, while information integrity "is not a fixed analytical framework, and still lacks a clear definition"[29], in the context of the European External Action Service there is a specific team dedicated to Information Integrity and Countering Foreign Information Manipulation and Interference under the orbit of the European External Action Service[30]. The Second report on FIMI[31] by the European External Action Services (SG.STRAT) follows the definition of information integrity given by the Global Declaration on Information Integrity Online, and therefore conceptualizes it as "an information ecosystem that produces accurate, trustworthy, and reliable information, meaning that people can rely on the accuracy of the information they access while being exposed to a variety of ideas. [The] term "information integrity," [can] offer a positive vision of a broader information ecosystem that respects human rights and supports open, safe, secure, prosperous and democratic societies" [32]. It also refers to the United Nations Policy Brief "Information Integrity on Digital Platforms", which states that "information integrity

[28] EPRS | European Parliamentary Research Service, Information integrity online and the European democracy shield, December 2024, p. 2., available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767153/EPRS_BRI(2024)767153_EN.pdf

[29] EPRS | European Parliamentary Research Service, Information integrity online and the European democracy shield, December 2024, p. 2., available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767153/EPRS_BRI(2024)767153_EN.pdf

[30] EPRS | European Parliamentary Research Service, Information integrity online and the European democracy shield, December 2024, p. 2., available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767153/EPRS_BRI(2024)767153_EN.pdf

[31] European Union External Action Service, Second EEAS Report on Foreign Information Manipulation and Interference (FIMI) threats, January 2024, p. 13, available at https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

[32] Government of the Netherlands (September 2023) Global Declaration on Information Integrity Online. Diplomatic Statement. https://www.government.nl/documents/diplomatic-statements/2023/09/20/globaldeclaration-on-information-integrity-online

refers to the accuracy, consistency and reliability of information. It is threatened by disinformation, misinformation and hate speech"[33].

While these definitions emphasize different aspects (the one provided by the Global Declaration focuses on a "positive vision" of the information ecosystem, and the one in the UN brief adopts a more "negative" perspective centered on the threats), they have one common feature: they are both concerned by the accuracy and reliability of the information that the people can access online. We believe this is not a useful nor human rights-abiding framework to approaching phenomena like disinformation and election integrity. Truthfulness is not a relevant criterion to determine whether a piece of expression is protected under Human Rights Law. "Disinformation", "unreliable information" and "untrustworthy information" are labels that encompass both legal and illegal expression. Therefore, the new framing of old problems under the incipient "information integrity framework" does not provide any additional reason for state intervention.

Conclusion

Given the scarce information provided in the consultation materials, it is hard to predict what the concrete initiatives comprised within the European Democracy Shield will be. The diagnosis presented by the consultation document is that European democracy is threatened by the coordinated action of foreign authoritarian governments—mainly Russia and China—and private "bad actors" acting as their proxies, intending to manipulate public opinion and tilt it against the European Union and more generally against democracy. This is consistent with prior declarations by high European officials. However, we believe that some of these assertions lack concrete foundations.

These activities are included within the novel category of FIMI (Foreign Information Manipulation and Interference), which comprises all sorts of legal and illegal actions, performed by both public and private agents, both from within and beyond the borders of the EU, with a "manipulative intent". We believe that the definition of FIMI, while perhaps useful for defense or intelligence purposes, is dangerous if taken as a legal category, since virtually any critique of the European Union or the governments of member states could be framed within that definition. Therefore, it cannot be used as the basis for curtailing rights.

---

[33] United Nations, Our Common Agenda, Policy Brief 8: Intormation Integrity on Digital Platforms, June 2023, available at https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrityen.pdf

Moreover, foreign interference must be demonstrated: calling out "bad actors" or pinning certain behaviour to authoritarian governments does not exempt their expression from the protection of Freedom of Expression. In that sense, past experience of governing reacting to the anxiety of an external threat, real or perceived, should bring caution to any attempt to invoke national security grounds to restrict one of the most important rights in a democratic society.

Likewise, the "information integrity" framework does not provide any meaningful guide for the State to distinguish between acceptable and unacceptable restrictions to the free flow of information. In the context of this consultation, it rather looks like a new framing for the classic phenomenon of restrictions on freedom of expression during wartime, except that this time, no state in the European Union is at war. The utilization of war metaphors by high officers of the European Union should not obscure this fact.

According to the European Court of Human Rights, "freedom of expression constitutes one of the essential foundations of a democratic society, one of the basic conditions for its progress and for the development of every person"[34], and "it is applicable not only to "information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population"[35]. Restricting access to information under the patronising premise that public opinion can be manipulated goes against the basic tenets of liberal democracies, which rest on the capacity of citizens to judge and decide by themselves about the truthfulness or falsehood of political expression. Any action taken by the EU under the Democracy Shield framework that does not comply with the three-part test for restrictions upon freedom of expression is self-defeating. It undermines the very essence of democracy and creates less-informed citizens, with less capacity to identify and critically evaluate falsehoods and disinformation.

[34] European Court of Human Rights, Handyside v. The United Kingdom, [5493/72], ECtHR 5493/72, par. 49.
[35] Id.