Utrecht Law Review

The EU's Arsenal to Protect Its Democracy from the Threat of Foreign Disinformation

ARTICLES

ANNA FIORENTINI

ABSTRACT

Democracy relies on the existence of a well-informed and pluralistic public debate, yet the digital transformation of the information environment has rendered democratic processes increasingly vulnerable. The proliferation of online disinformation – especially when orchestrated by foreign actors – poses a direct threat to the integrity of democratic decision-making and the rule of law within the European Union (EU). This paper critically examines the EU's evolving legal and policy framework to counter such hybrid threats, focusing on the interplay between internal market regulation and instruments of external action. It first analyses the extent to which key legislative measures – namely the Digital Services Act, the European Media Freedom Act, the Artificial Intelligence Act and the Regulation on political advertising – can be used to counter disinformation disseminated by non-EU actors. It then turns to external action tools, with particular attention to restrictive measures and bilateral agreements. The paper argues that each category of instruments has distinct strengths and limitations, and it ultimately concludes that the EU cannot rely on a single model to address foreign disinformation. Instead, it should adopt a differentiated approach, combining unilateral measures and cooperative frameworks, depending on the Union's ability to assert jurisdiction and the nature of the actor involved.

CORRESPONDING AUTHOR:
Anna Fiorentini
University of Bologna, IT
anna.fiorentini3@unibo.it

KEYWORDS:
foreign disinformation; hybrid threats; democracy; EU law; digital regulation; fundamental rights

TO CITE THIS ARTICLE:
Anna Fiorentini, 'The EU's Arsenal to Protect Its Democracy from the Threat of Foreign Disinformation' (2026) 22(2) Utrecht Law Review 105–124. DOI: https://doi.org/10.36633/ulr.1271

DOI: 10.36633/ulr.1271

'The battle against FIMI is a matter of European security. It is one of the battles of our times. And with the tools we are developing, it is a battle that can be won.'

(Josep Borrell Fontelles, 2024)[1]

1. INTRODUCTION

The essence of democracy lies in the existence of a free and pluralistic public debate through which collective opinion is formed.[2] This paradigm depends on citizens' access to diverse and reliable sources of information, enabling them to participate meaningfully in public life. The rise of digital communication technologies has profoundly disrupted these conditions. While such technologies have multiplied opportunities for participation and pluralism, they have also intensified the dissemination of false or manipulative content, blurring the line between reality and fiction. The ease with which content can be produced, amplified and circulated online has thus generated a new type of informational disorder that threatens democracy by undermining citizens' right to accurate information and impairing their capacity to make informed decisions and engage effectively in democratic processes.[3]

Compared to forms of disinformation disseminated through analogue media (eg, newspaper radio or broadcasting), online disinformation – leveraging an expanding ecosystem of social media platforms (including X, Facebook, Telegram and TikTok) and increasingly sophisticated artificial intelligence (AI) techniques (eg, AI-generated text, synthetic audio and manipulated video)[4] – presents heightened risks for democratic integrity and the rule of law. These risks stem not only from the unprecedented speed and scale of dissemination in the digital environment,[5] but also from the fact that traditional media is subject to national rules on editorial responsibility and stronger public oversight of publishers and media outlets, which help mitigate its impact.[6]

In response to these emerging challenges, the European Union (EU) has adopted various measures aimed at protecting democracy as one of the foundational values enshrined in Article 2 of the Treaty on European Union (TEU).[7] Prompted by the European Parliament, the Commission initially launched soft law initiatives,[8] later reinforced by legislative acts, including the Digital Services Act (DSA),[9] European Media Freedom Act (EMFA)[10] and Artificial Intelligence

1 EEAS, '2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats: A Framework for Networked Defence' (2024) 2.

2 J Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (MIT Press 1996) 291–96.

3 Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Action Plan against Disinformation' JOIN(2018) 36 final 1; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on defence of democracy COM/2023/630 final; European Commission, '2025 State of the Union Address by President von der Leyen' (Strasbourg, 10 September 2025) <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_25_2053> accessed 10 October 2025.

4 EEAS, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Exposing the Architecture of FIMI Operations' (2025) 10–11; EEAS, '4th EEAS Report on Foreign Information Manipulation and Interference Threats. Dismantling the FIMI House of Cards' (2026) (4th EEAS Report) 5 and 9.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling Online Disinformation: A European Approach' COM(2018) 236 final; Commission guidelines 2024–2029 23.

6 G Morgese, 'Il contrasto alla disinformazione originata da ingerenze straniere nell'Unione europea' in M Messina, *Strengthening the European Union through the European Citizenship and the Rule of Law* (Editoriale scientifica 2024) 112.

7 Consolidated Version of the Treaty on European Union [2008] OJ C115/13 (TEU).

8 eg Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling Online Disinformation: A European Approach' (n 5); Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Action Plan against Disinformation' (n 3).

9 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L277/1 (Digital Services Act/DSA).

10 Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU [2024] OJ L2024/1083 (European Media Freedom Act/EMFA). For a critical and in-depth analysis of the EMFA as proposed by the Commission, cf M Cole, 'Act-ing on Media Freedom: The Proposed European Media Freedom Act (EMFA) of the European Union' (2023) 55 The University of Pacific Law Review 290.

Act (AIA).[11] Scholars have extensively analysed these measures, particularly their compatibility with fundamental rights like freedom of expression and access to information, which is protected by Article 10 of the European Convention on Human Rights (ECHR)[12] and by Article 11 of the EU Charter of Fundamental Rights (Charter).[13]

Comparatively less attention, however, has been paid to disinformation campaigns orchestrated by non-EU actors. These campaigns are most frequently associated with Russia, but they are not confined to it. Other foreign State actors, including China, have also been identified as engaging in information manipulation campaigns affecting the European information space. In this context, disinformation operates as a tactic of foreign interference: a coercive and deceptive measure employed by foreign actors to 'distort or falsely represent facts, artificially inflate one-sided arguments, discredit information to degrade political discourse and ultimately undermine confidence in the electoral system and therefore in the democratic process itself'.[14] Having this effect, large-scale disinformation campaigns on social media – used to control political narratives and to radicalise direct domestic actors – are a typical vector of what are now considered 'hybrid threats'.[15]

A partially overlapping, but broader, concept is Foreign Information Manipulation and Interference (FIMI). The European External Action Service (EEAS) defines FIMI as 'a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes', it is 'manipulative in character' and is 'conducted in an intentional and coordinated manner, involving state or non-state actors'.[16] Unlike disinformation as such, FIMI captures coordinate patterns of conduct forming part of a broader hybrid strategy aimed at disrupting the free formation and expression of individuals' political will by foreign actors, especially before elections, deepening social divisions and undermining trust in governments and institutions.[17]

A striking – though not isolated – example of how foreign disinformation campaigns may affect democratic security within the EU is provided by Romania. Investigations into the November 2024 presidential elections identified the presence of a coordinated foreign disinformation effort, attributed to Russian actors, aimed at amplifying specific political narratives on social media platforms, notably through networks of influencers on TikTok, thereby polarising public debate. At the same time, the Romanian case illustrates that such external interference operates within a broader domestic context shaped by long-standing political fragmentation, resource imbalances and pre-existing distrust in institutions. Foreign disinformation thus acted

11 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689 (Artificial Intelligence Act/AIA), as modified by Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI).

12 Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (European Convention on Human Rights, as amended) (ECHR).

13 Charter of Fundamental Rights of the European Union [2012] OJ C326/391. See, among others, A Renda, *The Legal Framework to Address 'Fake News': Possible Policy Actions at the EU Level* (European Parliament 2018); E Shattock, 'Lies, Liability and Lawful Content: Critiquing the Approaches to Online Disinformation in the EU' (2023) 60(5) Common Market Law Review 1313; RÓ Fathaigh, D Buijs and J van Hoboken, 'The Regulation of Disinformation under the Digital Services Act' (2025) Media and Communication 5; M Bonelli, *The European Union's Democratic Turn* (re:constitution Working Paper, 2025) 14; G De Gregorio and O Pollicino, 'The European Constitutional Way to Address Disinformation in the Age of Artificial Intelligence' (2025) German Law Journal 453; M Coli, 'The Role of the European Union in Protecting Democracy through Legislation: The Case of Disinformation' (2026) European Papers 81.

14 Resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI)) para B.

15 Joint Communication to the European Parliament and the Council, 'Joint Framework on countering hybrid threats: A European Union response' JOIN(2016) 18 final, 6 April 2016 2. In literature, see L Lonardo, 'EU Law Against Hybrid Threats: A First Assessment' (2021) 6(2) European Papers 1075–1096; L Lonardo (ed), *Addressing Hybrid Threats. European Law and Policies* (Edward Elgar Publishing 2024).

16 EU External Action, '2021 Stratcom Activity Report'. cf N Hénin, 'Towards a European Redefinition of Foreign Interference' (EU DisinfoLab 2023).

17 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, '2024 Rule of Law Report. The rule of law situation in the European Union' COM(2024) 800 final 7.

DOI: 10.36633/ulr.1271

not as a decisive cause of the electoral outcome, but as a destabilising force that exploited existing vulnerabilities.

Electoral processes have also been targeted in several other Member States. In the Czech Republic, for instance, hundreds of anonymous TikTok accounts reportedly spread pro-Kremlin narratives ahead of parliamentary elections. In Germany and Poland, foreign information manipulation followed a recurring operational logic: first, the delegitimatisation of political leadership months before the vote; second, the weaponisation of domestic divisions during the electoral campaign; and third, late-stage attempts to undermine trust in electoral integrity. Although the themes varied according to national context – immigration in Germany and anti-refugee sentiment in Poland – the underlying objective remained to polarise societies, discredit pro-European actors and weaken confidence in democratic procedures.[18]

Comparable patterns have been observed in several countries undergoing the EU accession process, including Ukraine and Moldova, which have become prime targets for foreign actors seeking to weaken international support, foment anti-EU sentiment and delay or derail their path toward membership. More recently, attention has also shifted to Armenia, particularly following legislative developments signalling a political willingness to initiate accession. In these contexts, disinformation narratives frequently portray pro-European leaders as corrupt, morally compromised or subservient to foreign interests. Although such narratives often exploit local fears and social cleavages, they are frequently disseminated in Western European languages, suggesting that FIMI campaigns may target wider international audiences beyond domestic voters.[19]

EU institutions have long recognised the severity of this threat. The Council of the EU has stressed that information manipulation and foreign interference are intended to mislead, deceive and destabilise democratic societies, exploit cultural and social frictions and negatively affect the Union's ability to conduct foreign and security policy.[20] The European Parliament has voiced similar concerns,[21] while the Commission has identified strategic risks associated with the online dissemination of information, especially where linked to foreign interference, warning that such activities may directly threaten the EU's democratic stability and shared values.[22]

Despite these warnings, the scale and sophistication of foreign interference campaigns have increased. EEAS reports record a progressive intensification of FIMI incidents, both in frequency and complexity.[23] These events exploit market freedoms and the openness of the digital space to erode trust in democratic institutions and European values, particularly during critical events such as the Covid-19 pandemic and the war in Ukraine,[24] and – as already underlined – elections.[25] Their impact is especially significant where electoral outcomes influence not only domestic political direction but also the evolution of the European integration process.

18 An in-depth analysis of these episodes has been developed in the 4th EEAS Report (n 4) 12.

19 ibid 3.

20 Council Conclusions on Foreign Information Manipulation and Interference (FIMI) (18 July 2022) 2.

21 Resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties (2016/2030(INI)); Recommendation of 13 March 2019 to the Council, the Commission and the Vice-President of the Commission/High Representative of the Union for Foreign Affairs and Security Policy on the scope and mandate for EU Special Representatives (2018/2116(INI)); Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)); Resolution of 9 March 2022 (n 14); Resolution of 1 June 2023 on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI)).

22 Joint Communication to the European Parliament and the Council, 'Joint Framework on countering hybrid threats: A European Union response' (n 15); Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling online disinformation: A European Approach' (n 5); Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Action Plan against Disinformation'(n 3); Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling COVID-19 disinformation – Getting the facts right' JOIN(2020) 8 final; Communication from the European Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the European democracy action plan COM(2020) 790 final.

23 4th EEAS Report (n 4) 5.

24 cf Lonardo (n 15) 1075.

25 4th EEAS Report (n 4) 12 and 15.

DOI: 10.36633/ulr.1271

The implications of foreign disinformation for the EU are therefore twofold. Internally, such campaigns threaten the stability of an EU legal order founded on the values enshrined in Article 2 TEU, at a time when those values are already under pressure from democratic backsliding in several Member States. Externally, they weaken the Union's capacity to pursue enlargement and to support democratic resilience in candidate and associated countries.

Against this background, foreign disinformation deserves closer scholarly attention, not only because of its systemic implications but also because of persistent gaps in the existing literature. On the one hand, there is still no comprehensive account of the instruments that the EU currently employs – or could employ – to counter online disinformation originating from non-EU actors, whether through internal market regulation or external action. On the other hand, further critical analysis is still needed to determine how these instruments relate to one another, and which combination is best suited to mitigating foreign disinformation while minimising the risks of backlash, circumvention and disproportionate interference with freedom of expression.

This paper addresses those gaps through two main contributions. The first is to provide a systematic reconstruction of the EU legal arsenal against foreign disinformation across both internal market law and external action. In that regard, Section 2 examines the Union's existing legislative instruments, including the DSA, EMFA, AIA and related measures, by assessing their scope, relevance and limitations in responding to foreign disinformation campaigns, while Section 3 turns to the external dimension, with particular attention to restrictive measures and bilateral agreements. The second contribution is to argue that association agreements should be understood as a distinct preventive instrument within that arsenal. Their value lies not in replacing unilateral or coercive measures, but in strengthening democratic resilience, media pluralism and institutional cooperation in neighbouring and candidate countries that are particularly exposed to FIMI and only partially reachable through EU internal market regulation. On that basis, the paper advances a differentiated model of EU action, in which the choice of the instrument depends on the Union's jurisdictional reach and the nature of the foreign actor involved.

2. EU LEGISLATIVE MEASURES AGAINST FOREIGN DISINFORMATION

Initially aimed at curbing the broad discretion of non-State actors – particularly online platforms – in determining, in the absence of a shared definition,[26] what constitutes disinformation, the EU's early response to disinformation primarily involved 'soft law' measures.[27] In 2018, the Commission promoted the EU Code of Practice on Disinformation, signed by major platforms such as Facebook, Google and Microsoft, along with industry associations. However, this instrument did not impose binding obligations on the signatories; it merely encouraged voluntary actions such as the removal of fake accounts and the adoption of measures to safeguard platform integrity against actors engaged in the dissemination of disinformation.

The limited effectiveness of the 2018 Code – further exposed by the COVID-19-related 'infodemic'[28] and the threat of disinformation campaigns ahead of the 2019 European Parliament elections – prompted the Commission to introduce a Strengthened Code of Practice on Disinformation in 2022. This revised version incorporates, on the one hand, more robust commitments, such as the reduction of financial incentives for disinformation actors, enhanced transnational fact-checking cooperation and greater transparency in political advertising. On the other hand, it established a more structured monitoring system through the creation of a Transparency

26 Nevertheless, some guidance can be drawn from Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling Online Disinformation: A European Approach' (n 5) 4 and Resolution of 9 March 2022 (n 14) para I, which suggest that disinformation can be understood as i) false or misleading information that is created, presented and disseminated for profit or with the intent to deceive the public (in contrast to *misinformation*, which is shared without the intention to deceive or generate profit) and; ii) content likely to cause public harm or provoke potentially negative societal consequences.

27 Resolution of 1 June 2023 (n 21) paras AI–AJ.

28 E Cirone, 'Misinformation about COVID-19: Is the European Union Well Equipped to Fight the "Info-demic"?' in D Utrilla and A Shabbir (eds), *EU Law in Times of Pandemic* (EU Law Live Press 2021) 177.

DOI: 10.36633/ulr.1271

Centre and a dedicated task force. Nonetheless, the Strengthened Code remains a non-binding instrument, lacking enforceable obligations and independent oversight mechanisms.

Recognising the limitations of self-regulation in ensuring meaningful compliance, the EU has progressively moved towards the adoption of binding legislative instruments, such as the DSA, the EMFA, the AIA and the Regulation on political advertising.[29] Although these measures were not specifically designed to address foreign disinformation – as their primary objective is to ensure the proper functioning of the internal market – several of their provisions may nonetheless play a significant role in countering this phenomenon. Notably, they introduce a combination of content moderation duties, transparency requirements and constraints on AI-driven manipulation.

As mentioned in the introduction, disinformation campaigns are increasingly taking place in the online environment. They leverage the reach of major platforms, such as X, which is responsible for a significant share of documented incidents of information manipulation.[30] They also make use of the capabilities of emerging technologies. AI tools in particular facilitate the rapid production of content and enable influence operations to scale up with limited resources.[31]

This evolution underscores the need for regulatory intervention targeting the key actors involved in the dissemination and amplification of disinformation. These include intermediary services and media service providers, which are addressed by the DSA and the EMFA respectively, as well as actors placing technologies such as micro-targeting tools and deepfake systems on the market. The latter are regulated by the AIA and the Regulation on political advertising, and contribute to the increased sophistication of disinformation content, making it more difficult for users to identify and assess its credibility.

In the following pages, before examining the substantive provisions of the aforementioned regulatory instruments – not only to map their scope, but also to assess their potential and limitations in addressing foreign disinformation campaigns – their territorial scope of application will be analysed. This preliminary step is essential to determine whether, and under what conditions, these legal frameworks apply to entities established outside the EU.

2.1. THE TERRITORIAL EXTENSION OF THE EU LEGISLATIVE MEASURES

A close reading of the regulatory instruments under examination (DSA, EMFA, AIA and Regulation on political advertising) clearly reveals the EU legislator's intent to grant them 'territorial extension',[32] in line with what can already be considered the mainstream normative approach since the General Data Protection Regulation (GDPR).[33]

Each of these instruments explicitly states that it applies to providers (and, in the case of the AIA, also deployers) who, although not established within the Union, offer intermediation services, media services or political advertising, or provide or deploy AI systems and general-purpose AI (GPAI) models to individuals or entities located in the internal market. More precisely, their territorial applicability rests on two alternative connecting factors: i) the existence of an establishment within the Union, or ii) in the absence thereof, the targeting of activities or services towards the Union. The latter criterion is considered satisfied where non-EU services or

29 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on transparency and targeting of political advertising [2024] OJ L2024/900 (Regulation on political advertising/Regulation (EU) 2024/900).

30 4th EEAS Report (n 4) 10.

31 ibid 14.

32 Unlike extraterritoriality, understood as 'the application of a measure triggered by something other than a territorial connection with the regulating state', territorial extension presupposes the existence of a relevant link with EU territory. cf J Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 The American Journal of Comparative Law 90.

33 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation/GDPR).

DOI: 10.36633/ulr.1271

AI systems are offered,[34] made available, or otherwise deployed within the Union,[35] directed at EU citizens,[36] placed on the market or put into service,[37] or even simply used within the Union.[38]

Among these instruments, the AIA stands out for providing more precise guidance on its territorial scope, notably defining key notions such as 'on the market' and 'putting into service',[39] thereby delineating its reach with greater accuracy. By contrast, the other regulations adopt a more open-textured approach and do not, for instance, define what constitutes an 'establishment' or when a service should be regarded as being 'offered to' or 'targeted at' EU citizens. Only the DSA offers partial clarification, specifying that a service is considered to be 'offered' in the Union where natural or legal persons in one or more Member States are able to use it and the provider has a 'substantial connection' to the Union.[40] Such a connection may derive either from the provider's establishment in the EU or from certain factual circumstances, such as the presence of a significant number of service recipients in one or more Member States or the targeting of activities towards them.[41]

In the absence of statutory definitions for key terms such as 'establishment' or 'targeting', interpretative guidance may be drawn from the case law of the Court of Justice of the European Union (CJEU) and from the European Data Protection Board (EDPB) guidelines developed in the context of the GDPR. In particular, in *Weltimmo*, the CJEU endorsed a broad and flexible understanding of 'establishment', defining it as 'any real and effective activity – even a minimal one – exercised through stable arrangements'.[42] Such arrangements may consist, for example, of a single representative operating within the EU on behalf of a non-EU entity.[43] Furthermore, according to EDPB guidance, the assessment of whether the data processing is carried out 'in the context of the activities of an establishment' requires, first, the existence of an inextricable link between the relevant activity and the operations of the EU establishment, and, second, the latter's activities to be directed at rendering the non-EU entity's operations profitable.[44]

Applying these interpretative criteria to the instruments under consideration suggests that their scope may extend to providers or deployers who, despite lacking a formal establishment within the Union, maintain stable arrangements functionally connected to the regulated activities. By contrast, the analogy with the GDPR is less straightforward when considering the factual indicators of a 'substantial connection' under the DSA, particularly the requirement that services be directed at a significant number of recipients in one or more Member States. This threshold is neither present in the GDPR nor further specified in the DSA. Nonetheless, it is reasonable to infer that a non-EU Internet Service Provider (ISP) with a substantial user base in the Union would fall within the scope of the DSA, especially where they qualify as Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) that exceed 45 million monthly active users.

With regard to the notion of 'targeting' – which is relevant not only under the DSA but also for the Regulation on political advertising and the EMFA – a clearer parallel with the GDPR can be established. The DSA provides an indicative list of factors to assess whether an ISP's activities

34 DSA (n 9) art 2(1).

35 Regulation 2024/900 (n 29) art 2.

36 EMFA (n 10) art 17.

37 AIA (n 11) art 2(1)(a) and (c).

38 ibid Recital 22.

39 ibid art 3(10) and (11).

40 DSA (n 9) art 3(d).

41 ibid art 3(e) and Recital 7.

42 Case C-230/14, *Weltimmo*, EU:C:2015:639, para 31. For commentary on the judgment, see M Cole and A Giurgiu, 'The "Minimal" Approach: The CJEU on the Concept of "Establishment" Triggering Jurisdiction for DPAs and Limitations of Their Sanctioning Powers' (2015) 4 European Data Protection Law Review 310; D Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 International Data Privacy Law 226; D Svantesson, 'The CJEU's Weltimmo Data Privacy Ruling: Lost in the Data Privacy Turmoil, Yet So Very Important' (2016) 23 Maastricht Journal of European and Comparative Law 332; A Wales, 'Major Legal Ruling on a Company's Data Protection Obligations Outside the Country where it is Headquartered: Weltimmo srov Nemzeti Adatvédelmi és Információszabadság Hatóság' (2018) 1(4) Journal of Data Protection & Privacy 356.

43 GDPR (n 33) Recital 22.

44 EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)' 8.

DOI: 10.36633/ulr.1271

are directed towards the Union, largely reflecting the criteria developed by the CJEU in *Pammer and Alpenhof*.[45] These include, *inter alia*, the use of a Member State's language or currency, the possibility of ordering products or services in that State, the availability of applications in national app stores, the presence of localised advertising and the provision of customer support in the language of the target market. Conversely, the mere technical accessibility of a website from within the Union is not sufficient, in itself, to establish such targeting.[46]

In conclusion, although the lack of precise statutory definitions introduces a degree of legal uncertainty regarding the exact contours of their territorial scope, it does not preclude an expansive application of the instruments under review. On the contrary, in light of the 'borderless'[47] nature of the digital environment and the risk that the freedoms of the internal market may be exploited to undermine the Union's democratic values, it is plausible that these instruments will be interpreted broadly, in continuity with the trajectory already established by the GDPR, which has effectively paved the way for an increasingly global regulatory reach.[48]

2.2. THE BINDING NATURE OF THE NORMATIVE OBLIGATIONS

Having clarified the territorial scope of the relevant regulations, the analysis now turns to the manner in which these instruments contribute to countering the production and dissemination of disinformation by foreign actors, introducing specific legal obligations addressed to those actors that, more than others, play a pivotal role in generating and amplifying disinformation content.

Starting from the DSA, it is important to note that the Regulation does not impose a general obligation on intermediary service providers to remove content that may undermine integrity. This choice reflects the fact that disinformation and foreign interference are not, as such, classified as illegal content – unlike defamation, incitement to hatred or violence[49] – even though they may produce similarly harmful effects.

Consequently, rather than imposing a blanket prohibition on disinformation – whose abstract definition is inherently complex[50] – the DSA adopts a more targeted and risk-based approach. It concentrates on those actors that pose the most significant challenges in terms of the scale and impact of information dissemination, namely the VLOPs and the VLOSEs. Under Article 34 DSA, these entities are required to diligently identify, analyse and assess any systemic risks stemming from the design, functioning or use of their services, including those arising from algorithmic systems and their potential to amplify disinformation and manipulative content.[51]

Importantly, the concept of 'systemic risks' under the DSA is defined in broad terms, encompassing not only the dissemination of illegal content but also any activity that may adversely affect the exercise of fundamental rights, public discourse or electoral processes.

45 Joined cases C-585/08 and C-144/09, *Pammer and Alpenhof*, EU:C:2010:740, para 76, later discussed by, *inter alia*, D Svantesson, 'Pammer and Hotel Alpenhof-ECJ Decision Creates Further Uncertainty about When E-Businesses "Direct Activities" to a Consumer's State under the Brussels I Regulation' (2011) 27(3) Computer Law & Security Review 298; A Van Hoek, 'CJEU-Pammer and Alpenhof-Grand Chamber 7 December 2010, Joined Cases 585/-8 and 144/09' (2012) 8 European Review of Contract Law 93.

46 DSA (n 9) Recital 8.

47 A Azzi, 'The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation' (2018) 9(2) Journal of Intellectual Property, Information Technology and Electronic Commerce Law 126.

48 ibid.

49 DSA (n 9) art 3(h) and Recital 12.

50 See AM Guess and BA Lyons, 'Misinformation, Disinformation, and Online Propaganda' in N Persily and JA Tucker (eds), *Social Media and Democracy* (CUP 2020) 10 ff; G Pitruzzella and O Pollicino, *Disinformation and Hate Speech – A European Constitutional Perspective* (EGEA Spa – Bocconi UP 2020) 97 ff; G Caggiano, 'Il contrasto alla disinformazione tra nuovi obblighi delle piattaforme online e tutela dei diritti fondamentali nel quadro del Digital Service Act e della co-regolamentazione (2021) 1 Papers di diritto europeo – Riflessioni e ricerche 45 ff.; S Giusti and E Piras (eds), *Democracy and Fake News. Information Manipulation and Post-Truth Politics* (Routledge 2021).

51 Platforms that, pursuant to DSA (n 9) art 33, 'have a number of average monthly active recipients of the service in the Union equal to or higher than 45 million', and are designated as such. An updated list of VLOPs and VLOSEs can be found here: <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> accessed 26 May 2026.

DOI: 10.36633/ulr.1271

Disinformation clearly falls within this category.[52] Recital 84 DSA indeed explicitly acknowledges that VLOPs and VLOSEs must address lawful content that contributes to systemic risks, including misleading or deceptive information, even where it does not reach the threshold of illegality.

The DSA requires VLOPs and VLOSEs to monitor and mitigate algorithmic amplification of harmful content. This includes assessing how content recommendation systems[53] may promote polarising, misleading or deceptive material, even when such content is not strictly false. Where such amplification contributes to systemic risk, for instance through the use of fake accounts or coordinated disinformation campaigns, platforms are required to adopt their design and content moderation practices accordingly. These risk assessments must be conducted at least annually, be subject to independent audits and lead to the adoption of mitigation measures under Article 35(3) DSA, including participation in codes of conduct such as the Strengthened 2022 Code of Practice, which was integrated into the DSA in February 2025.

In situations of crisis,[54] VLOPs and VLOSEs may also be required – upon a decision of the Commission – to adopt urgent measures, including tailored risk assessments, specific mitigation action and enhanced reporting obligations, such as adjustments to content moderation processes.[55] However, in order to safeguard freedom of expression, such emergency measures must be 'strictly necessary, justified and proportionate', and are limited in duration to a maximum of three months.[56]

Complementing the DSA, the EMFA regulates the relationship between VLOPs and media service providers. Given that VLOPs may act as vectors for polarisation and foreign-sponsored disinformation,[57] the EMFA introduces safeguards designed both to empower legitimate media service providers and to enhance transparency, without mandating direct content control.

Under Article 18 EMFA, VLOPs are required to offer media service providers the possibility to identify themselves by submitting declarations of editorial independence – both from EU Member States and from third countries – or by demonstrating adherence to recognised regulatory or co-/self-regulatory frameworks. Moreover, to benefit from enhanced protection against unjustified content moderation, media service providers must also commit not to disseminate AI-generated content without meaningful human oversight.[58] This mechanism is intended to help distinguish trustworthy media actors from those potentially acting as conduits for foreign interference, without granting blanket immunity or introducing forms of *ex ante* censorship.

Within this framework, the newly established European Board for Media Services – composed of national media authorities – is tasked with facilitating regular dialogue between VLOPs, media providers and civil society. Its role in monitoring compliance with self-regulatory initiatives – particularly in the area of harmful but lawful content such as disinformation and manipulation – further emphasises a collaborative and rights-preserving regulatory approach.[59] Additionally, the Board may contribute to coordinating national measures targeting non-EU media providers that reach EU audiences and pose risks to public security, thereby enabling more targeted interventions.

52 As argued by Fathaigh, Buijs and van Hoboken (n 13) 8–9; L Nannini et al, 'Beyond Phase-In: Assessing Impacts on Disinformation of the EU Digital Services Act' (2025) 5(2) AI and Ethics 1246; S Gallone, 'Affrontare la disinformazione online: il sistema di mitigazione dei rischi nel Digital Services Act' in L Califano, F Fabrizzi and G Sartor, *Disinformazione digitale. Modelli algoritmici e valori democratici* (FrancoAngeli 2026) 419.

53 According to DSA (n 9) art 3(s), a 'recommender system' is 'a fully or partially automated system used by an online platform to suggest in its online interface specific information to recipients of the service or prioritise that information, including as a result of a search initiated by the recipient of the service or otherwise determining the relative order or prominence of information displayed'.

54 DSA (n 9) art 36(2).

55 ibid Recital 91.

56 ibid art 36(3).

57 EMFA (n 10) Recitals 3–4.

58 ibid art 18. On the precautionary safeguards introduced during the legislative process to prevent the abusive exploitation of this provision, see M Monti, 'The Missing Piece in the DSA Puzzle? Article 18 of the EMFA and the Media Privilege' (2024) Rivista italiana di informatica e diritto 195.

59 EMFA (n 10) art 19(1)(c).

DOI: 10.36633/ulr.1271

Alongside the DSA and EMFA, the Regulation on political advertising and the AIA introduce further tools capable of strengthening the EU's response to foreign disinformation. These instruments focus on specific mechanisms – namely micro-targeting and synthetic content generation – which have already been exploited to manipulate public opinion and undermine democratic processes, particularly through foreign interference.

While not synonymous with disinformation, micro-targeted political advertising[60] can be used to disseminate deceptive, manipulative or polarising messages to highly segmented audiences, often escaping public scrutiny.[61] The Regulation on political advertising addresses this risk by introducing specific restrictions. Notably, Article 5(2) prohibits the provision of political advertising services sponsored by third countries in the three months preceding elections or referenda, with the aim of limiting foreign interference during particularly sensitive political periods.[62]

In parallel, however, the Regulation on political advertising carefully preserves freedom of expression by excluding from its scope political opinions expressed under editorial responsibility or personal views shared by individual users.[63] In addition, it promotes voluntary best practices, encouraging platforms to adopt policies aimed at demonetising disinformation and preventing the dissemination of misleading political advertisements, thereby reinforcing systemic safeguards without imposing disproportionate constraints.[64]

Finally, the AIA complements this regulatory framework by addressing the technological tools that facilitate the creation and dissemination of deceptive content, such as deepfakes and synthetic media. It does so by introducing transparency obligations for both providers and deployers of AI systems, including GPAI. In particular, providers of AI systems capable of generating synthetic audio, images, video or text must ensure such content is machine-readable and identifiable as artificially generated or manipulated. Similarly, deployers of AI systems to produce deepfakes or to manipulate content of public interest are required to clearly disclose that the content has been generated or altered by AI.[65]

These measures pursue a dual objective: enhancing public awareness and supporting VLOPs and VLOSEs in fulfilling their obligations under the DSA, especially with regard to the identification and mitigation of systemic risks linked to deceptive or AI-generated content.[66] In this sense, the AIA operated as part of the broader co-regulatory model, analogous to that of the DSA, including the development of codes of conduct to facilitate effective implementation.[67]

Furthermore, the AIA imposes design-related obligations on AI systems that interact directly with individuals, requiring users to be informed when they are engaging with an AI system.[68] This provision specifically targets the use of social bots and automated accounts, which are frequently deployed to amplify disinformation or simulate artificial consensus around polarising

60 The definition offered by Regulation (EU) 2024/900 (n 29) is broad, including, pursuant to art 3(2), 'the preparation, placement, promotion, publication, delivery or dissemination, by any means, of a message, normally provided for remuneration or through in-house activities or as part of a political advertising campaign: (a) by, for or on behalf of a political actor, unless it is of a purely private or a purely commercial nature; or (b) which is liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level'.

61 Regulation (EU) 2024/900 (n 29) Recital 4 specifies that '[p]olitical advertising can be a vector of disinformation, in particular where the advertising does not disclose its political nature, comes from sponsors outside of the Union or is subject to targeting techniques or ad-delivery techniques. A high level of transparency is necessary inter alia to support open and fair political debate and political campaigns, and free and fair elections or referendums, and to counter information manipulation and interference, as well as unlawful interference, including from third countries'.

62 cf M Bonelli (n 13) 14.

63 Regulation (EU) 2024/900 (n 29) art 1(2)–(3).

64 Regulation (EU) 2024/900 (n 29) Recital 20.

65 AIA (n 11) art 50(2) and (4).

66 ibid Recital.

67 On the EU approach to countering disinformation in the context of advanced digital technologies, see De Gregorio and Pollicino (n 13) 460–70.

68 AIA (n 11) art 50(1).

DOI: 10.36633/ulr.1271

narratives.[69] Notably, where an AI system used to generate deepfakes is employed to influence electoral outcomes, referenda or individual voting behaviour – as documented in several recent cases involving semi-automated fake accounts which were reportedly used to distort public debate in countries such as Romania, Germany and Poland – such systems may qualify as 'high risk' under Annex III (8)(b) AIA. Consequently, they become subject to the stricter requirements applicable to high-risk AI systems.

However, the EU legislator has not fully addressed concerns related to foreign interference within the AIA. In particular, the Regulation does not prevent the possibility of such interference from being channelled through European standardisation organisations (eg, CEN and CENELEC), to which it confers significant powers in defining technical standards, which shape essential aspects of the regulatory framework in practice.[70] This is problematic for a number of reasons. For the purposes of this analysis, it is sufficient to recall the documented participation of individuals associated with companies in third countries (eg, Huawei or other State-affiliated enterprises) in standard-setting processes. This raises the risk of regulatory capture, insofar as actors operating within legal systems where the protection of fundamental rights diverges significantly from that of the EU may exert undue influence over the development of standards with substantive regulatory implications.[71]

Beyond these considerations, the analysis conducted thus far highlights that the capacity of the internal market instruments examined to safeguard democracy and freedom of expression appears constrained by several structural factors. First, although the EU has developed a complex and evolving regulatory framework aimed at countering foreign disinformation – combining content moderation duties, transparency obligations and constraints on AI-driven manipulation – its scope of application remains tied to a territorial or economic nexus with the internal market. While these instruments extend, in principle, to actors located outside the Union that target EU users, they nevertheless require some form of connection to the EU. As a result, actors operating entirely outside EU jurisdiction and without a meaningful link to the internal market may remain beyond the effective reach of these rules. The EU thus projects its normative influence beyond its borders, but the effectiveness of this 'territorial extension' ultimately depends on both political will and the practical feasibility of enforcement.

Second, the effectiveness of these instruments is further limited by their circumscribed material and personal scope. Each regulation targets specific categories of actors – such as intermediary service providers, media service providers or developers and deployers of AI systems – and covers defined activities, including the dissemination of political advertising of the deployment of high-risk AI system. Consequently, foreign actors operating outside formal market structures – for instance, informal networks coordinating disinformation campaigns through encrypted messaging services, or State-sponsored entities disseminating content via diplomatic channels or proxy accounts – may fall only partially, if at all, within the regulatory perimeter. Similarly, certain practices – such as organic content amplification through loosely coordinated user behaviour, or influence operations that do not rely on regulated advertising or AI tools – may escape the scope of current EU legislation.

A further and crucial challenge concerns enforcement, particularly with regard to non-EU actors that may not share the Union's normative commitments or strategic priorities. The imposition of EU regulatory standards on global digital platforms has already generated tensions. For instance, the European Commission's use of its enforcement powers under Article 66 DSA – such as in proceedings against Meta over the shutdown of CrowdTangle,[72] actions against X for

69 As broadly acknowledged in the literature by, among others, N Bontridder and Y Poullet, 'The Role of Artificial Intelligence in Disinformation' (2021) 3 Data & Policy 3; O Pollicino, 'Disinformazione e intelligenza artificiale: a groovy kind of love' (2024) Annuario di diritto comparato e di studi legislativi 265; M Mesarčík and N Slosiarová, 'Regulating AI for a Truthful Tomorrow: Addressing Disinformation in the EU Artificial Intelligence Act' (2025) 33 International Journal of Law and Information Technology 4–5; De Gregorio and Pollicino (n 13) 452.

70 AIA (n 11) art 40.

71 cf M Cantero Gamito, 'The Influence of China in AI Governance through Standardisation' (2023) 47 Telecommunications Policy 9; A Volpato, 'Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale' (2024) 2 Quaderni AISDUE 14.

72 An essential tool for social media monitoring, used by journalists and researchers to detect the spread of disinformation. According to the Commission, the closure of CrowdTangle without an adequate alternative could indicate that Meta has not diligently assessed or adequately mitigated the systemic risks related to the effects of Facebook and Instagram on civic debate and electoral processes (Press release of 30 April 2024, IP/24/2373).

DOI: 10.36633/ulr.1271

alleged failures to mitigate disinformation risks[73] or the issuance of data preservation orders to TikTok[74] – is indicative of an increasingly assertive regulatory posture.[75] Yet these interventions have also prompted resistance on the part of large technology companies, highlighting the inherent limitations of unilateral rule-setting in a fragmented digital environment.[76]

Finally, aside from matters of jurisdiction and enforcement, a deeper normative concern relates to the risk of overreach and unintended restrictions on freedom of expression.[77] The contested nature of 'disinformation' raises fundamental questions as to who should be entrusted with defining harmful content and according to which criteria. If enforcement mechanisms are applied in an overly expansive or politicised manner, there is a risk that legitimate dissent, investigative journalism or minority viewpoints could be inadvertently suppressed. Moreover, platforms, seeking to minimise regulatory exposure, may adopt overly cautious moderation practices, leading to the pre-emptive removal of lawful but controversial content. Such dynamics risk producing a chilling effect on public debate, ultimately undermining the very democratic values that these regulatory initiatives seek to protect.

3. THE EU'S EXTERNAL ACTION INSTRUMENTS AGAINST FOREIGN DISINFORMATION

With regard to instruments falling within the EU's external action, including the Common Foreign and Security Policy (CFSP), the Union's initial response to the threat posed by FIMI to European security took the form of the establishment of a Strategic Communication Task Force within the EEAS. These bodies were specifically designed to counter disinformation campaigns, particularly those attributed to Russia, by strengthening the EU's strategic communication capacities.[78]

Subsequently, the 2018 Communication on tackling online disinformation,[79] together with the accompanying Action Plan,[80] marked a further step in the institutionalisation of the EU's response. In this context, the Rapid Alert System was created to facilitate the real-time exchange of information among Member States and EU institutions regarding ongoing disinformation campaigns through a dedicated technological infrastructure. This mechanism proved particularly valuable during the COVID-19 pandemic, as it enabled the timely sharing of data, analyses and situational awareness, thereby contributing to a more comprehensive understanding of the information environment surrounding the crisis.[81]

Alongside these initiatives, other instruments of EU's external action may serve as effective tools in the Union's broader strategy to counter foreign disinformation, especially when it takes the form of FIMI. This paper focuses on two specific tools.[82] The first consists of restrictive

73 Press release of 18 December 2023, IP/23/6709.

74 Press release of 17 December 2024, IP/24/6487.

75 Fathaigh, Doris and van Joris (n 13) 13–14.

76 See, for instance, M Scott, 'The EU's Online Content Rulebook isn't Ready for Primetime' (*Politico*, 2024).

77 As highlighted by Morgese, in several EU Member States, the risk of censorship drift has materialised, raising questions about the compatibility of some measures with democratic principles and the rule of law. cf Morgese (n 6) 118–20.

78 More precisely, its mandate encompasses three main lines of action, namely: i) effectively communicate and promote the EU policies and values towards the Eastern neighbourhood; ii) strengthen the overall media environment including support for independent media; iii) increase the awareness of disinformation activities by external actors, and improve EU capacity to anticipate and respond to such activities ('EU Action Plan on Strategic Communication' (2015) 1). More recently, two supplementary task forces have been set up: the Western Balkans Taskforce and the South one which covers the countries in the Middle East, North Africa and the Gulf region.

79 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling Online Disinformation: A European Approach' (n 5).

80 Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Action Plan against Disinformation' (n 3).

81 Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Tackling COVID-19 disinformation – Getting the facts right' (n 22).

82 For a comprehensive overview of the current initiatives at bilateral and multilateral levels, cf E Bressanelli and S Bernardi, *Strengthening Resilience. Towards the European Democracy Shield* (European Parliament 2025) 37–48.

measures, which have already been employed to address disinformation-related threats. The second concerns the conclusion of bilateral agreements, which – although not yet used for this purpose – hold significant potential as a means of enhancing cooperation and preventing external interference in the EU's information space.

3.1. SANCTIONS AND FOREIGN DIRECT INVESTMENTS SCREENING

Restrictive measures – also referred to as sanctions – constitute a key instrument of the EU's CFSP. In the fight against foreign disinformation, they can be used to disrupt the financial and organisational structures underpinning hostile information activities, to limit their reach within the Union and to signal strong political condemnation of conduct that threatens the Union's security, democratic values and public order. In practice, these measures have most prominently taken the form of broadcasting restrictions, such as prohibiting designated media outlets from operating or disseminating content within the EU. However, they may also include asset freezes – aimed, for example, at cutting off financial support to disinformation networks – as well as travel bans targeting individuals responsible for orchestrating or facilitating such activities.

The EU has relied on such measures in recent years, particularly in the context of armed conflict and acute geopolitical crises. In this setting, the Union has targeted foreign media even where they are formally established within the Union but directly or indirectly controlled by third-country actors. These interventions aim to prevent the dissemination of content used to justify or legitimise acts of aggression. From the Council's perspective, such activities pose a serious risk to democratic institutions and public order, as they may undermine political pluralism, social cohesion and trust in democratic processes.[83]

A first notable precedent is the Union's response to Russia's military aggression against Ukraine. In *Kiselev*, the General Court upheld the legitimacy of restrictive measures imposed on the director of the Russian news agency *Rossiya Segodnya*.[84] The Court endorsed the Council's assessment that his activities – namely the systematic promotion of State-controlled media narratives legitimising the annexation of Crimea – went beyond the exercise of journalistic freedom and formed part of a broader propaganda strategy attributable to the Russian State. On that basis, the measures were considered consistent with the objectives pursued under the CFSP.

This line of reasoning was further developed in *RT France*,[85] where the General Court upheld the Council's decision (CFSP) 2022/351, which suspended the broadcasting and dissemination of content produced by RT and Sputnik across all transmission channels within the Union, including cable, satellite, online platforms, social media and websites.[86] In its proportionality analysis, the Court accepted the Council's characterisation of these outlets as instruments of Russian State propaganda, directly financed and controlled by the Russian authorities,[87] and assessed the measures against the exceptional security backdrop created by the 2022 invasion of Ukraine. It concluded that the objectives pursued – namely the 'safeguarding of the Union's values, fundamental interests, security, integrity and public order' – were legitimate and sufficiently

83 See S Poli, 'The Europeanisation of "Public Order": The Cases of Restrictive Measures to Counter the Spread of False Information and of Restrictions to Foreign Direct Investments' (2024) European Papers 1424.

84 Case T-262/15, *Kiselev*, EU:T:2017:392.

85 Case T-125/22, *RT France v Council*, EU:T:2022:483, paras 53 and 56. For a comment on the judgment, cf S Poli, 'Prime riflessioni sulla sentenza del Tribunale "RT France" sulle misure restrittive contro le attività di disinformazione russe' (2022) 2 Quaderni AISDUE 131; L Lonardo, 'Censorship in the EU as a Result of the War in Ukraine. Case T-125/22 RT France v Council' (2023) 48(6) European Law Review 707; V Szép and RA Wessel, 'Balancing Restrictive Measures and Media Freedom: RT France v. Council' (2023) Common Market Law Review 1383; JP Jacqué, 'Liberté d'information et mesures restrictives:(obs sous Trib UE, arrêt RT France c Conseil, 27 juillet 2022)' (2024) 139(3) Revue trimestrielle des droits de l'Homme 719; S Gallone, 'Il diritto all'informazione nell'era della disinformazione: Una prospettiva europea tra giurisprudenza e strumenti normativi' (2026) 3 MediaLaws 138.

86 Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

87 Case T-125/22, *RT France v Council* (n 85) paras 185–93.

DOI: 10.36633/ulr.1271

important to justify the restrictions imposed on the applicants' freedom of expression and their freedom to provide services.[88]

A similar approach can be seen in the *MegaFon* case, which concerned a major Russian telecommunications operator.[89] In that instance, the General Court accepted that the company's services supported the Russian military and security apparatus and could therefore contribute, albeit indirectly, to activities linked to information manipulation. The judgment further illustrates the broad margin of appreciation afforded to the Council in CFSP matters, particularly where restrictive measures are based on complex security assessments, and confirms the Court's relatively deferential approach in reviewing such determinations.

Collectively, this body of case law shows that EU judges have accepted that, in situations of acute geopolitical conflict, State-controlled propaganda activities may be treated as a security concern capable of justifying the adoption of restrictive measures, provided that such activities are attributable to foreign State actors and form part of a broader context of armed aggression. At the same time, this acceptance remains strictly context-dependent and does not amount to a general validation of sanctions as a counter-disinformation instrument as such. Rather, in line with the Court's role of reviewing the legality of individual measures, the compatibility of restrictive measures with fundamental rights – most notably, freedom of expression – has been assessed through a case-specific proportionality analysis. It follows that any future measures adopted by the Council[90] are likely to be reviewed according to the same criteria, in particular the gravity of the security context, the attribution of the relevant conduct and the proportionality of the interference with fundamental rights.

The restrictive measures adopted by the EU in response to Russia's aggression exemplify the potentially far-reaching nature of such interventions, especially when compared with the internal market tools discussed above. Their intensity is closely linked to the specific circumstances in which they are deployed, namely the need to counter coordinated campaigns of information manipulation conducted as part of a wider strategy of destabilisation, including during politically sensitive periods such as elections.[91]

However, precisely because of this intensity, the broader relevance of sanctions as a general tool to counter disinformation appears limited. Both the case law and institutional practice examined show that such measures have so far been adopted in narrowly defined situations marked by serious breaches of international law and acute threats to the Union's security and public order.[92] In these circumstances, the objectives pursued correspond to those set out in Article 21(2) TEU, including safeguarding the Union's values and interests and contributing to international peace and security.[93]

As a result, CFSP restrictive measures currently appear to be predominantly reactive tools, closely associated with armed conflict or comparable geopolitical crises. This limits their suitability for addressing the more diffuse and systemic vulnerabilities of the European information space in

88 ibid para 226. The Court also specified that: 'As regards the objectives pursued by the Council, recitals 4 to 10 of the contested acts refer to the need to protect the Union and its Member States against disinformation and destabilisation campaigns conducted by the media outlets under the control of the leadership of the Russian Federation which threatened the Union's public order and security, in a context marked by military aggression against Ukraine. Those objectives thus relate to public interests which aim to protect European society and form part of an overall strategy … which is designed to put an end, as quickly as possible, to the aggression suffered by Ukraine' (para 55).

89 Case T-193/23, *MegaFon v Council*, EU:T:2025:7.

90 In December 2024, the list of sanctioned individuals and entities has indeed been expanded to include those involved in the so-called 'Doppelganger operation' (Council Implementing Regulation (EU) 2024/3188 of 16 December 2024 implementing Regulation (EU) 2024/2642 concerning restrictive measures in view of Russia's destabilizing activities [2024] OJ L2024/3188), a Russian-led digital disinformation campaign aimed at manipulating public discourse and supporting the Russian war of aggression against Ukraine, including through the targeting of EU Member States. Moreover, in February 2025, as part of the sixteenth sanctions package, the Union further extended the broadcasting ban to eight additional Russian media outlets found to be under the permanent control of the Russian political authorities and systematically engaged in disinformation and propaganda activities (Council Implementing Regulation (EU) 2025/389 of 24 February 2025 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine [2025] OJ L2025/389).

91 Recitals 6–7 Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine.

92 Case T-125/22, *RT France v Council* (n 85) paras 86 and 198.

93 ibid paras 161 and 163; Case T-262/15, *Kiselev* (n 84) para 81.

peacetime. Moreover, extending their use beyond such contexts raises significant normative concerns. While their deployment may be justified as an emergency response to coordinated manipulation campaigns, their continued or expanded use in situations of relative political normalcy risks transforming exceptional measures into de facto instruments of content control.[94] In the absence of a rigorous proportionality assessment under Article 52 of the Charter,[95] such measures could therefore give rise to serious and lasting interferences with freedom of expression and information.

It is clear from these findings that sanctions cannot serve as the primary or long-term regulatory response to foreign disinformation. Given their exceptional and reactive nature, greater attention should instead be devoted to instruments capable of operating preventively. In this respect, foreign direct investment (FDI) screening may offer a complementary – albeit indirect – avenue for addressing disinformation risks that arise not from specific content, but from the ownership and control structures of media undertakings operating within the Union.

At the EU level, FDI screening is governed by Regulation (EU) 2019/452 (FDI Regulation),[96] which, while preserving the principles of market openness and economic integration, allows Member States – and, within the limits of its competences, the Commission – to assess and, where necessary, restrict foreign investments likely to affect security or public order.[97] In carrying out this assessment,[98] national authorities and the Commission may consider a wide range of factors, including both the characteristics of the investment (eg, its impact on critical infrastructure, technologies or media pluralism) and the profile of the investor (eg, link to the third-county governments or involvement in activities affecting public security).[99]

Although disinformation is not explicitly identified as an autonomous ground for intervention, concerns closely related to information manipulation can nonetheless arise in practice. In particular, investments in the media and telecommunications sectors may trigger enhanced scrutiny where they risk enabling foreign influence over public discourse. Such risks can be captured within the broader notions of 'security' and 'public order', especially where investments may affect media pluralism, editorial independence or the integrity of the information environment. This interpretation is further supported by recent policy developments: while Article 4(1)(e) of the FDI Regulation already refers to media freedom and pluralism as relevant factors, the proposal to revise the Regulation clarifies that this assessment should also take into account online platforms that may be used for large-scale disinformation or other harmful activities. In this way, FDI screening can indirectly address disinformation risks without resorting to direct content-based regulation.

Allowing FDI screening to be used for these purposes is consistent with the broader evolution of the instrument. Originally conceived as a mechanism for protecting national strategic interests, it is increasingly being employed to safeguard collective European interests,[100] with the Commission playing a progressively more prominent role within the cooperation framework established by the Regulation. On the one hand, national screening authorities are required to

94 There are concerns that the doctrine has been shared, especially in a context where we are moving away from situations of armed conflict towards less serious 'hybrid threats' originating from outside the EU. See Morgese (n 6) 118 and 122.

95 In the *RT France* judgment, the Court held that the restriction on freedom of expression was admissible because: i) it is provided for by law; ii) it respects the essential content of art 11 of the Charter, in view of the temporary and reversible nature of the ban, as well as its subordination to the continuation of the aggression against Ukraine and the propaganda actions of the Russian Federation against the Union; iii) capable of pursuing an objective of general interest, iv) proportionate, since the applicant has not demonstrated that the Council made an error of assessment. cf Case T-125/22, *RT France v Council* (n 85) para 191.

96 Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union [2019] OJ L791/1 (FDI Regulation); G Napolitano (eds), *Foreign Direct Investment Screening. Il controllo sugli investimenti esteri diretti* (Mulino 2019); N Ali, 'Il controllo degli investimenti esteri diretti nell'Unione europea e la protezione delle attività strategiche europee nel contesto dell'emergenza da Covid-19' in P Acconci and E Baroncini (eds), *Gli effetti dell'emergenza Covid-19 su commercio, investimenti e occupazione. Una prospettiva italiana* (Dipartimento di Scienze Giuridiche 2020) 183.

97 On the definition of these notions, see S Barbou des Places (ed), 'Special Section on European Paper: Public Order and Public Security in EU Law' (2024)9(3) European Papers 1316–1328.

98 FDI Regulation (n 96) art 2(1) codifies the definition of FDI under the common commercial policy provided by the CJEU, Opinion 2/15 EU:C:2017:376 (16 May 2017) para 80.

99 FDI Regulation (n 96) art 4(1)–(2) and Recital 12.

100 Napolitano (n 96).

give due – or, in some cases, utmost – consideration to the Commission's opinions,[101] particularly where investments affect projects or programmes of specific Union interest, and to justify any departure from them. On the other hand, the Commission is empowered to adopt delegated acts to amend the list of such projects and programmes,[102] thereby shaping the scope of investments subject to heightened scrutiny. Through its opinions, coordination functions and guidance on risk factors, the Commission may contribute to a more integrated and EU-oriented interpretation of 'security' and 'public order', fostering the emergence of a more supranational understanding of security concerns.[103]

Despite this growing Europeanisation of the mechanism, the power to authorise, block or condition foreign investments ultimately remains with the Member State in which the investment is planned or carried out.[104] This allocation of competences is preserved in both the current Regulation and the proposed revision, which, notwithstanding the strengthened weight of the Commission's opinions,[105] does not alter the Member States' final decision-making authority or their broad discretion in assessing risks and determining appropriate mitigation measures.[106] As a result, the capacity of FDI screening to address disinformation-related risks remains both uneven and contingent. It depends, in practice, on the willingness of Member States to incorporate concerns relating to information integrity and foreign influence into their security assessments. While the Commission's enhanced role introduces important elements of coordination and policy steering, it does not fundamentally transform the decentralised nature of the system, thereby allowing divergent national priorities and sensitivities to persist in this domain.

3.2. BILATERAL AGREEMENTS AND THE INCORPORATION OF ANTI-DISINFORMATION CLAUSES

Beyond being a concern for democratic processes within the EU, foreign online disinformation can represent a source of disruption to the functioning of the global economy and international trade. The widespread dissemination of false or manipulated information can distort markets, mislead consumers, undermine trust in economic operators and influence investment decisions. In this sense, disinformation operates not merely as a political threat, but as an economic one. It has progressively been weaponised as a tool of geopolitical competition, capable of shaping perceptions of a country's political stability, regulatory reliability and financial soundness among investors and trading partners.

Recent developments provide a good illustration of this trend. In Romania, disinformation campaigns attributed to pro-Russian actors contributed to electoral instability and ultimately led the Constitutional Court to annul election results.[107] The resulting period of political uncertainty had tangible economic consequences, weakening investor confidence and international commercial relations within the internal market. What this episode makes visible is how disinformation can generate concrete cross-border economic spillovers,[108] thereby establishing a potential link between information integrity and international trade.

This connection is equally evident in the context of foreign disinformation campaigns targeting non-EU countries such as Moldova and Ukraine. In these cases, disinformation is strategically

101 FDI Regulation (n 96) arts 6(9) and 8(1)(c).

102 ibid art 8(4).

103 F Casolari, 'Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited' (2023) 28(4) European Foreign Affairs Review 334.

104 FDI Regulation (n 96) arts 6, 7 and 8.

105 Pursuant to art 7(5) of the Proposal for a Regulation of the European Parliament and of the Council on the screening of foreign investments in the Union and repealing Regulation (EU) 2019/452 of the European Parliament and of the Council COM/2024/23 final, national screening authorities are required, in all cases of disagreement, to provide a detailed explanation.

106 ibid Recitals 28 and 36.

107 Press release (6 December 2024) <https://www.ccr.ro/comunicat-de-presa-6-decembrie-2024/> accessed 23 May 2026.

108 'Foreign Direct Investment in Romania' (*Lloyds*) <https://www.lloydsbanktrade.com/en/market-potential/romania/investment#:~:text=FDI%20in%20Figures,stood%20at%20USD%20125.5%20billion> accessed 23 May 2026. cf R Cornea, 'Romanian Militant Democracy in Action: Shielding Democracy from Subversion and Annulling the Elections' (*Verfassungsblog*, 1 April 2025).

DOI: 10.36633/ulr.1271

deployed to undermine pro-European political orientations, erode trust in public institutions and support anti-EU parties or narratives. The potential outcome – far from merely hypothetical – is to jeopardise, among other things, the credibility of the accession process or delay its progress, with significant economic implications. Such disruptions could indeed slow the convergence with the EU law, weaken integration into EU markets and supply chains in key sectors (eg, energy, agriculture and transport) and reduce trade volumes with the Union.

The economic repercussions of foreign disinformation campaigns suggest that, at least at first glance, EU trade policy may offer a credible avenue for incorporating commitments aimed at limiting the use of information manipulation as a tool of market distortion or geopolitical destabilisation. These kinds of commitments could, in principle, focus on transparency in digital markets, cooperation between competent authorities, joint risk assessments and the promotion of common standards in areas such as political advertising, content moderation and the use of AI in digital markets.[109] Framed in this way, anti-disinformation provisions would not seek to regulate speech directly, but to strengthen trust in digital trade and reinforce the EU's role as a promoter of democratic values in its external action, in line with Articles 3(5) and 21(1) TEU.[110]

Nonetheless, the scope for such provisions within Free Trade Agreements (FTAs) concluded under Article 207 of the Treaty on the Functioning of the European Union (TFEU)[111] is limited. Despite their increasing breadth,[112] FTAs are anchored in the common commercial policy and must maintain a sufficiently direct link to trade. Following Opinion 2/15, it is not enough to argue that misinformation affects democratic stability in general terms. Instead, any proposed provision must be convincingly connected to trade flows, market access, competition in digital markets or consumer protection in cross-border transactions.

This requirement considerably narrows what can realistically be included. Broad commitments to counter foreign interference or safeguard democratic debate would sit uneasy within the legal framework of common commercial policy and might require an additional legal basis. By contrast, more specific provisions – such as rules on transparency in online advertising, cooperation against deceptive commercial practices, information-sharing on coordinated manipulation affecting digital markets or dialogue on AI-generated commercial content – are more likely to fall within trade competences. Even then, their design would have to emphasise regulatory cooperation rather than substantive obligations aimed at protecting democracy as such.

Additional constraints arise from digital trade disciplines, particularly those relating to intermediary liability. Some trade agreements limit the ability of parties to impose liability on online platforms for third-party content.[113] In such contexts, anti-disinformation provisions could not introduce direct liability for hosted content without risking inconsistency with existing commitments. Instead, they would need to rely on non-liability-based mechanisms, such as transparency obligations, voluntary codes of conduct, exchanges of best practices, regulatory cooperation and dialogue on systemic risk mitigation.

109 See, for instance, UN Global Principles for Information Integrity (2024); Recommendation of the OECD on Information Integrity (2024); Venice Commission of the Council of Europe Principles for a fundamental rights-compliant use of digital technologies in electoral processes (2020).

110 On the obligation of the EU's institutions to uphold and promote the values of art 2 TEU both internally and externally, see Opinion of AG Ćapeta in Case C-769/22, *Commission v Hungary*, EU:C:2025:408, para 172.

111 Consolidated Version of the Treaty on the Functioning of the European Union [2012] OJ C326/47 (TFEU).

112 Since the 2006 Global Europe Communication (COM (2006) 567), the so-called 'new-generation' FTAs have marked a significant shift in the EU trade policy. These agreements increasingly extend beyond tariff reduction to include provisions on intellectual property rights, data protection and sustainable development, reflecting a broader understanding of trade as a vehicle for regulatory cooperation and normative influence under art 21 TEU (n 7) and art 205 TFEU ibid. This phenomenon has been extensively analysed by the literature. See, *inter alia*, L Pasquali, 'The EU-MERCOSUR Agreement as Source of Development of Specific Global Norms and Standards' in CG Segura, J Ibanez and P Pareja, *Actores Regionales y Normas Globales: La Uniòn Europea y Los BRICS Como Actores Normativos* (Tirant lo Blanch 2021) 133; ; G Rugani, 'La strategia di promozione a livello internazionale dei valori dell'UE, con particolare riferimento agli standard in materia di lavoro: punti di forza e criticità degli attuali meccanismi' (2022) Quaderni AISDUE 532–554; V Remondino, 'Gli accordi sul commercio digitale tra liberalizzazione degli scambi e protezione dei dati personali e della privacy: implicazioni per la politica commerciale comune dell'Unione europea' (2024) 2 Quaderni AISDUE 1–11; G Rugani, 'The Data Protection Provisions in the New EU-Chile Interim Trade Agreement: A Step Forward from the Past' (2025) Quaderni AISDUE 1.

113 See, for instance, FTA between the United States of America, the United Mexican States and Canada, art 19; US-Japan Digital Trade Agreement, art 18.

DOI: 10.36633/ulr.1271

It should also be acknowledged that anti-disinformation clauses in FTAs would be unlikely to qualify as 'essential elements' of the agreement. Their breach would therefore not normally justify suspension or termination of the agreement under Article 60 of the Vienna Convention on the Law of Treaties.[114] At most, they would trigger consultations, dispute-settlement procedures (where available) or reputational consequences.

For these reasons, association agreements under Article 217 TFEU appear to be a more suitable instrument than FTAs for addressing disinformation, especially in the EU's neighbourhood. Although they are more politically demanding to conclude, their scope is broader. They combine economic integration with political dialogue, foreign and security cooperation, regulatory approximation and commitments related to democratic principles, human rights (as defined in both binding and non-binding international instruments, eg, the Universal Declaration of Human Rights[115] and the ECHR) and the rule of law – whose breach may justify the suspension of Treaty benefits.

Within this wider framework, disinformation can be addressed as a component of a broader effort to strengthen democratic resilience, rather than an isolated issue. This is particularly relevant in accession and pre-accession contexts, where – as highlighted above – candidate and associated countries frequently become the target of foreign disinformation campaigns aimed at eroding support for European integration. Agreements with Moldova and Ukraine, and also Armenia, already include extensive commitments to comply with democratic principles and cooperate to develop, consolidate and enhance the stability and efficiency of democratic institutions and of the rule of law, supported by mechanisms of monitoring, dialogue and civil society participation.[116]

By treating democratic principles, the rule of law and fundamental rights as essential elements of the relationship and establishing frameworks for cooperation on media freedom and judicial reform, these agreements create conditions that allow for the indirect yet meaningful addressing of disinformation, and their structure is well suited to accommodating anti-disinformation provisions. Therefore, building on these frameworks, it seems that more specific commitments could be envisaged. These might include cooperation in detecting FIMI, establishing early-warning mechanisms during electoral periods, supporting independent media and fact-checking initiatives, ensuring transparency in media ownership, implementing media literacy programmes and facilitating exchanges between electoral and media regulators. They could also address emerging challenges, such as AI-generated content, through structured dialogue and joint risk assessments.

Crucially, such clauses would not require partner countries to restrict lawful expression, but to enhance transparency by jointly defining the means to achieve this outcome. Including them would also serve a broader strategic purpose. By reducing the impact of foreign disinformation campaigns, they would help to prevent the erosion of trust in EU institutions, which can otherwise slow down accession processes. Concurrently, they would contribute to preparing candidate countries for full compliance with EU values, as required by Article 49 TEU. Furthermore, as the EU is unlikely to conclude comparable agreements with States that are themselves the main originators of hostile disinformation – most notably Russia – these provisions would primarily strengthen the resilience of neighbouring countries that are particularly exposed to such interference. This would indirectly reduce the effectiveness of disinformation strategies that exploit institutional fragility and political instability in the EU's neighbourhood.

114 Vienna Convention on the Law of Treaties (adopted 22 May 1969, entered into force 27 January 1980) 1155 UNTS 331 (VCLT).

115 Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR).

116 Association Agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Moldova, of the other part (2014); Comprehensive and enhanced partnership agreement between the European Union and the European Atomic Energy Community and their Member States, of the one part, and the Republic of Armenia, of the other part (2018); Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part (2025).

DOI: 10.36633/ulr.1271

4. CONCLUSION

The EU has developed a growing arsenal of instruments to counter the 'hybrid warfare' of online disinformation orchestrated by foreign actors. As former High Representative Josep Borrell has suggested, these efforts may contribute to a strategic advantage in the defence of democratic systems.[117] However, the foregoing analysis demonstrates that no single instrument can be regarded in absolute terms as the most effective means of countering disinformation originating from actors outside the EU. Rather, what emerges is the need for a differentiated regulatory approach, combining unilateral measures and cooperative frameworks within the Union's external action. Each of these instruments offers specific strengths while also being subject to significant constraints, which it may be useful to highlight briefly.

Internal market instruments – most notably the DSA and related measures – provide the highest degree of legal certainty where a sufficient territorial or economic link to the Union can be established. They enable the imposition of binding obligations (eg, systemic risk assessment, content moderation procedures, disclosure of AI-generated content), supported by supervision mechanisms and judicial remedies. In practice, they represent the most robust response where disinformation is channelled through large platforms operating within or targeting the EU market (eg, TikTok, X, Facebook, YouTube or Telegram). Their effectiveness, however, remains conditioned by the existence of a connection to the internal market and by their focus on regulated service providers, which leaves parts of the broader disinformation landscape outside their scope.[118] These limits, combined with enforcement constraints, create gaps that may be exploited by actors capable of relocating activities or shifting to less regulated environments.

Restrictive measures adopted under the CFSP respond to a different logic. Although used sparingly in the disinformation context, they allow the EU to target the most severe forms of foreign interference, particularly when embedded in broader strategies of geopolitical confrontation. Their function is primarily deterrent. However, their scope remains narrow, as they are directed at specifically identified actors and have so far been tied to exceptional circumstances, often linked to armed conflict or acute threats to international security. Their intensity, as well as the potential implications for freedom of expression, makes them unsuitable as a general response to disinformation in ordinary political settings.

More broadly, reliance on predominantly unilateral instruments – whether regulatory or coercive – raises concerns relating to both effectiveness and legitimacy. Measures developed within the EU legal order do not operate in a vacuum: when projected externally, they interact with diverse political, legal and societal contexts. If perceived as overly prescriptive, they risk constraining legitimate counter-narratives, undermining pluralism, weakening the Union's normative credibility in global digital governance. Meanwhile, a strategy centred on unilateral enforcement may inadvertently encourage evasion, as disinformation networks have a high capacity to adapt by migrating to smaller platforms, exploiting decentralised technologies or moving to more permissive jurisdictions.[119]

Recent initiatives under the European Shield for Democracy[120] may address some of these shortcomings by improving enforcement coordination and institutional oversight.[121] Nevertheless, they do not fundamentally alter the structural tension between regulatory

117 2nd EEAS Report (n 1) 2.

118 From the second report on FIMIs, it emerged that 'new and niche platforms', in addition to the well-known Telegram and X, are involved in FIMI incidents (6).

119 For instance, some Russian companies have reportedly sought to circumvent or avoid EU-imposed sanctions by relocating to Serbia. As there is no general prohibition on foreign interference within the EU, those responsible for such conduct can be sanctioned only when their actions fall within the scope of an existing criminal offence. The Council could, pursuant to TFEU (n 111) art 83(1), adopt a decision identifying other areas of particularly serious crime with a cross-border dimension. See Directive (EU) 2024/825 of the European Parliament and of the Council of 28 February 2024 amending Directives 2005/29/EC and 2011/83/EU as regards empowering consumers for the green transition through better protection against unfair practices and through better information [2024] OJ L2024/825.

120 For an overview of the recent proposals put forward under the European Democracy Shield, see Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'European Democracy Shield: Empowering Strong and Resilient Democracies' JOIN(2025) 791 final.

121 To this end, in February 2025, the European Parliament established the European Shield for Democracy Committee, tasked, among other responsibilities, with assessing the effectiveness of EU mechanisms to counter disinformation.

ambition and jurisdictional reach, nor do they fully resolve concerns relating to proportionality and freedom of expression.

It is against this background that bilateral agreements acquire particular significance. While still underdeveloped in this field, they offer a complementary avenue that operates on a different premise: one centred on cooperation rather than unilateral imposition. Unlike internal regulatory interventions and sanctions, they enable shared development and gradual diffusion of standards and practices aimed at strengthening information integrity, thereby reducing the risk of circumvention while enhancing the legitimacy of the measures adopted.

Such engagement does not entail a dilution of core EU values, but it allows, instead, their promotion through adaptive and context-sensitive mechanisms. Especially in the case of association agreements, the EU can engage with partner countries in a way that contributes strengthening information integrity indirectly by reinforcing democratic institutions and safeguarding media pluralism against external interference. The successful realisation of this result, nevertheless, is reliant on the readiness and capability of partner nations to participate effectively in these obligations, as well as on the legal and political limitations that regulate the conclusion and execution of such treaties. Furthermore, bilateral cooperation is not a viable option in relations with openly adversarial States, where other instruments are necessary.

Overall, the considerations made in this paper suggest that the EU's responses to online foreign disinformation should be tailored to the specific context be tailored to the specific context. Where disinformation is disseminated via major platforms operating within the EU, existing legislation offers the most effective solutions. On the contrary, where it is directly attributable to hostile State actors and forms part of broader geopolitical strategies, restrictive measures may be justified. Where, instead, disinformation exploits vulnerabilities in neighbouring countries – often with indirect repercussions for the Union – bilateral agreements can play a crucial preventive role.

COMPETING INTERESTS

The author has no competing interests to declare.

AUTHOR AFFILIATIONS

Anna Fiorentini orcid.org/0009-0003-2164-6169
University of Bologna, IT

TO CITE THIS ARTICLE:
Anna Fiorentini, 'The EU's Arsenal to Protect Its Democracy from the Threat of Foreign Disinformation' (2026) 22(2) Utrecht Law Review 105–124. DOI: https://doi.org/10.36633/ulr.1271

Published: 29 October 2026

COPYRIGHT:
© 2026 The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC-BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited. See https://creativecommons.org/licenses/by/4.0/.

Utrecht Law Review is a peer-reviewed open access journal published by Utrecht University School of Law.