Not Only the Digital Services Act:

Systemic Threats to Freedom of Speech and the Integrity of Democratic Elections in the European Union

Edited by

Jerzy Kwaśniewski

Not Only the Digital Services Act: Systemic Threats to Freedom of Speech and the Integrity of Democratic Elections in the European Union

Edited by

JERZY KWAŚNIEWSKI

Ordo Iuris Institute for Legal Culture

Warsaw, 2026

Table of Contents

Executive summary

- The European Democracy Shield is intended to transform the European internet by making it a safe, heavily moderated space, where the dominant liberal views are promoted.
- This creates numerous challenges to the freedom of speech, in particular in its political aspect and, thus, is aimed at influencing elections in the Member States.
- These goals are to be attained mainly by way of a multi-layered moderation (i.e., censorship) process.
- Firstly, the EU demands the **creation of a robust notice and takedown framework**, whereby the balance should be tipped towards aggressive moderation rather than the preservation of the freedom of speech.
- Secondly, a pervasive **system of labelling** is to be introduced – speech is to be labelled by external providers as trustworthy or not; separate commentaries should provide information about given speech being fact-checked or likely to be fake news and also should indicate whether it constitutes a political ad or not, among other things.
- Moreover, online service providers should also ensure that the applied algorithms would remove any speech deemed as problematic.
- **The scope of the moderated speech** is defined **very broadly**. It concerns not only widely understood "illegal" content, but also speech labelled as "disinformation," "hate speech" or "divisive speech."
- Both the set **standards and the enforcement process** are organized in a **deeply undemocratic fashion.** The decisive role is given to the Commission's list of Member-State-approved NGOs cooperating with the competent regulatory authorities.
- Most of the aforesaid regulations are stipulated in the **Digital Services Act**, accompanied by a plethora of theoretically non-binding acts.
- These regulations are supplemented by **severe restrictions on political advertisement,** consisting of, most importantly, labelling obligations and severe restrictions on data use and targeting.
- **Aggressive enforcement** of the European Democracy Shield is secured by **severe sanctions** for both online service providers and the Member States showing too much leniency.

- Thus, the European Democracy Shield poses a clear and present danger to the freedom of speech and information within the EU, in particular with regard to conservative speech. These limitations aim specifically to influence political discourse in the EU.

Introduction

The U.S. House Judiciary Committee report titled "The Foreign Censorship Threat, Part II: Europe's Decade-Long Campaign to Censor the Global Internet and How it Harms American Speech in the United States"[1] was definitely a watershed moment. By bringing to a wider public the evidence of the EU's pressure on online service providers and, even more importantly, calling it by its real name, i.e., censorship, it galvanized the advocates of freedom of speech and gave a fresh impulse for even more robust engagement in its protection on both the national and European levels. The aim of this analysis is to supplement the Committee's factual findings by providing the broader legal background for this report.

As will be demonstrated below, in light of the regulations and soft law provisions adopted by the EU, the examples demonstrated in the report, shocking as they may be, should not come as a surprise. These provisions prove that the EU decided to take unprecedented steps in order to limit the freedom of speech on the European internet. In fact, one could even call it organized lawfare against online freedom of expression. What is even more disconcerting is that EU institutions are not even trying to hide this fact. This legislative offensive and its goals are fully described in the Commission's Communication on the European Democracy Shield, explaining in detail the goals and synergies between the EU acts regulating the EU digital marketplace.

The goal is to create a "safe and stable online environment" where EU citizens would be protected not only against directly harmful messages, such as pornography or those with violent content, but also against political speech diverging from the leftist-liberal orthodoxy. In particular, online service providers are expected to actively engage in fighting "hate speech," "disinformation," and other "divisive" or "discriminatory" content. The European Commission makes it clear that the achievement of these goals requires the creation of a multi-layered censorship framework. Not only are online service providers requested to introduce robust notice and takedown mechanisms, but they also have to label their users' speech, e.g., as fact-checked, untrustworthy, coming from untrustworthy sources, etc. Furthermore, speech qualified as a "political advertisement" should be expressly labelled as such, together with a lot of financial details. In order to ensure compliance, these censorship activities would be carried out not only by online service providers, but also by the supervising public authorities and Commission (Member State)-approved NGOs labelled as "fact checkers" or "trusted flaggers." The whole system clearly favors aggressive moderation rather than the protection of freedom of speech.

[1] *New Report Exposes European Commission Decade-Long Campaign to Censor American Speech*, 3 February 2026, House Judiciary Committee GOP, https://judiciary.house.gov/media/press-releases/new-report-exposes-european-commission-decade-long-campaign-censor-american, accessed: 1 March 2026.

Compliance with EU law is to be ensured by draconian penalties against both online service providers and the Member States that would like to tip the balance in favor of the freedom of speech.

The above is even more disconcerting since the limitations on freedom of speech are clearly linked to the electoral process in many of the EU's documents. The European Commission is not even trying to hide that one of the main goals of these regulations is to limit voter access to political speech contradicting the views of the Commission and predominantly liberal legacy media, to prevent such speech from influencing elections. In practice, this means limiting voters' exposure to the political speech of conservative parties that challenge the liberal *status quo*.

I. Existing framework: shielding democracy or shielding society from democracy?

1. Introduction

This section focuses on the analysis of the regulatory framework for limiting the freedom of speech in the EU's digital space, particularly in connection with democratic elections. In order to understand the meaning and function of these regulations, this section begins with the analysis of the Commission communications (i.e., soft law) rather than specific legislative acts. This approach, however, is fully justified since the European Democracy Shield Communication lays down in detail the aim and purpose of the encroachments upon the freedom of speech on the internet. The aim of the European Commission is nothing short of creating an isolated, heavily moderated information space under the constant supervision of the state authorities and NGOs, intensively promoting the legacy media. The main instrument serving this purpose is the Digital Services Act, a comprehensive regulation on the obligations of internet providers, stipulating an elaborate system of online surveillance conducted largely by EU-approved NGOs. This system is largely implemented by soft law acts, including "voluntary" codes of conduct. The Political Advertising Regulation is intended to limit the distribution of political advertisements on the internet. Thus, in conjunction with the Digital Services Act, it severely limits the possibilities to communicate political speech in connection with elections. In any case, the disconcerting features of these mechanisms are further amplified by other EU legislation limiting the freedom of speech in the context of data processing (the AI Act) or legal acts concerning specific sectors, such as the Directive on Combating Gender-based Violence.

2. EU Democracy Shield: A Necessary Safeguard or Instrument of Suppression

2.1. What is the European Democracy Shield?

On 12 November 2025, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy issued the Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions titled "European Democracy Shield: Empowering Strong and Resilient Democracies"

(**Democracy Shield Communication (DSC)**).[2] This document, although not legally binding and subsequent to most of the legal acts discussed in this analysis, from the logical standpoint should be viewed as the high-level framework for EU institutions' (the Commission's) attempts to reshape the public marketplace within the EU and its Member States. It contains not only a comprehensive and rather straightforward exposition of the Commission's goals, but also an explanation of the role to be played in the Commission's project by individual legal acts. Thus, this document should serve as the point of departure for further analysis. Unfortunately, despite the declared noble goals of strengthening democracy within the EU (and its Member States), this document instead proves the Commission's real agenda, which is to limit democratic discourse in the Member States and interfere with their electoral processes.

The document makes clear that its main aim is to protect EU citizens against the threats of populism, in particular by cutting them off from social media as a source of information (Democracy Shield Communication, pp. 1-2):

> *These threats do not come in isolation, but feed on and reinforce other important challenges democracy is facing today.* ***These include rising extremism and polarisation, declining trust*** *and engagement, threats to the integrity of elections and the plurality of public debate and free speech,* ***and a deterioration of the environment in which journalists and civil society operate*** (…). *These challenges come* ***amidst a deep digital transformation*** *of our societies which has reshaped the way in which public debate takes place, how information flows and how citizens engage in the public sphere...* (…) *However, it has also exposed and created new vulnerabilities.* ***People's views are being increasingly shaped by algorithm-based****, personalised sources,* ***which limits the shared space for democratic debate. Social media platforms also impact the sustainability of media revenue models. The developments in Artificial Intelligence (AI)*** *can also severely impact the democratic space, including electoral processes.*
>
> *Protecting democracy and building the democratic resilience of citizens, societies and institutions is an urgent collective endeavour, which requires a whole-of-government and whole-of-society approach.*

The answer to these challenges is unambiguous (DSC, p. 2):

> *Building on that framework,* (…) *the Commission and the High Representative for Foreign Affairs and Security Policy are presenting a set of new measures in three priority areas, aimed at empowering strong and resilient democracies by:*

[2] Joint Communication of 12 November 2025 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, https://commission.europa.eu/document/download/2539eb53-9485-4199-bfdc-97166893ff45_en?filename=JUST_template_comingsoon_standard_1.pdf, accessed: 1 March 2026.

> *– **reinforcing** situational awareness and support response capacity to safeguard **the integrity of the information space**,*
>
> *– strengthening democratic institutions, free and fair elections and **free and independent media,***
>
> *– boosting societal resilience and citizens' engagement.*

Of these, safeguarding the integrity of the information space is viewed as the most fundamental task. As explained by the Commission: "Strengthening the integrity of the information space to support everyone in society to access reliable and trustworthy information, exercise their democratic rights and engage meaningfully with institutions and communities is essential. Transparency, accountability and integrity in the information space are key for ensuring that people's voices are heard, to empower them to be active citizens and to build and sustain their trust in democratic processes." (DSC, pp. 4-5). The most pressing issues were defined as "the inauthentic use of social media, fake social media accounts, websites designed to mimic official sources, **artificial amplification of divisive content**, use of synthetic content like deepfakes and other Artificial Intelligence ('AI')- generated content." (DSC, p. 5).

According to the Democracy Shield Communication, these threats should be countered first and foremost by the Digital Services Act and the AI Act. While the latter should enable AI-generated content to be filtered out, the Digital Services Act is supposed to put pressure on the big internet platforms with regard to moderating the content uploaded by users and disclosing their algorithms. These acts are to be accompanied by other executive acts, of which the Code of Conduct on Disinformation,[3] explaining in detail the providers' obligations, is of particular importance (DSC, pp. 4-6).

In a broader perspective, the EU also seeks to attain this goal by supporting legacy media in opposition to online platforms. As stated by the Commission:

> ***Citizens rely increasingly on online platforms** and recently on generative AI to access information and form their opinions on a **wide range of issues, including politics**. Online platforms are becoming the main sources of information for young people, especially via influencers. **The algorithms that online platforms use to sort content drive engagement, often by prioritising sensational or controversial content** over reliable and substantiated information. This risks amplifying disinformation, societal divisions and challenges the visibility of media content. (DSC, pp.16-17)*

Consequently, the Commission stated that

> *To ensure that the providers of VLOPs and VLOSEs [i.e. social media and search engines providers] pay due regard to media freedom and pluralism, the DSA*

[3] Code of Conduct on Disinformation, available at *The Code of Conduct on Disinformation*, European Commission,13 February 2025, https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation, accessed: 1 March 2026.

> *requires that they **diligently identify and mitigate any systemic risks** stemming from the design or functioning of their services, including as regards freedom and pluralism of the media. (DSC, p. 17)*

In this respect, the Audiovisual Media Services Directive is expected to play the main role.[4]

One of the main goals of insulating the European informational space is "strengthening the fairness and integrity of electoral and other democratic processes," with the elections in Romania somewhat interestingly being referred to as a case showing the need for deeper EU involvement (DSC, p.10). In this respect, the Political Advertising Regulation is declared the main tool, which should "**make it easier for citizens to recognise political** ads, know if they are targeted by such ads, and distinguish them from other types of content and ban the provision of ads to third country sponsors in the three months before an election or referendum in an EU country," as well as store information on the persons involved in the preparation of political ads (DSC, p. 11). In addition, the EU plans to supplement these actions by creating common references, joint standards, and guidelines related thereto, with a prominent role to be played by the Commission Guidelines for Mitigation of Systemic Risks for Electoral Processes[5] (DSC, p. 12).

In addition, these measures should be facilitated by promoting citizen engagement and participation, entailing providing networking venues, support, and financing for NGOs (pp. 23-27).

To coordinate and facilitate these activities, a new European institution was to be created—the **European Centre for Democratic Resilience (ECDR)**. **It started its operations on 24 February 2026**.[6] According to the official communication, it is "to facilitate a consolidated approach involving all of society to increase awareness and boost the capacity to respond to the threats faced by democracies today, and build democratic resilience," and its flagship activities for the first year should include:

- ***Developing tools to support resilient elections**, including by bringing together relevant existing EU rules, soft measures and tools for Member States **that help address Foreign Information Manipulation and Interference (FIMI)** and **disinformation campaigns** targeting electoral processes in the Member States.*

[4] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services, PE/33/2018/REV/1, OJ L 303, pp. 69–92, https://eur-lex.europa.eu/eli/dir/2018/1808/oj, accessed: 1 March 2026.

[5] Communication from the Commission – Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/2537, OJ C, C/2024/3014, 26.4.2024, https://eur-lex.europa.eu/eli/C/2024/3014/oj/eng, accessed: 1 March 2026.

[6] *The new European Centre for Democratic Resilience starts its work*, European Commission, 24 February 2026, https://enlargement.ec.europa.eu/news/new-european-centre-democratic-resilience-starts-its-work-2026-02-24_en, accessed: 1 March 2026.

- ***An EU blueprint to counter FIMI and disinformation*** *intended to support preparedness and help to build capacities across the Union.*
- ***Launching a dedicated Stakeholder Platform bringing together independent actors like civil society organisations****, think tanks, researchers, academia,* ***fact-checkers*** *and media organisations* ***to support the dissemination of research*** *and other output and encourage exchange among different stakeholders, providing knowledge and insights to work with Member States in the Centre.*
- ***Fostering capacity building and mutual learning,*** *including sharing of expertise and best practices, enabling Member States with* ***advanced experience in countering FIMI and strengthening democratic resilience*** *to support others, raising the overall level of preparedness across the EU.*

  (…)

- *explore various models for* ***involving citizens*** *in our efforts* ***to protect democracy, building on the valuable experience developed in many Member States****. The Commission will support this reflection by organizing this year* ***two citizens panels*** *on preparedness and on building democratic resilience.*

While the ECDR is, undoubtedly, the most important element of the institutional framework for the democracy shield, it is only one of the network of institutions, encompassing, among others, the European Network of Fact Checkers (a network of NGOs supported by the Commission), the European Digital Media Observatory (a research and analysis institution), a common research framework to be established by the Commission, and the FIMI Toolbox (DSC, pp. 6-7).

2.2. Key Takeaways

A. The analysis above clearly indicates that the Democracy Shield Communication shows that the European Commission not only wishes to create an EU-information space, but also adopted a comprehensive and interdisciplinary approach to attain this goal. While the aim itself sounds laudable, the means utilized to achieve it raise numerous concerns, many of which threaten the freedom of expression and democratic debate, in particular in the context of elections.

B. To begin with, the ideal information landscape sought by the Commission would entail first and foremost the legacy media accompanied (out of necessity) by severely weakened social media, controlled by in-house and external censors and "fact-checkers" and populated by influencers and entities having the backing or, at least, acceptance of the European Commission. This is obviously deeply concerning.

C. If a certain political party, critical of the policy goals and narratives promoted by the European Commission, for example with regard to energy transformation or mass migration, wanted to take its message to the broader public, it would face immense difficulties. First and foremost, the legacy media would not be likely to promote their views due to the overwhelming majority of their workers supporting the liberal agenda. Furthermore, it would be immensely difficult for them to reach a broader audience. Firstly, their options with regard to sending a political message would be severely limited due to restrictions on political advertisement in social media, encompassing, among others, a practical ban on utilizing personalized ads and limitations on the group of recipients. Secondly, their message shared on social media would be subject to various forms of intervention by both internet censors and "fact-checkers." At the same time, their opponents would likely not only have the support of the legacy media, but also could promote their views within the framework of government-sponsored, allegedly only informative advertising campaigns. Similarly, most likely their message would be less prone to intervention by the government-funded censors and "fact-checkers."

D. Looking at the matter from the perspective of citizens, not only would their ability to communicate their views be impaired (their posts would be subject to "fact-checking" or even censorship), but they would also be effectively insulated from the political speech representing views diverging from the liberal mainstream.

3. Digital Services Act – the main tool for shaping the EU's digital market

3.1. Introduction

As explained above, 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 (the "**Digital Services Act**") is the cornerstone of the EU's regime for the digital services market. Given the breadth of the regulation, the analysis conducted here will focus on selected provisions of fundamental importance for the freedom of speech and democratic debate accompanying the election process.

Furthermore, we also address the supplementary acts (guidelines and codes of conduct) due to their practical relevance to the operational enforcement of the aforesaid provisions and at least indirectly their binding character.

3.2. Digital Services Act

First, it should be emphasized that this act is a **regulation.** This means, that, unlike the directives discussed above, similar to acts of international law, which have to be implemented into the national legal order of Member States by national legislation, the Digital Services Act is directly applicable to the Member States by their administrative agencies and courts. Any national legislation would serve the purpose of only implementing the Digital Services Act provisions or filling in any legislative gaps.

The scope of regulation of the Digital Services Act is extremely broad, so as to cover the functioning of intermediary services that are to be provided on the territory of the EU (Articles 1-2). Consequently, it is applicable also to social media platforms and search engines such as Google, Facebook and X. Its aim is to create "**a safe, predictable and trusted online environment** that facilitates innovation and in which fundamental rights enshrined in the Charter, including the principle of consumer protection, are effectively protected" (Article 1.1 of the DSA). As elaborated further in the Preamble (para. 9), its goal is to address "**the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate**, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated."

In the pursuit of this goal, among others, the DSA foresees the creation of notice and takedown mechanisms (Article 16 of the DSA) and any sanctions should be justified (Article 17 of the DSA). Further, online platform providers should also have a redress system for the victims of content moderation. Furthermore, as per Article 23 of the DSA, the providers of online platforms should suspend accounts generating a disproportionate amount of illegal content or

manifestly unfounded complaints. Platform providers are obliged to produce yearly reports on their activities (Article 24).

Operators of very large online search engines and platforms (e.g., Google, YouTube, Facebook, X) have additional obligations, one of the most important being the obligation to make a risk assessment. As per Article 34.1 of the DSA:

> *This risk assessment shall be specific to their services and proportionate to the systemic risks, taking into consideration their severity and probability, and shall include the following systemic risks:*
>
> *(a) the* ***dissemination of illegal content*** *through their services;*
>
> *(b) any* ***actual or foreseeable negative effects*** *for the exercise of fundamental rights, in particular the fundamental rights to human dignity enshrined in Article 1 of the Charter, to respect for private and family life enshrined in Article 7 of the Charter, to the protection of personal data enshrined in Article 8 of the Charter,* ***to freedom of expression and information, including the freedom and pluralism of the media****, enshrined in Article 11 of the Charter, to non-discrimination enshrined in Article 21 of the Charter, to respect for the rights of the child enshrined in Article 24 of the Charter and to a high-level of consumer protection enshrined in Article 38 of the Charter;*
>
> *(c) any actual* ***or foreseeable negative effects on civic discourse and electoral processes,*** *and public security;*
>
> *(d) any* ***actual or foreseeable negative effects in relation to gender-based violence****, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being.*

Illegal content should be understood widely. As per Motif 12 of the Preamble,

> *In particular, the concept of* ***'illegal content'*** *should be defined broadly to cover information relating to illegal content, products, services and activities. In particular, that concept should be understood to refer to information, irrespective of its form, that under the applicable law is either itself illegal,* ***such as illegal hate speech*** *or* ***terrorist content*** *and* ***unlawful discriminatory content*** (…).

For the avoidance of doubt, the systemic risks should be understood even more broadly. As per para. 84 of the Preamble:

> *When* ***assessing the systemic risks*** *identified in this Regulation, those providers should also focus* ***on the information which is not illegal, but contributes to the systemic risks*** *identified in this Regulation. Such providers should therefore* ***pay particular attention on how their services are used to disseminate or amplify misleading or deceptive content****, including* ***disinformation****.*

Article 35.1 explains the ways to mitigate the risks, such as, among others:

> *(b)* ***adapting their terms and conditions and their enforcement****;*
>
> *(c)* ***adapting content moderation processes****, including the speed and quality of processing notices related to specific types of illegal content and, where appropriate, the expeditious removal of, or the disabling of access to, the content notified, in particular* ***in respect of illegal hate speech*** *or cyber violence, as well as adapting any relevant decision-making processes and dedicated resources for content moderation;*
>
> *(d) testing and adapting* ***their algorithmic systems****, including their recommender systems;*
>
> (…)
>
> *(g)* ***initiating or adjusting cooperation with trusted flaggers*** *in accordance with Article 22 and* ***the implementation of the decisions of out-of-court dispute settlement bodies*** *pursuant to Article 21;*
>
> *(h)* ***initiating or adjusting cooperation with other providers of online platforms or of online search engines through the codes of conduct*** *and the crisis protocols referred to in Articles 45 and 48 respectively;*
>
> *(I)* ***taking awareness-raising measures*** *and adapting their online interface in order to give recipients of the service more information;*

In light of the above, it is thus clear that not only are many systemic risks identified with the content of the speech of internet platform users, but also service providers are invited to aggressively moderate the content of users together with NGOs (trusted flaggers – see *infra*). The ideological character of these ambiguous concepts is evident in the light of the codes of conduct and other non-binding documents discussed below. The main legal basis for them is stipulated in Article 45 of the DSA. Its paragraph 2 stipulates that the codes of conduct may be created especially where there exists a systemic risk as per Article 34 of the DSA. What merits attention is that these codes should be drawn up not only by the representatives of the industry, but also by the authorities and "civil society organisations and other relevant stakeholders." Moreover, online service providers are expected to create and implement voluntary standards relating to technical aspects of their functioning (Article 44 of the DSA).

Article 36 lists the Commission's tools to interfere with very large online service providers in matters related to mitigating systemic risks, while Article 37 specifies the obligation to conduct yearly audits.

Preferential treatment, however, should be provided to the so-called trusted flaggers whose notices should be given priority and be decided without delay (Article 22.1 of the DSA). As per Article 22.2 of the DSA, the status of

> *'**trusted flagger**' under this Regulation shall be awarded, upon application by any entity, by the Digital Services Coordinator of the Member State in which the applicant is established, to an applicant that has demonstrated that it meets all of the following conditions:*
>
> *(a) it **has particular expertise and competence for the purposes of detecting, identifying and notifying illegal content**;*
>
> *(b) it is **independent from any provider of online platforms**;*
>
> *(c) it carries out its activities for the purposes of submitting notices diligently, accurately and objectively.*

Furthermore, the trusted flaggers have to prepare yearly reports on their activities. In practice, as discussed in other parts of this analysis, only NGOs meeting the requirements set by the Commission would be trusted flaggers.

3.3. GUIDELINES AND CODES OF CONDUCT

3.3.1. Electoral Process Guidelines

In order to enhance the enforcement of the DSA, the European Commission issued Commission Guidelines of 26 April 2024 for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, C/2024/3014 (the "**Electoral Process Guidelines**"). The Commission was rather straightforward in defining what danger these Guidelines should help to avoid. In para. 3, the Commission stated:

> *A wide range of phenomena involving online platforms and search engines give rise to a heightened risk to election integrity. These include, but are not limited to, the **proliferation of illegal hate speech** online, threats linked to foreign information manipulation and interference ("FIMI") as well as the **wider phenomenon of disinformation**, the spread of (violent) **extremist content and such with the intent to radicalise people**, as well as the spread of content generated through new technologies such as generative Artificial Intelligence ("AI").*

As per para. 12, the Guidelines are aimed at the providers of "Very Large Online Platforms and Search Engines" (i.e., in particular, Google, YouTube, Facebook and X). The obligations of such entities in respect of these platforms are specified by stressing the need for the operators "to have adequate content moderation resources with local language capacity and knowledge of the national and/or regional contexts and specificities," whereby they should also "ensure they have adequate internal processes to take into account **independent analyses** of the state of media

freedom and pluralism, such as the Media Pluralism Monitor, knowledge of media literacy initiatives and indicators, and information on the existence **of an enabling space for civil society organisations** to participate in policy-making and civic discourse" (para. 21). In addition, they should "consider setting up **a dedicated, clearly identifiable internal team** prior to each individual electoral period, which should cover all relevant expertise including in areas such as **content moderation**, **fact-checking,** threat disruption, hybrid threats, cybersecurity, **disinformation and FIMI**, **fundamental rights** and public participation and cooperate with relevant **external experts**, for example with the **European Digital Media Observatory** (EDMO) hubs and independent **fact-checking organisations**" (para. 22). Further, these mitigation measures should be guided, among others, by codes of conduct related to hate speech and disinformation "as well as recommendations from civil society, such as those from the Civil Liberties Union for Europe and European Partnership for Democracy" (see *supra*).

As to the substance, the mitigation measures should encompass, among others, "**Fact**-checking **labels** on identified disinformation and FIMI content **provided by independent fact-checkers** and fact-checking teams **of independent media organisations**; and **Tools and information to help users assess the trustworthiness** of information sources, such as trust marks focused on the integrity of the source based on transparent methodologies and **developed by independent third parties**" (para. 27).

In addition, on the technical front, service providers should consider, among other things: "Ensuring that recommender systems are designed and adjusted in a way that gives users meaningful choices **and controls over their feeds**, with due regard to media diversity and pluralism; **Establishing measures to reduce the prominence of disinformation** in the context of elections based on clear and transparent methods, e.g., regarding deceptive content that **has been fact-checked** as false or coming from accounts that have been repeatedly found to spread disinformation; **Demonetisation of disinformation content"** (para. 27).

In order to ensure that these steps would be most effective, "the Commission recommends that providers of VLOPs and VLOSEs **collaborate with independent fact-checking organisations** that **adhere to high standards of methodology, ethics and transparency,** for example by being a member of the European Fact-Checking Standards Network (EFCSN) and following its Code of Standards" (para. 50).

3.3.2. Hate Speech Code of Conduct +

The revised Code of Conduct on Countering Illegal Hate Speech Online + (the "**Code of Conduct+**"), which was integrated into the Digital Services Act framework on 20 January 2025[7] (the "**Hate Speech CoC**"), is a self-governance act signed by many large online platforms,

[7] Code of conduct on countering illegal hate speech online +, available at *The Code of conduct on countering illegal hate speech online* +, European Commission, 20 January 2025, https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online, accessed: 1 March 2026.

including Google, Facebook and YouTube that, however, has legal significance by virtue of Article 45 of the DSA. The signatories of this code obliged themselves "to have in place terms and conditions informing users that they prohibit illegal hate speech on their services" (para. 1.1). According to para. 2.1, "the Signatories will have in place notice and action mechanisms to allow any user in the EU, **including Trusted Flaggers** [i.e., Commission-approved NGOs], to notify them of the presence on their service of specific content that **the user considers to be illegal hate speech content**." Further, "[a]fter receiving a valid notice, the Signatories will review it in a timely, diligent, non-arbitrary and objective manner and act expeditiously to remove or to disable access to the reported content" (para. 2.2). They should also "review the majority (at least 50%) of notices received (…)" (para. 2.3). To boost their effectiveness, the online platforms oblige themselves to share knowledge under the auspices of the Commission (para. 4). The effectiveness of the steps taken by the online platforms is to be measured annually, within the framework of monitoring exercises, where the effectiveness of the platforms' internal procedures would be measured by Commission-approved NGOs (Annex 1).

3.3.3. Disinformation Code of Conduct

The Revised Code of Conduct on Disinformation of 16 June 2022, integrated into the Digital Services Act legal framework on 13 February 2025 (the "**Disinformation CoC**")[8] was also signed by most of the biggest online service providers, including Google and Facebook, and selected civil society organizations. Its core areas include, among others, the demonetization of disinformation, and empowering the fact-checking community as well as strengthening reporting and monitoring (pp. 6-7).

In order to demonetize disinformation (Measure 1.1):

> *Relevant Signatories involved in the selling of advertising, inclusive of media platforms, publishers and ad tech companies, will deploy, disclose, and enforce policies with the aims of:*
>
> • *First,* ***avoiding the publishing and carriage of harmful disinformation*** *to protect the integrity of advertising supported businesses;*
>
> • *Second,* ***taking meaningful enforcement and remediation steps*** *to* ***avoid the placement of advertising next to disinformation content*** *or on sources that repeatedly violate these policies.*

According to Measure 2.2:

[8] Code of Conduct on Disinformation, available at *The Code of Conduct on Disinformation*, European Commission,13 February 2025, https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation, accessed: 1 March 2026.

> *Relevant Signatories will develop tools, methods, or partnerships, which may* ***include reference to independent information sources*** *both public and proprietary (for instance* ***partnerships with fact-checking*** *or* ***source rating organisations****, or services providing* ***indicators of trustworthiness****, or proprietary methods developed internally) to identify* ***content*** *and* ***sources as distributing harmful disinformation****, to identify and take action on ads and promoted content that violate advertising policies regarding disinformation* (…).

According to Commitment 6:

> *Relevant Signatories commit to make political or issue ads* ***clearly labelled and distinguishable as paid-for content*** *in a way that allows users to understand that the content displayed contains political or issue advertising.*

Measure 18.1 contains a commitment to:

> *mitigate risks of their services fuelling the viral spread of harmful disinformation, such as:*
>
> • *Recommender* ***systems designed to improve the prominence of authoritative information*** *and reduce the prominence of disinformation based on clear and transparent methods and approaches for defining the criteria for authoritative information* (…).

According to Measure 18.2:

> *Relevant Signatories will develop and enforce publicly documented, proportionate policies to limit the spread of harmful false or misleading information (depending on the service, such as* ***prohibiting, downranking, or not recommending*** *harmful* ***false or misleading information****, adapted to the severity of the impacts and with due regard to freedom of expression and information); and* ***take action on webpages or actors*** *that persistently violate these policies.*

According to Measure 21.1:

> *Relevant Signatories will further* ***develop and apply policies****, features, or programs across Member States and EU languages to help users benefit from the context and* ***insights provided by independent fact-checkers*** *or* ***authoritative sources****, for instance* ***by means of labels****, such as labels indicating* ***fact-checker ratings****, notices to users who try to share or previously shared the rated content, information panels, or* ***by acting upon content notified by fact-checkers*** *that violate their policies. When* ***cooperating with independent fact-checkers*** *to label content on their services, Relevant Signatories will further develop and apply tools or features to inform users, through measures such as labels and notices, that the content they interact* ***with has been rated by an independent fact-checker****, and work to implement them across all EU Member States languages.*

According to Commitment 22:

> *Relevant Signatories commit to* ***provide users with tools to help them make more informed decisions*** *when they encounter online information that* ***may be false or misleading****, and to facilitate user access to tools and* ***information to assess the trustworthiness*** *of information sources, such as* ***indicators of trustworthiness*** *for informed online navigation, particularly relating to societal issues or debates of general interest.*

In order to close any loopholes, as per Commitment 25, private messaging service providers undertake to include features limiting the possibility of disseminating disinformation, by, for example, preserving the labelling of forwarded links from social media or limiting the possibility of forwarding links leading to suspicious pages to many accounts.

To ensure the proper quality of the disinformation control, as per Measure 30.1:

> *Relevant Signatories will set up* ***agreements between them and independent fact-checking organisations*** *(as defined in whereas (e)) to* ***achieve fact-checking coverage in all Member States****. These agreements should meet high ethical and professional standards and be based on transparent, open, consistent and non-discriminatory conditions, and will ensure the* ***independence of fact-checkers.***

Furthermore, as per Measure 30.2:

> *Relevant Signatories* ***will provide fair financial contributions*** *to the* ***independent European factchecking organisations*** *for their work to combat disinformation on their services. Those financial contributions could be in the form of individual agreements, of agreements with multiple fact-checkers or with an elected body representative of the independent European fact-checking organisations that has the mandate to conclude said agreements*

To provide full effect to the above Measures, as per Commitment 31:

> *Relevant Signatories* ***commit to*** *integrate, showcase,* ***or otherwise consistently use factcheckers' work*** *in their platforms' services, processes, and contents, with full coverage of all Member States and languages,*

Whereby, as per Commitment 32:

> *Relevant Signatories commit to provide fact-checkers with prompt, and whenever possible, automated, access to information that is pertinent to help them to maximise the quality and impact of fact-checking,*

As per Commitment 28, online platform providers are to support "good faith research" on disinformation, including by financing the research.

These provisions are supplemented by institutional provisions on creating a permanent task force and monitoring compliance with the code.

These rather aggressive fact-checking activities are to be balanced by the commitment to introduce a transparent and swift appeal mechanism (Commitment 24).

3.4. Effects of the Digital Services Act

The effects of the Digital Services Act, together with the implementing acts on freedom of speech and the electoral debate, are both profound and disconcerting. The Digital Services Act introduces multi-layered content moderation as the general rule for operating an online services platform. Internet services providers are made responsible for the content of the speech of platform users. Therefore, they should cooperate and be supervised by both EU and national regulators and Commission-approved NGOs (called "fact-checkers," "trusted flaggers," etc.).

The first area of concern is the scope of moderation obligations since social media platforms would be obliged to filter not only directly harmful content, such as incitation to or graphic depictions of violence, pornography, etc., but also content falling under the umbrella of ambiguous concepts, such as "illegality" or "hate speech." Further, it should be noted that, in addition to being ambiguous, these words have also leftist-liberal connotations. Consequently, it is clear that it would be political speech challenging the leftist-liberal consensus (i.e., "conservative" or "populist" speech) that would be particularly vulnerable to censorship.

The above dangers are even more evident due to the role granted to the European Commission- and Member State-approved NGOs conducting fact-checking or combating hate speech and disinformation. They are to be involved on many levels. To begin with, they shall enjoy a privileged position with respect to the removal of contested content from the online platforms. Furthermore, they shall participate in the drafting of the moderation standards that would later be enforced against platform users on many levels, e.g., by performing ongoing mandatory consultations, sitting in the permanent consultation and standard-setting bodies or by conducting mandatory reviews of the effectiveness of the policies adopted by a given social platform. Thirdly, they are supposed to directly interfere with the content of online speech, first and foremost by attaching labels indicating the trustworthiness of the information or its source, fact-checker assessment, etc. Last but not least, they are also expected to educate EU citizens by providing them with digital media literacy education.

The above structure of the moderation framework should also raise concerns. To begin with, the DSA introduces a robust notice and takedown framework with little, if any, regard to the rights of the authors of incriminating speech. Within the framework of such measures, preferential treatment shall be given to complaints submitted by the Commission (Member State)-approved NGOs. In this context, it should be remembered that compliance is to be ensured also by the fact that the same NGOs would conduct yearly reviews of the online platforms' conformity with the DSA and submit them to the competent authorities. Censorship obligations are not only to be reactive, however. Platforms are also expected to label their users' speech, largely by integrating into it materials prepared by external NGOs, usually in the form of a label (e.g., indicating the degree of the posted information's trustworthiness, containing the comments of

fact-checkers, the trustworthiness of the source, etc.). At the same time, the NGOs fighting unwanted content are invited to co-create the very standards they are going to implement within different frameworks, networks, etc., including through educational actions aimed at the general public, such as digital media literacy classes. Last but not least, online operators are expected to alter platform algorithms so that any information deemed non-compliant with the EU regulations would be more difficult to be listed by search engines.

Finally, the aforesaid negative effects on freedom of speech are further amplified by the fact that the Digital Services Act is only one of the elements, albeit a crucial one, of the Democracy Shield, and there are harsh penalties for online operators showing too much leniency towards unwelcome speech. These issues are examined in more detail below.

4. Political Advertising Regulation

4.1. Political Advertising Regulation

Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (text with EEA relevance), OJ L, 2024/900 (the "**Political Advertising Regulation**") is an act regulating the rules on disseminating political advertisements in the EU. The act was adopted as a regulation, thus is directly applicable. It entered into force in April 2024 and most of its provisions became applicable as of 10 October 2025. The Political Advertising Regulation is accompanied by the official Guidelines of 8 October 2025 to support the implementation of Regulation (EU) 2024/900 on the transparency and targeting of political advertising (C(2025) 6829 final) (the "**Political Advertisement Guidelines**").

First of all, it should be noted that the Regulation applies to all providers of political advertisements in the EU, regardless of their seat. According to Article 2.1 of the Regulation:

> *This Regulation applies to political advertising where the political advertisement is disseminated in the Union, is brought into the public domain in one or several Member States or is directed to Union citizens, irrespective of the place of establishment of the provider of political advertising services or of the place of residence or establishment of the sponsor, and irrespective of the means used.*

The concept of "political advertisement" was defined in Article 3(2) rather broadly as:

> *the preparation, placement, promotion, publication, delivery or* ***dissemination, by any means, of a message, normally provided for remuneration or through in-house activiti****es 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,*

with the exception of official means of communication. Article 8, aimed at providing further guidance with regard to the definition of an advertisement, specifies that:

> *1. For the purpose of determining whether a message constitutes political advertising within the meaning of Article 3, point 2, point (b), account shall be taken* ***of all its features****, including: (a) the content of the message; (b) the sponsor of the message; (c) the language used to convey the message; (d) the context in which the message is conveyed, including the period of dissemination; (e) the means by which the message is prepared, placed, promoted, published, delivered or disseminated; (f) the target audience; (g) the objective of the message.*

This definition is clearly excessively broad and not very helpful in, for example, discriminating between political advertisements and social awareness campaigns. This is particularly true since all these concepts are to be understood dynamically, which means that the same entity, such as a charitable organization, may or may not provide services concerning political advertisements. These ambiguities are even more disconcerting given that, as openly admitted in para. 20 of the Regulation, this is the first EU legal act containing a definition of political advertisements.

Similar ambiguities surround the role of social media and search engine providers, who are generally excluded from the scope of application of the regulation, yet may become involved in the process of political advertisement, e.g., by boosting the visibility of the materials falling under the definition. As explained by the Commission in its Guidelines (example to para. 1.2.1.1):

> *A political party requests a provider of a social media network to perform a political advertising service and* ***pays the provider of a social media network for boosting three new messages*** *it posted on its social media account. By boosting these three posts against specific remuneration, the provider of the social media* ***network provides a political advertising service*** *and would constitute a political advertising publisher under the Regulation.*

This classification is of extreme importance since the EU legislators impose a plethora of specific obligations connected to the status of political advertisement service providers. Articles 11-14 specify extensive information obligations. For example, political advertisements should be clearly labelled as such, so that recipients can instantly recognize a given message as a political advertisement and learn important details concerning, among others, the entity financing it, the amount of financing, etc.

Rather unsurprisingly, Article 15 obliges the publishers of political advertisements to implement robust notice and takedown mechanisms, enabling any interested parties to report political advertisements non-compliant with the Regulation.

The trickiest part concerns the text related to personal data protection, as the Political Advertising Regulation introduces a specific regime for acquiring consent for processing data for the purpose of political advertisements. According to Article 18:

> *1. Targeting techniques or ad-delivery techniques that involve the processing of personal data in the context of online political advertising shall be permitted* ***only when the following conditions are fulfilled****:*
>
> *(a) the controller* ***collected*** *the personal data from* ***the data subject****;*
>
> *(b) the data subject has* ***provided explicit consent*** (…) *to the processing of personal data separately for the purpose of political advertising; and*
>
> *(c) those* ***techniques do not involve 'profiling'*** *as defined in* (…) *using special categories of personal data referred to in* (…).
>
> *2. In the context of political advertising, targeting techniques or ad-delivery techniques that involve the processing of the personal data of a data* ***subject that is known by the controller with reasonable certainty to be at least one year under the voting age*** *established by national rules* ***are prohibited****. Compliance with the obligations set out in this paragraph shall not oblige the controller to process additional personal data in order to assess whether the data subject is one year under the voting age.*
>
> (…)
>
> *4. For the purposes of implementing the requirements of Regulations (EU)* (…) *on* ***providing explicit consent****, as well as on withdrawing it once given, controllers shall make sure that:*
>
> *(a) the data subject is not requested to consent if he or she has already indicated by automated means that* ***he or she does not consent to data processing for political advertising purposes,*** *unless the request is justified by a substantial change of circumstances;*
>
> *(b) the data subject who does not give his or her consent is to be offered an equivalent alternative for using the online service without receiving political advertising.*

These limitations are further underlined in the Regulation's Preamble:

> *(77) Targeting techniques and ad-delivery techniques involving profiling using special categories of personal data referred to* (…) *should be prohibited in the context of online political advertising****. It should not be possible to rely on the exceptions laid down in*** (…) ***for using those techniques in the context of online political advertisin****g. The use of targeting techniques and ad-delivery techniques involving the processing of personal data, other than special categories of personal*

data, in the context of online political advertising ***should only be permitted when it is based on personal data collected from the data subjects and with their explicit consent, provided separately for the purposes of political advertising.*** (…) *Targeting techniques and ad-delivery techniques, when used under the conditions set out in this Regulation, can be useful in disseminating political advertising and information and in reaching out to and informing citizens.*

(78) ***Data controllers should not use personal data obtained from third parties for the purposes of targeting or ad delivery of political advertising****. To help prevent manipulative microtargeting, it is essential that providers of political advertising services take specific measures to ensure that the personal data which is collected and processed for the purpose of targeting and ad delivery of political advertising is limited to what is necessary* (…).

In light of the above, it is clear that the Regulation imposes severe limitations on the ability of political actors to look for new supporters. Restrictive provisions on consent (specific consent to the receipt of political advertisements), data utilization (a ban on using data from third parties; limitations on microtargeting), and due diligence obligations regarding protecting minors from receiving political advertising severely limit the actual possibility of political advertising in the EU.

The above limitations are not offset by the explicit exemptions foreseen for political speech communicated in a personal or editorial capacity (Article 1) or official (governmental) communications.

4.2. EFFECTS OF THE REGULATION

The Political Advertising Regulation has already had a chilling effect on political advertisement in the EU. Even taking into account the Commission Political Advertisement Guidelines, the legal framework is opaque and creates many legal risks for the entities involved (or that may become involved) in the process of disseminating political advertisements.

The most important ambiguities concern the very definition of a political advertisement. It is a new concept of EU law, having no clear equivalent in the legal systems of the EU Member States. While the Political Advertising Regulation contains lengthy definitions, which are further accompanied by the Commission's guidelines, they provide little, if any, guidance with regard to borderline cases, such as campaigns regarding contentious societal issues that may be associated with elections or referendums, although not being directly part of a political agenda. Examples may vary, and include immigration, same-sex unions, abortion, and climate change. Consequently, there is a risk that campaigns organized by civil organizations, such as NGOs, religious movements, etc., could be labelled as political advertisement and their sponsors punished for failing to comply with the requirements of the Political Advertising Regulation. As a result of the murky criteria and the biased approach of the European Commission and most

of the national regulators, the majority of whom are servants of the leftist-liberal establishment, it is clear that the Regulation has a chilling effect on the public activity of conservative actors.

Secondly, reasonable doubts arise in relation to restrictions on the use of private users' personal data. According to the Political Advertising Regulation, political advertisement service providers may use personal data covered by the GDPR only upon the explicit consent of the affected parties. It is not clear what exactly should be understood as explicit consent in this respect. Would traditional consent contained in the terms and conditions of a service provider suffice? Or should it meet higher standards? These problems are even more daunting if one takes into account that these provisions would be enforced by the data protection authorities of different Member States that do not necessarily adopt the same approach. Consequently, any targeted political ad would run the risk of violating the provisions of EU law, entailing substantial fines for the service provider.

Thirdly, one could debate the effect on the freedom of speech of labelling requirements that are limited solely to political advertisements, clearly separating them from the information obtained from the sources approved by the Commission.

The threats discussed above are by no means purely theoretical. Quite the contrary, in response to the EU's regulations, some of the biggest social media platforms, such as Facebook and YouTube, have decided to ban any political ads within the understanding of the Political Advertising Regulation from their platforms.[9] Thus, political parties and other actors (social movements, NGOs, etc.) have been deprived of the possibility of presenting their views to a broader audience, including the most important group, swing voters. Needless to say, this situation is particularly burdensome for those who have limited access to "traditional" communication channels, such as public broadcasters, newspapers, and other legacy media. Given the preponderance of liberal parties and the general left-leaning orientation of the majority of the "traditional" media outlets within the EU, this means that the Regulation disproportionally targets the ability of conservative political actors to communicate their political ideas.

5. Other Acts

[9] For Facebook, see S. Jeffers, *Meta and Google's Ad Ban Upends Political Campaigning in Europe*, Tech Policy, 22 October 2025, https://www.techpolicy.press/meta-and-googles-ad-ban-upends-political-campaigning-in-europe, accessed: 1 March 2026; for Google, see A. Kroeber-Riel, An update on political *advertising in the European Union*, Google – The Keyword,14 November 2024, https://blog.google/company-news/inside-google/around-the-globe/google-europe/political-advertising-in-eu and *Update to Political Content policy (September 2025)*, Support Google – Advertising Policies Help, 5 August 2025, https://support.google.com/adspolicy/answer/16409999?hl=en, both accessed: 1 March 2026.

While the acts discussed above constitute the main tools for limiting freedom of speech in the EU, the Democracy Shield architecture is more than that. It also encompasses many other acts, which, however, do not target freedom of speech in such a direct manner.

Of them, particular attention should be paid to 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 (Artificial Intelligence Act) (the "**AI Act**"). While the AI Act focuses mostly on the challenges posed by generative AI, some of its provisions seem to be repetitive and, thus, enhance the most problematic provisions of the DSA. Rather unsurprisingly, potentially the most problematic part concerns an AI provider's obligation to mitigate "systemic risks" generated by their models (Article 55 *et seq.*). According to Article 3(65), "systemic risk" means "a risk that is specific to the high-impact capabilities of general-purpose AI models, **having a significant impact on the Union** market due to their reach, or due to **actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole**, that can be propagated at scale across the value chain." While the AI Act itself provides little guidance on what may be defined as systemic risks, the AI Act Code of Practice is slightly more precise, by listing, among others, risks to "**freedom of expression and information"** and from **"violent, hateful, radicalising, or false content"** (p. 34). While one could defend the discussed provisions as addressing real needs (sharing the responsibility for controlling the development and application of AI), in light of the analysis conducted above one could reasonably expect that these provisions would serve as an opening for limiting access to content diverging from the mainstream opinions, e.g., by excluding conservative opinions from AI learning materials as constituting toxic data, etc.

The threat to freedom of speech on the internet may also come from different sources. To give an example, Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence also contains provisions limiting the freedom of speech online. Its Article 8.1 criminalizes "**inciting** violence or **hatred** directed against **a group of persons or a member of such a group**, defined by reference to **gender**, by publicly disseminating, by means of ICT [Information and Communication Technology], material containing such incitement" (as this case concerns a directive, Member States are given certain leeway to limit the criminalization of such behavior). Article 23 of this Directive obliges the Member States to create robust frameworks for the removal of incriminating material from the internet. Already, vaguely hateful content concerning a group defined by gender should be understood in the light of the aim and purpose of the directive. As stipulated in para. 75 of the Preamble, "Member States should take measures to **prevent the cultivation of harmful gender stereotypes** in order to **eradicate the idea of** the inferiority of women **or stereotyped roles of women and men.** (…) Considering that, from a very young age, **children are exposed to gender roles** that shape their self-perception and influence their academic and professional choices **as well as expectations of their roles** as women and men

throughout their life, **it is crucial to address gender stereotypes as of early-childhood** education and care."

Thus, it is obvious that the risks to free speech stemming directly from the EU legal acts forming the Democracy Shield are further amplified by the regulatory environment, which aims to suppress the debate on controversial topics. This pertains, in particular, to open-ended terms such as "hate speech" or the notion of "illegality."

II. EU Democracy Sword: enforcement of the European Democracy Shield

1. Introduction

In order to properly assess the actual effects of the EU Democracy Shield on freedom of speech, one cannot omit the issue of incentives generated by the enforcement framework foreseen in these acts. As will be explained in detail below, this cannot be overstated. The possibility of harsh sanctions against both internet service providers and the Member States strongly encourages them to act in the interest of limiting freedom of speech and freedom of information on the internet.

2. Sanctions for the online service providers failing to comply with the EU Regulations

Rather unsurprisingly, the above-discussed EU regulations are strengthened by their strong enforcement mechanisms. According to the DSA, the competent authorities (i.e., digital market regulators) should have the investigative, as well as the monitoring and punitive powers (see in particular Articles 49-55 of the DSA). The system relies, first of all, on requesting online service providers to end infringements and ensure compliance with the DSA. In practice, this would mean that the targeted providers would have to adapt their business lines to the regulator's requests, submit action plans, etc. While the detailed procedures and specific penalties are to be stipulated in the Member States' national regulations, the DSA sets certain minimum requirements. In particular, the maximum penalties for failing to remediate a violation of the Regulation should equal "**6% of the annual worldwide turnover** of the provider of intermediary services concerned in the preceding financial year," while the maximum penalty for supplying "incorrect, incomplete or **misleading information**, failure to reply or rectify incorrect, incomplete or misleading information and failure to submit to an inspection shall be **1% of the annual income or worldwide turnover**" (Article 52.3 of the DSA). In addition, there should also be a possibility for individuals to seek damages (private enforcement), as stipulated in Article 54 of the DSA. The same 6% of the total worldwide annual turnover is foreseen for the penalties imposed by the European Commission (Article 74.1 of the DSA).

The catalogue of penalties foreseen in the Political Advertising Regulation is similarly harsh and, in particular, foresees "6% of the annual income or budget of the sponsor or of the provider of political advertising services as applicable and whichever is the highest" or "6 % of the annual worldwide turnover of the sponsor or the provider of political advertising services in the preceding financial year" (Article 25.2 of the Political Advertising Regulation).

3. Implementation: between state and international bureaucracies

As often happens in respect of EU law acts, even if they are directly applicable, as is the case with regulations, their enforcement not only requires the involvement of national authorities of the Member States, but also is at least partially governed by national laws.

In case of the DSA, its provisions should be enforced, in principle, by the Member States' organs (Article 49ff of the DSA), who should be ensured adequate resources to monitor their tasks. The DSA calls them Digital Service Coordinators. In practice, this role is ascribed to digital market regulators (Article 49.1). They have investigative and enforcement powers, which, however, are stipulated in detail only in the national regulations. In the case of very large online platforms and search engines, such as YouTube, Google and Facebook, it is the Commission that is in charge of conducting the investigation and imposing penalties.

The enforcement mechanisms for the Political Advertising Regulation are, by and large, similar (Article 22 expressly refers to the corresponding provisions of the DSA).

4. Structural challenges posed by the mechanisms

Thus, it is clear to see that the European Democracy Shield strengthens the position of leftist-liberal politicians and political groups. The financial penalties for violating the Democracy Shield are substantial, and the fact that they can be imposed for breaches of EU regulations rather than specific transgressions of national law makes them even more burdensome for online operators. Furthermore, the institutional framework of the EU's systems should be taken into account since it is there that input from the Commission's list of Member-State-approved NGOs may become the most relevant. After all, it is clear that, given the breadth and scope of the online platforms' obligations towards the "trusted flaggers" or "fact-checkers" (cooperation, support, reporting duties), the lack of cooperation with them may constitute a breach that would later be penalized by the Commission or the national Digital Service Coordinators. This poses a genuine threat to our liberty by incentivizing the curtailment of free speech while granting a prominent role to unaccountable NGOs that are exempt from democratic scrutiny.

One could very well imagine a situation where an online platform would adopt a stance more conducive to the protection of freedom of speech than the fact-checking NGOs, e.g., by refusing to remove content critical of abortion or decarbonization, only to be reported by these entities to the national authorities and the Commission. The responsible authority would subsequently start checking the compliance of the online service providers with the EU regulations. Throughout the investigation, the authority would mostly rely on the information prepared by the very same NGOs, whether in the form of periodic reports, general standards and guidelines,

or statistical assessments. Hence, the information-controlling NGOs would have a substantive impact on the outcome of the proceedings initiated against online operators, thus creating far-reaching incentives for restricting freedom of speech for ideological reasons.

5. Conditionality as the new convention? Forcing the Member States to promote censorship

Given the composite nature of EU law enforcement, one could legitimately ask whether and to what extent the chilling effect on the freedom of speech and democratic debate could somehow be mitigated at the level of the Member States. The answer to this question, however, would be somewhat ambiguous. On the one hand, the EU has indeed left the national legislators a margin of discretion with regard to both setting the regulatory framework and the organization of the national enforcement bodies. In some cases, such as in Poland, freedom of speech has been successfully protected by the outcome of the national legislative process (the president vetoed the bill put forward by the ruling liberal party that aimed to introduce even stricter regulations).[10] On the other hand, this margin of discretion is not universally applicable (the European Commission has the jurisdiction to launch investigations against very large online platforms and search engines, such as Google, Facebook or X) and is subject to the scrutiny of the EU itself.

When implementing EU law, Member States have to do so in a manner consistent with EU law as interpreted by the relevant EU bodies and, ultimately, the Court of Justice of the European Union, which typically sides with the Commission. Consequently, it is easy to imagine Member States being prosecuted by the Commission for failing to demonstrate sufficient involvement in online-speech censorship activities. Again, the Commission-backed NGOs would be best placed to formulate accusations against the noncompliant Member States and provide legitimacy for the Commission's actions. As to the punitive measures at the Commission's disposal, there are two main possibilities. Firstly, the Commission could commence infringement proceedings and impose a financial penalty under Articles 258 and 260 of the consolidated version of the Treaty on the Functioning of the European Union (OJ C 326, 26.10.2012, pp. 47–390). Secondly, it could use the extra-treaty conditionality mechanism foreseen in Regulation (EU, Euratom) 2020/2092 of the European Parliament and of the Council of 16 December 2020 on a general regime of conditionality for the protection of the Union budget (the "**Conditionality Regulation**").

The first option, having a strong basis in the treaties, would be more structured and would take more time since the Commission would have to conduct an investigation and then prepare a

[10] *Bill Implementing EU's Digital Services Act Vetoed by Polish President, Citing Arguments Put Forward by Ordo Iuris*, Ordo Iuris, 16 January 2026, https://ordoiuris.pl/en/press-newsdesk/bill-implementing-eus-digital-services-act-vetoed-by-polish-president-citing-arguments-put-forward-by-ordo-iuris, accessed: 5 March 2026.

reasoned opinion demanding that the given Member State remove any incompatibilities with EU law. If the Member State refused, the Commission could bring the case to the Court of Justice of the European Union (CJEU) and demand a declaration of a breach. If the court found the claim justified, the Member State would be obliged to secure compliance with the EU law. Only after failing to do so could the Commission demand payment of a financial penalty. This scenario has undergone some changes recently, however, with the CJEU being increasingly willing to apply financial penalties as a temporary measure, even prior to finding a breach of EU law.

Even taking these recent developments into account, however, the Treaty mechanisms would still grant the Commission far less leverage than the Conditionality Regulation. To make a long story short, the Conditionality Regulation allows the Commission to limit the payment of EU funds to a Member State showing deficiencies in its ability to manage them. These deficiencies are understood widely, and the Regulation expressly also recognizes so-called rule of law issues as a valid ground for freezing funds.[11] The procedure is discretionary and involves the Commission and, to a limited degree, also the Council. Importantly, the Regulation is applicable to all sorts of EU funds. Given the track record of the Commission, one could reasonably conceive a scenario where a Member State's reluctance to limit freedom of speech for the sake of eliminating fake news, disinformation, and the like would lead to the Commission freezing EU funds for that Member State. And this threat is by no means purely theoretical. The Commission has, for example, instrumentalized the EU budget rules to forestall payments to Poland (only to resume them immediately after the victory of the liberal party). In addition, the payment of funds for Hungary was frozen on the basis of the European Commission's decision,[12] and threats of weaponizing the conditionality regulation were raised against Slovakia with regard to its recent constitutional changes recognizing, among others, the reality of two biological sexes and the value of the family.[13]

It is also important to remember the role of the national courts in interpreting and enforcing EU laws. Under EU law, national courts are obliged to apply EU law directly. According to the CJEU's interpretation, EU law takes precedence even over national constitutions—this being one of the fundamental lines of conflict between centralist and sovereignist forces in the EU. In addition, each national court is empowered to raise a preliminary legal question to the Court of Justice of the European Union concerning the interpretation and application of EU law. This

---

[11] *The EU's Rule of Law Conditionality Mechanism: A Case for Suppression, Not Reform*, Ordo Iuris, 17 February 2026, https://ordoiuris.pl/en/analyses/the-eus-rule-of-law-conditionality-mechanism-a-case-for-suppression-not-reform/, accessed: 1 March 2026.

[12] *Rule of law conditionality mechanism: Council decides to suspend €6.3 billion given only partial remedial action by Hungary*, European Council, Council of the European Union, 12 December 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/12/12/rule-of-law-conditionality-mechanism/, accessed: 1 March 2026. The Commission eventually made a deal with the Hungarian government, which was later scrutinized by the CJEU.

[13] *Statement regarding the legislative amendments proposed by the Slovak government on whistle-blower protection*, European Public Prosecutor's Office (EPPO), 28 November 2025, https://www.eppo.europa.eu/en/media/news/statement-regarding-legislative-amendments-proposed-slovak-government-whistle-blower, accessed: 1 March 2026.

means that, even if Member States take legislative or organizational measures in order to protect freedom of speech, these could still be effectively undermined by strategic litigation and activist judges willing to disregard their national laws.