INNOVADE

Innovative Democracy Through Digitalisation

# European Democracy Shield

## Open Public Consultation Policy Recommendations by the Horizon Europe project **INNOVADE**

innovade-democracy.eu

Funded by the European Union

# Table of contents

# 1. Introduction

This policy brief is prepared as a response to the public consultation opened by the European Commission for further development and fine-tuning of the European Democracy Shield initiative. This brief is prepared by INNOVADE project consortium which is funded by the EU under its Horizon Europe programme.

INNOVADE project aims to advance our digital democracy by improving knowledge on the current state of the art, future trends, and emerging next practices; providing tools, frameworks, structures for inclusive digital governance; building a digital democracy application; and developing a conceptual framework, platform and the educational materials needed for democratising access to digital tools for citizens.

Although INNOVADE project is still in its initial research phase, we take this opportunity to share our recommendations based on our preliminary results. Our recommendations are based on the four critical domains of European Democracy Shield's strategic framework, followed by our reflections on the EU's transitioning towards its Digital Autonomy.

# 2. Countering Foreign Information Manipulation and Interference and Disinformation

In the contemporary digital landscape, **disinformation and foreign information manipulation** represent increasingly potent threats to democratic integrity across the European Union. With the widespread proliferation of social media platforms and advanced algorithmic systems, **hostile actors**—whether state-sponsored or domestic—can now easily orchestrate sophisticated campaigns designed **to mislead the public, undermine trust in democratic institutions, and distort public discourse.** These campaigns frequently exploit the vulnerabilities inherent in digital platforms, such as algorithmic amplification and the rapid, unchecked dissemination of false narratives, often leveraging **artificial intelligence tools and deepfake technologies to blur the lines between reality and fabrication.**

The consequences of unchecked disinformation extend far beyond immediate political disruptions; **they erode societal trust, deepen polarization, and weaken the resilience of democratic societies** against internal and external threats. Thus, effectively countering these sophisticated operations requires proactive and coordinated **actions at both technological and regulatory levels.** Strategic interventions must balance freedom of expression with robust protections against manipulation and deception.

The future of foreign information manipulation and interference (FIMI) and disinformation will largely be driven by future developments in technology. Noticeably, the role of large language models (LLMs) and other forms of artificial intelligence (AI) has continued to grow over the past few years. Some of the tactics that have been enabled by advancements in AI are fake online personas, automated botnets and copy-paste campaigns, and localized targeting through demographic specific narratives. **The speed in the transition from organic social media traction for disinformation to disinformation as a service to AI-augmented disinformation is worrying for the future.**

LLM grooming has become a serious concern as the output of content disseminated by disinformation campaigns has significantly increased due to lower barriers with the assistance of AI. When there are several campaigns active and connected within a network, the content they disseminate can inform or 'groom' AI chatbots into becoming biased and disinformed. Their responses will then be rooted in this disinformation, creating a harmful cycle of intentional/unintentional information laundering. Deepfakes are likely to be used in a more sophisticated way maliciously by foreign actors to manipulate information leading up to elections, increase geopolitical tensions, destabilize actors in situations of armed conflict.

## Recommendations:

- **Develop and implement advanced AI-based detection and intervention tools** capable of rapidly identifying, flagging, and mitigating disinformation across multiple digital platforms.
- **Mandate and enforce comprehensive transparency standards** for online political advertising, algorithm-driven content dissemination, and personalized information delivery, ensuring clear visibility into the origins, sponsors, and objectives of digitally delivered political messages.
- **Establish and support robust pan-European networks for fact-checking and verification**, enhancing cross-border information sharing, cooperation, and coordination among governmental institutions, independent researchers, civil society organizations, and media outlets.
- **Introduce and rigorously enforce clear sanctions and accountability frameworks** targeting entities proven to orchestrate or facilitate disinformation and foreign information manipulation campaigns, thereby creating a powerful deterrent against malicious activities aimed at destabilizing democratic societies.
- **Support the development of European big social media platforms.**

Together, these measures form a comprehensive, multi-layered defense capable of preserving democratic discourse and safeguarding citizens against the harms of information warfare.

# 3. Fairness and Integrity of Elections and the Strengthening of Democratic Frameworks

The advent of digital technologies has **transformed democratic processes**, bringing significant advancements in **transparency and civic engagement**. However, these benefits are accompanied by new and complex challenges that threaten the fairness, integrity, and transparency of electoral systems within the European Union. Cybersecurity vulnerabilities increasingly **expose election infrastructure to targeted cyber-attacks**, risking the manipulation of electoral outcomes. At the same time, widespread misinformation, amplified by digital media and algorithm-driven content curation, **distorts voter perceptions and polarizes societies**. Furthermore, the rapid adoption of artificial intelligence tools in political campaigning presents unprecedented ethical dilemmas, including the potential for **targeted voter manipulation, micro-targeted disinformation, and opaque political financing**.

As **electoral integrity** stands as the cornerstone of democratic legitimacy, addressing these threats is paramount. The European Democracy Shield advocates for a strategic and integrated approach that blends innovative technological solutions with clear regulatory frameworks. **Strengthening cybersecurity, increasing transparency, and setting ethical standards for digital political engagement** are essential measures to uphold voter confidence and ensure robust democratic processes.

## Recommendations:

- **Integrate blockchain-based technologies into electoral systems** to provide immutable, transparent records of votes in compliance with the GDPR (no personal or confidential data should be stored on blockchain), thereby significantly reducing the risks of electoral fraud and enhancing public trust in election outcomes.
- **Establish comprehensive regulatory frameworks and ethical guidelines** governing the deployment of artificial intelligence in election campaigns, clearly defining permissible uses and addressing issues of transparency, accountability, and fairness in AI-driven political activities.
- **Enhance cybersecurity measures and infrastructure resilience specifically tailored for electoral contexts**, ensuring protection against cyber threats such as hacking attempts, data breaches, and interference with voter registration systems and election result dissemination.
- **Standardize and enforce EU-wide transparency and accountability standards for digital campaign finance**,

demanding clear disclosure of funding sources, expenditures, and sponsorship of digital political content to curb hidden influences and uphold electoral fairness.

- **Implement specific media information literacy campaigns before elections** with an aim to immunise citizens against mis/disinformation.

Collectively, these initiatives form a comprehensive response to ensure electoral systems remain robust, fair, and transparent, safeguarding the integrity of democratic governance in the digital era.

# 4. Strengthening Societal Resilience and Preparedness

The integration of digital technologies into democratic processes not only enhances civic engagement but also **exposes societies to complex new threats**, such as **targeted cyberattacks, pervasive misinformation, and intensified societal polarization**. Digital platforms, while connecting individuals across borders, can also amplify divisive content, creating echo chambers and fueling polarization that undermines social cohesion and weakens democratic institutions. Moreover, **cyber threats targeting critical infrastructure and public services** pose substantial risks to democratic stability, potentially disrupting government functions, electoral processes, and essential communication channels.

To effectively respond to these interconnected threats**, building societal resilience and preparedness is crucial**. This involves equipping citizens with the necessary skills to navigate the digital environment critically and responsibly. **Education and awareness programs**, designed with an inclusive and comprehensive approach, can significantly enhance citizens' abilities to identify, resist, and mitigate misinformation and cyber threats. In addition, fostering robust **collaboration among government bodies, academia, civil society, and the private sector** can create dynamic, adaptive strategies to respond swiftly and effectively to emerging digital threats.

## Recommendations:

- **Implement extensive EU-wide (but local specific) digital and media literacy initiatives** covering diverse demographics, equipping citizens of all ages with the skills necessary to critically evaluate digital information and understand potential digital threats.
- **Integrate comprehensive critical thinking and media literacy education into national curricula** across member states, ensuring that future generations are resilient and well-prepared for an evolving digital landscape. Begin as early as possible to educate young people; and collaborate with civil society organizations to integrate them into the educational activities where different competencies and educational material are needed then the school capacity.
- **Strengthen cross-sectoral partnerships among governments, educational institutions, civil society, and the technology sector** to proactively tackle misinformation and digital polarization, leveraging expertise, resources, and best practices from all relevant stakeholders.
- **Establish effective rapid-response frameworks** capable of quickly identifying, addressing, and mitigating cyber incidents and coordinated misinformation campaigns that threaten democratic processes, maintaining public trust and democratic continuity in crisis situations.

By fostering informed, digitally literate societies and enhancing collaborative preparedness, these measures will build resilient democracies capable of navigating and thriving amidst the challenges posed by digital transformation.

# 5. Citizens' Participation and Engagement

In an era characterized by rapid digital transformation, empowering citizens to **meaningful civic engagement** is essential to maintaining vibrant and resilient democracies. Digital technologies offer unprecedented opportunities for citizens to **influence policymaking, express their voices, and engage with democratic processes** more directly and transparently. However, these promising developments are hindered by persistent **inequalities, digital divides, and insufficient protection of individual privacy**. Unequal access to digital infrastructure, disparities in digital literacy, and concerns about the misuse of personal data collectively create significant barriers to inclusive and meaningful participation, risking the marginalization of disadvantaged and vulnerable groups.

To harness the full potential of digital participation, it is imperative that European democracies actively address these barriers. This requires **substantial investments in infrastructure** and schooling to bridge the digital divide and ensure equitable access to essential democratic tools. Concurrently, developing secure and privacy-respecting digital platforms can bolster citizens' trust, encouraging broader and more meaningful participation. Establishing a reliable, transparent, and user-friendly digital identity system will further streamline citizen interactions with governance platforms, fostering a more accessible and responsive democratic ecosystem.

## Recommendations:

- **Significantly increase investment in digital infrastructure**, especially in underserved and rural areas, to guarantee equal access to democratic participation tools and prevent exclusion from digital democratic processes.
- **Develop and promote secure, privacy-focused digital engagement platforms (digital democracy applications)**, ensuring robust data protection and transparent data handling practices that reassure citizens and facilitate confident participation.
- **Implement standardized, EU-wide digital identity solutions**, simplifying secure citizen-government interactions and enhancing accessibility and ease of participation across various platforms and public services.
- **Create continuous, responsive feedback mechanisms and citizen consultation processes**, allowing for ongoing, structured input into policymaking and governance, thus strengthening the responsiveness and accountability of democratic institutions. Develop and spread inclusive digital democracy applications as a way of realising this with a diverse group of citizens.
- **Fund projects targeting especially vulnerable groups** who are not willing to participate through innovative mechanisms taking a multistakeholder approach (collaboration with cultural organisations, youth organisations, senior organisations, etc.)
- **Deploy User-Centered Design (UCD) principles to create accessible civic gov tools** that keep from exacerbating societal inequalities. Moreover, take into account User Experiences (UX) to optimize citizens' experience and motivate them to higher and more profound levels of engagement. For creating an equal level playing field in terms of access, in itself, does not yet guarantee actual participation.

By addressing infrastructure disparities, prioritizing digital security and privacy, and enabling continuous citizen engagement, these proposals lay the foundation for more inclusive, participatory, and resilient democracies across the European Union.

# 6. From Digital Imitation and Digital Regulation towards Digital Autonomy

The European Democracy Shield (EDS) is an initiative that wants to strengthen the resilience of European democracy against undemocratic attacks. Contexts include the increase of international political polarization, conflicts, and wars, including hybrid warfare with attacks on critical infrastructures. The basic idea of resilience is that a system continues to exist and work after attacks, disruptions, and crises. The Internet is a critical infrastructure that enables human information, communication, and co-operation. One aspect that arises in the context of the EDS is how to make the European Union's Internet infrastructure resilient. In this context, the question needs to be posed of what policies for regulating the digital world the European Union requires.

We suggest that the European Union needs to transition towards a third phase of digital policies, namely after digital imitation and digital regulation towards digital autonomy. The European Democracy Shield requires an **autonomous EU Internet infrastructure that is independent from the USA and China** whose digital giants dominate the Internet today.

The European Union's digital policy making has in respect to the Internet thus far followed **two phases: imitation (1990s, 2000s) and regulation (since 2010**). The first phase of digital imitation involved information society policy strategies such as eEurope: An Information Society for All and i2010: A European Information Society for Growth and Employment. Crucial in this phase was the European Union's goal formulated in the Lisbon strategy "to become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion" (Lisbon European Council 2000) by 2010. In 2010, this goal was not reached, the European Union did not catch up with and overtake the US Internet economy where the digital giants such as Amazon, Google, Facebook, Microsoft, Apple, eBay, Yahoo, Adobe, PayPal, etc. are located. The European Union did not succeed in its self-set goal of imitating Silicon Valley and establishing the likes of Google and Facebook in the EU. Today, the world's ten largest Internet companies ranked by revenue are all located in the USA and China: Amazon, Alphabet, JD, Meta, Alibaba, Tencent, ByteDance, Netflix, Meituan, and Paypal (Wikipedia 2025) Since 2010, the European Union has entered a **new, second stage in digital policy making: the stage of digital regulation**. In this phase of digital policy making, the EU has primarily focused on developing EU-wide policies that regulate Internet platforms in the EU. Such initiatives have resulted in a number of key EU Internet policies: **Regulation on Open Internet Access** (2015), **General Data Protection Regulation** (GDPR) (2016), **Regulation on Digital Service Portability** (2017), **Regulation on Geo-blocking** (2018), **Digital Markets Act (DMA)** (2022), **Artificial Intelligence Act** (2024), **Digital Services Act** (DSA) (2024).

The Internet is an international and global information and communication network. Therefore, its regulation needs to be international, too. However, there is not one institution able to globally regulate the Internet. In the times we live in, there is the rise of new authoritarian and nationalist forms of politics that question international agreements and regulation, which makes regulating the Internet ever more difficult.

The **EU faces the danger that in the future, the digital giants will, backed by the governments of the US and China, simply ignore EU legislation and exclude EU users from accessing these platforms**. The consequence would be that **Internet use in the EU** would severely decline as it **depends on US and Chinese platforms.** In addition to the questioning of EU Internet policies, the EU's Internet also faces a high level of **misinformation and foreign interferences** in politics and election campaigns in the form of fake news, hacking, hybrid warfare, deep fakes, post-truth, online hatred, and algorithmic politics. Between November 2023 and November 2024, European External Action Service (2025) observed and analyzed 505 foreign information manipulation and interference (FIMI), incidents that consisted of 68,000 pieces of information targeting 90 countries and 332 organizations by using a total of 25 media platforms. The operations were global but the absolute majority, namely 50.9% (257 in total) of the incidents were focused on Ukraine. The targets were especially organizations (international organisations such as the EU, news media, networks of journalists such as Bellingcat, and fact checking organizations such as Correctiv). Most operations use multiple media platforms. X and Facebook were the most frequently used platforms.

Given the EU's critical Internet infrastructure is dependent on the US and Chinese global digital giants and faces attacks, it is not resilient. Therefore, we see the need for the EU to enter a new stage of Internet policy making, the phase of Internet and digital autonomy. Internet and digital autonomy means the advancement of policies that create and strengthen an autonomous EU Internet infrastructure, including major Internet platforms, that operates from within the EU, adheres to democratic European principles and EU regulation. Autonomy is the best strategy to make the EU's Internet resilient and defend digital democracy in the EU.

**Public service media (PSM) are one of Europe's media strengths** in the public sphere. PSM originated in Europe in 1922 when the BBC was founded. In contrast to the USA and China, PSM play a key role in the European media landscape. Measured in terms of revenue, ARD (Germany) is the largest media company headquartered in Europe, BBC (UK) the third largest, France Télévisions (France) the seventh largest, RAI (Italy) the eleventh largest, ZDF (Germany) the twelfth largest and SRG-SSR (Switzerland) the eighteenth largest (data source: Council of Europe 2024). PSM are key democratic players in the European media landscape: As democratic communication is part of public service media's remit, they are committed to democracy and the democratic public sphere. Today, there are dozens of public service media operators in Europe and the world (see https://en.wikipedia.org/wiki/European_Broadcasting_Union). **PSM are already important actors on the Internet**. They operate Internet-based media players. These players have thus far been operated at a national scale independent from each other.

## Recommendations:

- Foster policies that **support and advance the EU's digital autonomy** from the US and Chinese digital giants.
- **Create an EU Internet and EU Internet platforms** that are operated autonomously from the US and Chinese digital giants is the best way to advance Internet resilience in the EU and a European Democracy Shield.
- Create an autonomous, resilient, and democratic EU Internet infrastructure and EU Internet platforms, the EU should not copy the US market-led Silicon Valley model and the Chinese state-controlled Internet model but rather **build on its own media strengths**.
- **Support and advance the networking of European public service media and their digital technologies/ platforms in order to bring about what some have termed a public service Internet** (see Fuchs and Unterberger 2021, PSMI Manifesto Collective 2021).
- **Increase the funding of the R&D invested in the fields of digital democracy, digital public sphere, and public service Internet** in order to advance Internet resilience, Internet autonomy, and the digital public sphere.
- **Bring together and support initiatives** of advancing a public Internet that fosters digital democracy and the digital public sphere **and actively integrate them into policy making, research, and development as important stakeholders** (for example, initiatives such as Manifesto for Public Service Media and a Public Service Internet (https://bit.ly/psmmanifesto), Council for European Public Space (https://europeanpublicspace.eu/), Public Spaces Incubator (https://newpublic.org/psi), and EuroStack (https://euro-stack.eu/).

Strengthening the resilience of European digital democracy in the light of authoritarianism, hybrid warfare, polarisation, misinformation, post-truth, and fake news culture requires, first and foremost, the vision of a democratic Internet and the practical realisation of this vision. The Public Service Media and Public Service Internet Manifesto, an initiative co-initiated by one of INNOVADE's research team leaders, formulates foundations of such a vision in the following way:

> *"We envision the creation of a Public Service Internet: an Internet of the public, by the public, and for the public; an Internet that advances instead of threatens democracy and the public sphere, and an Internet that provides a new and dynamic shared space for connection, exchange and collaboration. The Public Service Internet is based on Internet platforms operated by a variety of Public Service Media, taking the public service remit into the digital age in co-operation with civil society, individual media users, citizens, and the creative, cultural and educational sector. The Public Service Internet advances democracy. It enhances the public sphere. It supports active citizenship by providing comprehensive information and analysis, diversity of social representation and creative expression, and extended opportunities for participation. Public Service Internet platforms can support new and young creatives who will build the*

> *cultural industries of tomorrow and foster social cohesion. Now is the time for a Public Service Internet and revitalised Public Service Media. […] A democracy-enhancing Internet requires Public Service Media becoming Public Service Internet platforms that help to advance opportunities and equality in society. We call for the creation of the legal, economic and organisational foundations of such platforms. […] Public Service Internet platforms realise fairness, democracy, participation, civic dialogue and engagement on the Internet. […] The Public Service Internet requires new formats, new content, and vivid cooperation with the creative sectors of our societies. […] The Public Service Internet provides opportunities for public debate, participation, and the advancement of social cohesion. […] The Public Service Internet is a driver of change in the creation of new content and services while creating a sustainable ecosystem for media innovations. […] Public Service Media and the Public Service Internet contribute to a democratic, sustainable, fair, just, and resilient society" (PSMI Manifesto Collective 2021).*

# 7. Conclusion

The future of democracy in Europe hinges on our **collective ability to adapt and respond to the dynamic challenges and opportunities** presented by the digital age. The European Democracy Shield is not merely a defensive measure—it is **a forward-looking strategic framework** aimed at transforming the way democracy functions in the 21st century. At its heart lies the commitment to uphold the European Union's core values—**democracy, the rule of law, and fundamental rights—**by reimagining democratic engagement for a digitally interconnected society.

This framework recognizes that digital technologies, while offering tools for greater transparency, participation, and efficiency, also introduce vulnerabilities that can undermine public trust, electoral integrity, and social cohesion. As such, a comprehensive and coordinated response is essential. The proposals outlined across the four strategic pillars**—countering disinformation, ensuring electoral integrity, strengthening societal resilience, and fostering citizen participation—**offer a practical roadmap for building a more inclusive, secure, and responsive democratic infrastructure.

**Crucially, the European Democracy Shield must go beyond defence and regulation towards establishing digital autonomy**. Europe's digital landscape remains heavily dependent on platforms and infrastructure controlled by actors outside the EU, particularly in the United States and China. This dependency creates significant vulnerabilities, including exposure to hybrid threats, the circumvention of EU digital sovereignty, and diminished capacity to enforce regulatory standards. A strategic shift is therefore required—from the earlier phases of digital imitation and regulation to a new paradigm of **digital autonomy**.

To reinforce this transition, the EU must invest in the development of an **autonomous, resilient, and democratic Internet infrastructure**—one that is built on the foundational principles of European public service, democratic participation, and technological self-determination. Public service media (PSM), with their longstanding commitment to the democratic public sphere, should be scaled and networked into a **Public Service Internet** that serves citizens equitably and responsibly. This vision entails new funding priorities, legal frameworks, and collaborative platforms that empower civil society, cultural and educational sectors, and public broadcasters to co-create digital spaces rooted in transparency, equity, and civic responsibility.

Success will require **sustained investment, cross-sector collaboration, a firm commitment to democratic innovation, as well as a policy focus on strengthening the EU's digital autonomy.** Governments, civil society, academia, and the private sector must work together to ensure that technological advancements empower citizens rather than alienate them, protect rights rather than infringe upon them, and build trust rather than erode it.

By embracing both **democratic resilience and digital autonomy**, the European Democracy Shield can serve as a global model for protecting and advancing democratic governance in the digital era—solidifying the EU's leadership role in fostering inclusive, sovereign, and resilient democratic societies

# References

American Sunlight Project, LLM Grooming: A New Strategy to Weaponize AI for FIMI Purposes

Council of Europe. 2024. Top Players in the European AV Industry (2023 Data Tables). https://rm.coe.int/top-players-in-the-european-av-industry-2023-figures/1680b54718 (accessed on 21 May 2025)

European Commission, European Democracy Shield

European External Action Service. 2025. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the Architecture of FIMI Operations. Brussels: EEAS.

EU-HYBNET, State of Deception: Inside Russia and China's Information Playbook

Fuchs, Christian and Klaus Unterberger, eds. 2021. The Public Service Media and Public Service Internet Manifesto. London: University of Westminster Press.
Open access book: http://doi.org/10.16997/book60

INNOVADE Project, Knowledge Base on Digital Democracy (ongoing), https://innovade-democracy.eu/

IMMUNE 2 INFODEMIC Project, https://immune2infodemic.eu/

Lisbon European Council. 2000. Lisbon European Council 23 and 24 March 2000: Presidency Conclusions, https://www.europarl.europa.eu/summits/lis1_en.htm (accessed on 20 May 2025)

PSMI Manifesto Collective 2021. The Public Service Media and Public Service Internet Manifesto. In The Public Service Media and Public Service Internet Manifesto, edited by Christian Fuchs and Klaus Unterberger, 7-17. London: University of Westminster Press. DOI: https://doi.org/10.16997/book60.b. Latest version: https://bit.ly/psmmanifesto

Wikipedia. 2025. List of Largest Internet Companies. https://en.wikipedia.org/wiki/List_of_largest_Internet_companies#cite_note-145

INNOVADE

Innovative Democracy Through Digitalisation

Funded by
the European Union