
CENTRE *for*
JUSTICE *and*
LAW REFORM

AT THE LAW SOCIETY OF IRELAND

Safeguarding Irish Election
Integrity in the Era of
Emerging Digital Threats



Law Society
of Ireland

Advisory Board to the Centre

External Members



Noeline Blackwell, Online Safety Coordinator at the Children's Rights Alliance, Commission Member of the Irish Human Rights and Equality Commission, Adjunct Professor at the University College Dublin School of Law



Raymond Byrne, Barrister-at-Law, former full-time Commissioner and former Director of Research at the Law Reform Commission, Adjunct Full Professor, Sutherland School of Law, University College Dublin



Professor Deirdre Curtin, Professor of European Law and Former Dean of Graduate Studies at the European University Institute, former Director of the Centre for Judicial Cooperation at the Robert Schuman Centre



Caoilfhionn Gallagher KC, International human rights lawyer and Commissioner of the Irish Human Rights and Equality Commission



Sinéad McSweeney, Board Member of An Garda Síochána, former Vice President Global of Public Policy and Philanthropy at Twitter



Professor Niamh Moloney, Professor of Law at the London School of Economics



Professor Colin Scott, Registrar, Deputy President, and Vice President for Academic Affairs at University College Dublin

Law Society of Ireland Ex Officio Members



Rosemarie Loftus, President



Martin Lawlor, Senior Vice-President



Mark Garrett, Director General

Centre Staff

Director of Policy

Dr Brian Hunt, MLitt, PhD (Dubl), Solicitor

Head of Research

Suzanne Scott, LLB (Ling Germ) (Dubl), LLM (NUI), Barrister-at-Law

Associate Researchers

Dr Julia Volkmar, BA (RUG), LLM, PhD (QUB)

Dr Liam Edwards, LLB (Hons), PgDip, PhD (Ulster)

Lee Daly, BA (DCU) MLitt (St And)

Executive Summary

Free and fair elections are a cornerstone of Ireland's democratic system. However, the rapid evolution of digital technologies has created new opportunities for malicious actors to influence public debate, undermine trust in democratic institutions, and interfere with electoral processes. The increasing prevalence of social media, algorithmic amplification, anonymous online activity, and generative artificial intelligence (GenAI) has fundamentally altered the information environment in which elections take place.

This Discussion Paper examines the growing challenge of online election interference in Ireland, with particular focus on misinformation, disinformation, foreign information manipulation and interference (FIMI), and the emerging risks associated with AI-generated content.

While election interference is not a new phenomenon, digital technologies have enabled false information to be created, distributed, and amplified at an unprecedented scale and speed.¹ These developments have the potential to distort public discourse, damage confidence in electoral outcomes, and undermine democratic legitimacy.²

Misinformation and disinformation are increasingly prominent features of the online information environment. Although research that such activities directly determine election outcomes remains limited, there is growing evidence that it contributes to political polarisation, undermines trust in public institutions and media, and erodes confidence in democratic processes. Recent elections across the European Union (including in Ireland) have demonstrated the capacity of both domestic and foreign actors to exploit digital platforms to spread false narratives, attack political candidates, and challenge the legitimacy of electoral outcomes.

The Paper pays particular attention to the impact of GenAI. Advances in GenAI have made it easier to create convincing but entirely fabricated images, videos, and audio recordings that can be used to mislead voters or discredit candidates. The proliferation of AI-generated content presents new challenges for regulators, online platforms, and the public, particularly during election periods when voters rely upon timely and accurate information to make informed electoral choices.

The Paper also examines the effects of online harms on electoral candidates. Research indicates that a large number of candidates in Ireland are concerned about online harassment and disinformation targeting them personally.³ Such behaviour can deter individuals from participating in public life, disproportionately affecting women and minority candidates, and ultimately weakening representative democracy.

1 Office of the United Nations High Commissioner for Human Rights, 'Elections at Risk in the Digital Age' (OHCHR, 4 July 2025) <<https://www.ohchr.org/en/stories/2025/07/elections-risk-digital-age>> accessed 22 July 2026.

2 *ibid.*

3 Eugenia Siapera and others, *Report on the Abuse and Harassment of Members of the Houses of the Oireachtas and Political Staff*, (UCD Centre for Digital Policy 2024) 4.

A detailed analysis of Ireland's legal and regulatory framework demonstrates that significant progress has been made in recent years. Key reforms include the establishment of An Coimisiún Toghcháin under the Electoral Reform Act 2022, the establishment of Coimisiún na Meán under the Online Safety and Media Regulation Act 2022, the implementation of the EU Digital Services Act (DSA), and the establishment of Oifig IS na hÉireann (the AI Office of Ireland) by the Regulation of Artificial Intelligence Act 2026. The DSA represents a major shift in the regulation of online platforms by imposing obligations on very large online platforms (VLOPs) and very large search engines (VLOSEs) to assess and mitigate risks to civic discourse and electoral processes.

The Paper concludes that protecting election integrity cannot be achieved through content moderation or regulation alone. While the current legal and regulatory framework provides a strong foundation for safeguarding elections, it remains a work in progress. Challenges remain regarding the coordination of regulatory bodies, the promotion of trusted information, the regulation of political advertising, the operation of trusted flagger systems, and the balance between protecting elections and safeguarding freedom of expression. Furthermore, the effectiveness of many regulatory measures depends heavily on the willingness of online platforms to implement them meaningfully and consistently. Continued progress will also depend on strengthening institutional coordination, enhancing election monitoring capacity, improving access to platform data for independent researchers, and increasing the resilience of the wider information environment.

Long-term democratic resilience requires a combination of regulation, public education, institutional cooperation, media literacy, transparency, support for trusted sources of information, and effective cooperation between public authorities, civil society, academia, and online platforms. A multi-layered approach is therefore necessary to address the diverse and evolving nature of digital threats to elections.



'Ireland for All' March in Dublin. Crowds of protesters on Custom House Quay. (Image: Shutterstock)

Summary of Recommendations

This Discussion Paper makes eight recommendations designed to strengthen Ireland's capacity to protect election integrity while respecting fundamental rights and democratic values:

Recommendation 1: Expansion of the Trusted Flagger Network

Coimisiún na Meán, in cooperation with Oifig IS na hÉireann where appropriate, should continue to expand the trusted flagger system under the DSA, with particular emphasis on organisations possessing expertise in election integrity, political disinformation, foreign information manipulation and interference, and AI-generated content. Greater transparency regarding trusted flagger activities should also be encouraged.

Recommendation 2: Structured Engagement with Online Platforms on Political Advertising

Coimisiún na Meán, working alongside An Coimisiún Toghcháin and other relevant authorities, should establish a formal engagement framework with major online platforms to support compliance with political advertising obligations and encourage the responsible reintroduction of transparent political advertising where it has been withdrawn.

Recommendation 3: Alignment of Part 5 of the Electoral Reform Act 2022 with the Digital Services Act

Before Part 5 of the Electoral Reform Act 2022 is commenced, the Government should undertake a comprehensive review to ensure consistency with Ireland's obligations under the DSA. This review should clearly define the respective responsibilities of Coimisiún na Meán and An Coimisiún Toghcháin and prevent duplication or fragmentation of regulatory functions.

Recommendation 4: Establishment of a National Election Information Partnership Framework

The Department of the Taoiseach, in partnership with relevant public bodies, should develop a coordinated framework to support the dissemination and amplification of accurate and trustworthy electoral information through collaborations with fact-checkers, academic institutions, public service media, and civil society organisations.

Recommendation 5: Establishment of a National Election Integrity Coordination Mechanism

The Department of the Taoiseach, in collaboration with An Coimisiún Toghcháin, Coimisiún na Meán, Oifig IS na hÉireann, and the National Cyber Security Centre, should establish a permanent Election Integrity Coordination Mechanism to support information sharing, threat monitoring, and coordinated responses during electoral periods.

Recommendation 6: Strengthen Election Integrity Research and Monitoring Capacity

Coimisiún na Meán, in collaboration with the Department of the Taoiseach, An Coimisiún Toghcháin, and Oifig IS na hÉireann, should establish a national framework to support independent research, election monitoring, and evidence-based analysis of risks to election integrity in digital environments.

Recommendation 7: Strengthened Coordination Between SIPO and Digital Regulatory Bodies

A formal mechanism for cooperation should be established between the Standards in Public Office Commission (SIPO), Coimisiún na Meán, and An Coimisiún Toghcháin to address the growing intersection between political finance regulation and digital campaigning. This should include enhanced monitoring of online political advertising and campaign expenditure, improved information-sharing arrangements, and consultation with Oifig IS na hÉireann on the use of AI systems and synthetic media in political campaigning.

Recommendation 8: Coordination and Expansion of Existing Media Literacy Initiatives

The Government should strengthen and expand media literacy programmes across the education system and wider society to improve the public's ability to identify misinformation and disinformation and to evaluate online information critically. Building societal resilience remains one of the most effective long-term safeguards against online election interference.

Given the increasing role of AI systems, synthetic media, and automated information manipulation within online information environments, implementation of these recommendations should involve ongoing cooperation with Oifig IS na hÉireann to ensure coherence between Ireland's election integrity framework, the DSA, and the regulatory requirements arising under the EU Artificial Intelligence Act.

Conclusion

Ireland has taken significant steps in recent years to strengthen the protection of its electoral processes against evolving digital threats. However, technological change continues to outpace regulatory development, and emerging risks (particularly those associated with GenAI, digital disinformation, and foreign information manipulation) require ongoing vigilance.

Safeguarding election integrity will depend not only on effective regulation of online platforms, but also on strong institutions, informed citizens, trusted sources of information, and a coordinated whole-of-society response. By strengthening existing safeguards and implementing the recommendations outlined in this Paper, Ireland can continue to reinforce public confidence in its democratic institutions and ensure that elections remain free, fair, and resilient in the digital age.



Contents

- Executive Summary 3
- Introduction 9
- Election Integrity in a Digital World 25
- Legal and Regulatory Framework..... 37
- Assessing the Regulatory Framework..... 62
- The Future of Election Integrity..... 75
- Recommendations..... 93
- Conclusion 109



Dublin, Ireland - 24th October 2025 - A woman walks past a sign for a polling station at Saint Audoen's National School on Cook Street in Dublin city as Ireland votes in the Presidential Election (Image: Shutterstock)

Introduction

The Purpose of this Discussion Paper

It is essential to understand how Ireland is positioned to safeguard the integrity of its elections from emerging online threats, where these threats originate, and how they continue to evolve. Proactive, forward-looking measures must be developed and tested before the threat landscape intensifies. With 84% of the Irish electorate now relying on digital and online sources for news,⁴ there is a clear need to expand public education on online misinformation and disinformation.

This Discussion Paper aims to support an informed conversation regarding the extent of the threat that new and emerging technologies pose to elections in Ireland. It assesses current safeguards and explores potential future developments of regulatory frameworks. The Paper includes an in-depth analysis of the current legal framework, including relevant case law in Ireland and the European Union. It focuses in particular on the evolving risks of misinformation and disinformation, as well as the use of generative artificial intelligence (GenAI) on social media to influence the outcome of elections.

The Discussion Paper does not attempt to capture every potential threat to election integrity. Issues such as interference with the processes for updating the voting register,⁵ or the introduction of limitations to voting rights⁶ might also pose risks to election integrity.

However, the focus of this Discussion Paper is on the growing challenges arising from digital technologies and their impact on elections. A broader discussion on election integrity would necessarily extend beyond the scope of this Paper.

4 Niamh Kirk and Lauren Teeling, 'A review of political advertising online during the 2019 European Elections and establishing future regulatory requirements in Ireland' (2022) 37(1) Irish Political Studies 85, 86.

5 An Coimisiún Toghcháin, Oversight Report on the Electoral Registers (An Coimisiún Toghcháin, May 2025) <https://cdn.electoralcommission.ie/app/uploads/2025/04/30104313/Oversight-Report-on-the-Electoral-Registers_online_english_tagged.pdf> accessed 16 December 2025.

6 For example, *Sinnott v The Minister for the Environment* [2017] IEHC 214.

What is Online Election Interference?

Free elections are a cornerstone of the Irish democratic system, as they are of liberal European democracy.⁷ The right to free elections is intrinsically linked to several other human rights and freedoms. The rights to free elections,⁸ to freedom of expression, and of freedom of assembly and association⁹ are recognised as fundamental rights by the Council of Europe in part because they underpin and promote democratic values.¹⁰ Public trust in the integrity of electoral processes is essential to a functioning democracy and reinforces confidence that elected governments enjoy genuine popular support.¹¹

Attempts to influence or interfere with elections are not a new phenomenon. During the Cold War, for example, major powers employed both covert and overt measures, including bribery, coercion, propaganda, and military activity, to influence electoral outcomes in pursuit of geopolitical objectives.¹² What has changed in recent years is the scale, speed, and sophistication with which interference can now be conducted through digital technologies.

The widespread use of social media platforms, online communication tools, and increasingly powerful artificial intelligence systems has transformed the information environment in which elections take place. Digital technologies enable false or misleading information to be created and disseminated rapidly, often anonymously and at relatively low cost.¹³ They also permit coordinated influence campaigns to reach large audiences with unprecedented efficiency, while making it more difficult to identify the actors responsible.¹⁴

Online election interference may take many forms, including misinformation and disinformation campaigns, foreign information manipulation and interference (FIMI), coordinated online influence operations, cyber-attacks on electoral infrastructure, and the misuse of artificial intelligence to generate deceptive content. Advances in GenAI have further increased these risks by making it easier to produce realistic, fabricated text, images, audio recordings, and videos capable of misleading voters or undermining confidence in democratic institutions.¹⁵

Research suggests that information manipulation has become a common feature of modern elections. One study found that between 2016 and 2021, 92% of elections

7 European Commission, 'European Democracy Shield: Empowering Strong and Resilient Democracies' (Communication) JOIN (2025) 791 final.

8 Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms 1952, art 3.

9 European Convention on Human Rights 1950, arts 10 and 11.

10 Venice Commission, *Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report* (30 October 2002) CDL-AD (2002) 23,10.

11 Fiona Buckley and Theresa Reidy, 'Managing the Electoral Process: Insights from, and for, Ireland' (2015) 30(4) Irish Political Studies 445.

12 Calder Walton, 'Spies, Election Meddling, and Disinformation' (2019) 26(1) The Brown Journal of World Affairs 107, 108.

13 Jens Ohlin, 'Election Interference: A Unique Harm Requiring Election Interference' in Duncan Hollis and Jens Ohlin (eds), *Defending Democracies: Combating Foreign Election Interference in a Digital Age* (OUP 2021) 239.

14 UNESCO, 'At UNESCO, a Call to Regulate Digital Platforms in the Face of Online Disinformation and Hate' (UNESCO, 23 February 2023) <<https://www.unesco.org/en/articles/unesco-call-regulate-digital-platforms-face-online-disinformation-and-hate>> accessed 22 July 2026.

15 UNESCO-UNDP, *Freedom of Expression, Artificial Intelligence and Elections* (CI-2025/FEJ/ME-1, 2025).

worldwide were targeted by disinformation campaigns.¹⁶ More recently, the European Commission identified examples of FIMI affecting more than 80 countries and targeting hundreds of organisations worldwide.¹⁷

In Ireland, concerns regarding misinformation, disinformation, and online influence operations have become an increasingly prominent feature of public and political debate.¹⁸ European and national regulators have responded by introducing new legal and regulatory frameworks aimed at increasing transparency, strengthening platform accountability, and mitigating risks to electoral processes. Nevertheless, recent elections have demonstrated that significant challenges remain. False and misleading information can spread rapidly online, attribution is often difficult, and platform responses may not always occur quickly enough to prevent harmful content from achieving widespread reach.

Against this backdrop, it is necessary to examine both the nature of the threats facing electoral processes and the effectiveness of the existing legal and regulatory framework in safeguarding election integrity in Ireland.



Fake news propaganda conspiracy theories disinformation manipulation. (Image: Shutterstock)

16 Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, *National Counter Disinformation Strategy* (Government of Ireland, 2025) 26.

17 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (European Union, March 2025) 2.

18 Joint Committee on Tourism, Culture, Arts, Sport and Media, *The State's Response to Online Disinformation and Media/Digital Literacy, Including Social Media and Fake News* (Houses of the Oireachtas, November 2024) 7; and Brian O'Donovan, 'Rise of far-right highlighted in new study on disinformation in Ireland' (RTÉ News, 20 November 2023) <<https://www.rte.ie/news/2023/1120/1417344-disinformation-ireland/>> accessed 29 July 2026.

Definitions

Election Integrity

Election integrity refers to the conduct of elections that are free, fair, transparent, secure, and capable of maintaining public confidence in democratic outcomes.¹⁹

Election Interference

For the purposes of this Discussion Paper, election interference refers to activities intended to undermine the legitimacy of elections, weaken electoral processes, or erode trust in democratic institutions. Online election interference is a type of election interference conducted through digital means.

Election interference can take many forms, including misinformation, disinformation, FIMI, coordinated inauthentic behaviour (CIB), cyber-attacks, and the misuse of AI.

Misinformation

Misinformation refers to false or misleading information that is shared without an intention to deceive. It may result from misunderstanding, misinterpretation, or the uncritical sharing of inaccurate content.²⁰

Disinformation

Disinformation refers to false or misleading information that is deliberately created, disseminated, or amplified to deceive the public, achieve political or economic objectives, or cause public harm.²¹ Disinformation does not include accidental errors, satire, parody, or clearly identified partisan reporting of events.²²

Foreign Information Manipulation and Interference (FIMI)

Foreign Information Manipulation and Interference (FIMI) refers to coordinated and intentional activities conducted by foreign state or non-state actors, including their proxies, which seek to manipulate the information environment in a manner that threatens or has the potential to negatively affect democratic values, political processes, public debate, or societal cohesion.²³

FIMI may involve disinformation, CIB, deceptive amplification, synthetic media, or other

19 ACE Electoral Knowledge Network, 'Electoral Integrity' <<https://aceproject.org/ace-en/topics/ei/onePage>> accessed 23 July 2026; International Foundation for Electoral Systems, 'Election Integrity' <<https://www.ifes.org/our-expertise/election-integrity>> accessed 23 July 2026.

20 Claire Wardle and Hossein Derakhshan, *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making* (Council of Europe, DGI(2017)09, 2017) 5.

21 Commission, 'On the European Democracy Action Plan' (Communication) COM (2020) 790 final.

22 Commission, 'Tackling online disinformation: a European approach' (Communication) COM (2018) 236 final.

23 European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 23 July 2026; Council of the European Union, 'Disinformation and Democratic Resilience' <<https://www.consilium.europa.eu/en/policies/disinformation-and-democratic-resilience/>> accessed 23 July 2026.

forms of information manipulation. Unlike misinformation and disinformation, FIMI focuses on the broader activity and intent of a foreign influence operation rather than solely on the content being disseminated.²⁴

Coordinated Inauthentic Behaviour (CIB)

Coordinated inauthentic behaviour (CIB) refers to coordinated activity involving multiple accounts, pages, groups, or actors working together to mislead users regarding the source, popularity, or authenticity of content or political messages.²⁵

Generative Artificial Intelligence (GenAI)

Generative artificial intelligence (GenAI) refers to artificial intelligence systems capable of creating new content, including text, images, audio, video, or software code, in response to user prompts or other inputs.^{26 27} Such systems may be general-purpose GenAI platforms (for example ChatGPT, Google Gemini, Anthropic Claude, Microsoft Copilot, and Grok) or bespoke GenAI systems that are designed, configured, or approved for specific organisational, professional, or sectoral use cases.²⁸

GenAI may facilitate the creation and dissemination of misinformation, disinformation, synthetic media, and other forms of election interference at unprecedented scale and speed.

Deepfake

A deepfake is synthetic audio, video, or image content that has been generated or manipulated using artificial intelligence in a manner that falsely appears authentic or truthful.²⁹

Information Integrity

Information integrity refers to the accuracy, reliability, transparency, and trustworthiness of information within the public sphere, particularly as it relates to democratic discourse and decision making.³⁰

24 Council of the European Union, 'Disinformation and Democratic Resilience' <<https://www.consilium.europa.eu/en/policies/disinformation-and-democratic-resilience/>> accessed 23 July 2026; Nicolas Hénin, 'FIMI: Towards a European Redefinition of Foreign Interference' (EU DisinfoLab, 2023) <https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf> accessed 23 July 2026.

25 Meta, 'How We Respond to Inauthentic Behavior on Our Platforms: Policy Update' (21 October 2019) <<https://about.fb.com/news/2019/10/inauthentic-behavior-policy-update/>> accessed 23 July 2026; Cynthia Khoo, 'Coordinated Inauthentic Behavior' in *Glossary of Platform Law and Policy Terms* (FGV Direito Rio, 17 December 2021) <<https://platformglossary.info/coordinated-inauthentic-behavior/>> accessed 23 July 2026.

26 OECD, 'Initial Policy Considerations for Generative Artificial Intelligence' (OECD 2023) <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/initial-policy-considerations-for-generative-artificial-intelligence_1a9ab450/fae2d1e6-en.pdf> accessed 26 August 2026, 5.

27 Naja Bentzen, 'Information manipulation in the age of generative artificial intelligence' (European Parliamentary Research Service, December 2025) 3.

28 OECD, 'Initial Policy Considerations for Generative Artificial Intelligence' (OECD 2023) <https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/initial-policy-considerations-for-generative-artificial-intelligence_1a9ab450/fae2d1e6-en.pdf> accessed 26 August 2026, 5.

29 United Nations Regional Information Centre, 'Artificial Intelligence: What Are Deepfakes?' (15 May 2026) <<https://unric.org/en/artificial-intelligence-what-are-deepfakes/>> accessed 23 July 2026; US Government Accountability Office, 'Science & Technology Spotlight: Combating Deepfakes' (GAO-24-107292, 11 March 2024) <<https://www.gao.gov/products/gao-24-107292>> accessed 23 July 2026.

30 United Nations, 'Information Integrity' <<https://www.un.org/en/information-integrity>> accessed 23 July 2026; United Nations, 'United Nations Global Principles for Information Integrity' <<https://www.un.org/en/information-integrity/global-principles>> accessed 23 July 2026.

Status of Misinformation and Disinformation in Law

Neither misinformation nor disinformation is currently defined in EU law. While both concepts are widely used in EU policy documents and regulatory guidance, including those relating to the Digital Services Act (DSA) and the European Democracy Action Plan,³¹ the EU's regulatory approach generally focuses on the risks posed by misleading content rather than on statutory classification of the content itself.

In Ireland, Part 5 of the Electoral Reform Act 2022 contains proposed definitions of misinformation and disinformation, but those provisions have not been commenced. Consequently, there is at present no operative statutory definition of either term in Irish law.



Votes being counted at the RDS in Dublin. (Image: Shutterstock)

31 For example, under the Digital Services Act, disinformation may be addressed within the framework of illegal content: 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 (Digital Services Act)[2022] OJ L 277/1, recital 9. See also Commission, *On the European Democracy Action Plan* COM (2020) 790.

Challenges Posed by Online Election Interference

Disinformation and misinformation create significant challenges for national governments, both in verifying the vast volume of content produced each day and in addressing the misconceptions that arise from it. Disinformation has, in several instances, spread rapidly, aided by limited transparency in respect of social media accounts and by platform responses that often come too late to prevent false information from reaching a wide audience.³²

Additionally, it can be difficult to differentiate acts that constitute disinformation, which is the creation and dissemination of false information with intent to deceive, from misinformation, which includes genuine misconceptions or misunderstanding of the facts. An example can be found in the case of *Salov v Ukraine*, in which the applicant circulated a fabricated version of a Ukrainian national newspaper that contained false claims that the President of Ukraine had died and been replaced by an impostor.³³ While the applicant had shared false information, they alleged they had done so with the asserted belief that the information was true. The European Court of Human Rights determined that discussion of the information, while untrue, was protected by the right to freedom of expression under Article 10 of the European Convention on Human Rights.³⁴ Similarly, in the Polish case of *Brzeziński v Poland*, the European Court of Human Rights held that, while the aim of protecting fair electoral processes from fake news is a legitimate aim, there is a limit to the extent to which that aim can interfere with the freedom of expression.³⁵

The dissemination of misinformation and disinformation during the period leading up to elections in Ireland has become increasingly prevalent in recent years. While rogue states run official and semi-official campaigns to influence voters across Europe, the 2025 Irish presidential election demonstrated that individuals within Ireland can create and promote false narratives to advance personal political agendas. In 2018, the dissemination of dubious claims in the week preceding Ireland's referendum on whether to repeal or retain the Eighth Amendment to the Constitution led some voters to recall "false memories" of fabricated news stories about the campaign.³⁶ In a survey by Coimisiún na Meán, 68% of respondents to the Digital News Report stated that they were concerned about what was real or fake in terms of online news.³⁷

32 Philip N Howard, Bharath Ganesh and others, *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (Computational Propaganda Research Project, University of Oxford 2018).

33 *Salov v Ukraine* App no 65518/01 (ECtHR, 2005) [13].

34 *Salov v Ukraine* App no 65518/01 (ECtHR, 2005) [113]-[114].

35 This case is discussed in further detail later in this Discussion Paper (page 40). *Brzeziński v Poland* App no 47542/07 (ECtHR, 2019).

36 Gillian Murphy and others, 'False Memories for Fake News During Ireland's Abortion Referendum' (2019) 30(10) *Psychological Science* 1449.

37 Coimisiún na Meán, 'Digital News Report Ireland 2025' (17 June 2025) <<https://www.cnam.ie/digital-news-report-ireland-2025/>> accessed 8 December 2025.

Risks of Generative Artificial Intelligence in the Information Sphere

GenAI introduces additional challenges for states seeking to combat misinformation and disinformation.³⁸ It transforms the information landscape through its ability to quickly create large volumes of content that appears plausible and factual. In the context of a disinformation campaign, this means that a substantial quantity of false or misleading material can be created in a short time, creating persuasive narratives designed to mislead voters on a range of political topics.³⁹

The volume of unverified and user-generated information available through online platforms has changed the information landscape and is increasingly influencing and polarising voters' perceptions.⁴⁰ Some social media bots are known to spread false or misleading information, amplifying divisive content, and perpetrating scams. Research has documented the use of such bots in a range of electoral contexts, including the 2010 US midterm elections and the 2016 US presidential election, where automated accounts on social media platforms interacted with users while presenting themselves as authentic participants in public debate.⁴¹ These risks are particularly evident in electoral contexts.

The Council of Europe has noted that advanced AI technologies (defined as machine-based systems that generate outputs based on input data) have been used to “tamper” with elections and influence voting patterns.⁴² Some elections across the European Union from 2023 to 2025 provided early indications of the growing role of GenAI technology on electoral processes.

A recent example of GenAI in electoral processes can be found in the 2025 Irish Presidential Election.

Example: Irish Presidential Election 2025

Reports indicate that during the 2025 Irish Presidential Election, all three primary candidates – Catherine Connolly, Heather Humphreys, and Jim Gavin – were targeted by disinformation campaigns involving GenAI. False information ranged from unsubstantiated allegations that the presidential candidates were affiliated with controversial groups to digitally fabricated videos purporting to show the candidates making manifestly untrue statements.⁴³

38 European External Action Service, '3rd EEAS Report on Foreign Information Manipulation and Interference Threats' (European Union, March 2025) 11.

39 Aqsa Farooq and others, 'Generative AI Generating Concerns: Citizens Perspectives During the 2024 European Elections' (2025) *The International Journal of Press/Politics* 1, 3.

40 Anna Elisabetta Galeotti, 'Political Disinformation and Voting Behavior: Fake News and Motivated Reasoning' (2020) 37(142) *Politeia* 64, 65-66.

41 Nick Hajli and others, 'Social Bots and the Spread of Disinformation in Social Media: The Challenges of Artificial Intelligence' (2022) 33(3) *British Journal of Management* 1238.

42 Venice Commission, Interpretative Declaration of the Code of Good Practice in Electoral Matters as Concerns Digital Technologies and Artificial Intelligence (Council of Europe, 10 December 2024) 6.

43 Institute for Strategic Dialogue, 'Irish presidential election 2025: Renewed attacks on election integrity and repeated platform failures' (Institute for Strategic Dialogue, 31 October 2025) <https://www.isdglobal.org/digital_dispatches/irish-presidential-election-2025-renewed-attacks-on-election-integrity-and-repeated-platform-failures/> accessed 3 December 2025.

Research by the Microsoft AI for Good Lab found that humans often struggle to differentiate between authentic images and those produced by AI.⁴⁴ The same research found that identifying AI-generated images becomes more difficult when genuine images have been manipulated by AI tools.⁴⁵ As GenAI models become more sophisticated in producing photorealistic content,⁴⁶ the public may face significant challenges in recognising false content, such as the videos that purported to show Catherine Connolly withdrawing from the Irish Presidential race.

Current research does not demonstrate that GenAI directly influences election results.⁴⁷ However, researchers have found that AI-enabled misinformation may contribute to political polarisation, undermine trust in online information, and facilitate attacks on political figures.⁴⁸ An example of this occurred during the 2025 Dutch general election campaign.

Example: Dutch General Election 2025

During the 2025 general election campaign in the Netherlands, Partij voor de Vrijheid (PVV) leader Geert Wilders launched his party's campaign with an AI-generated video depicting a fictional future Netherlands living under Sharia law.⁴⁹ Researchers later found that PVV-linked accounts were responsible for a significant proportion of AI-generated election content online. Separately, it emerged that two PVV members of parliament had been involved in circulating AI-generated images targeting opposition leader Frans Timmermans. Following these revelations, Wilders publicly apologised to Timmermans.⁵⁰ Professor Claes de Vreese of the University of Amsterdam described the election as “one of the first elections in Europe where we see that [AI] has become an integral part in electoral campaigns”.⁵¹

It is well established that risks to political figures arise from the misuse of GenAI to create realistic but false audio, image, and video content depicting them saying or doing things that never occurred.⁵² During the Slovakian parliamentary election in 2023, for example, a fake audio recording was circulated in an apparent attempt to discredit one of the presidential candidates.

44 Thomas Roca and others, 'How Good Are Humans at Detecting AI-Generated Images? Learnings from an Experiment' (ArXiv, May 2025) 8 <https://www.researchgate.net/publication/394048511_How_good_are_humans_at_detecting_AI-generated_images_Learnings_from_an_experiment> accessed 9 December 2025.

45 *ibid* 7.

46 *ibid* 7.

47 Sam Stockwell, 'AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections' (The Alan Turing Institute, 19 September 2024) 27.

48 *ibid* 17.

49 Pieter Haeck and Eva Hartog, 'The week that AI deepfakes hit Europe's elections' (Politico, 31 October 2025) <<https://www.politico.eu/article/elections-europe-ai-deepfakes-social-media/>> accessed 9 December 2025.

50 *ibid*.

51 Pieter Haeck and Eva Hartog, 'The week that AI deepfakes hit Europe's elections' (Politico, 31 October 2025) <<https://www.politico.eu/article/elections-europe-ai-deepfakes-social-media/>> accessed 6 January 2026.

52 Ian Sample, 'What are Deepfakes? And How can You Spot Them', (The Guardian, 13 January 2020) <<https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them>> accessed 17 December 2025.

Example: Slovakian Parliamentary Election 2023

In September 2023, shortly before Slovakia's parliamentary election, AI-generated audio recordings were circulated online purporting to show Progressive Slovakia leader Michal Šimečka discussing election manipulation with a journalist and, in a separate recording, proposing substantial increases in beer prices.⁵³ The recordings quickly went viral but were subsequently identified as deepfakes generated using artificial intelligence. The recordings were released during Slovakia's pre-election moratorium period, which limited opportunities for political actors and media organisations to respond publicly before polling took place. Although Progressive Slovakia was ultimately defeated in the election, the extent to which the deepfake recordings influenced voting behaviour remains uncertain. Commentators have cautioned against drawing a direct causal connection between the disinformation campaign and the election outcome.⁵⁴

The growing use of GenAI to fabricate the words and actions of candidates will make it increasingly difficult for the public to determine what is genuine and what is not. Additionally, the use of AI-generated images, video and audio content provides creators of disinformation with additional tools to discredit political candidates.⁵⁵

Regulatory and Enforcement Challenges Relating to Malicious Deepfakes

The increasing use of AI-generated content in electoral contexts has prompted calls for stronger regulatory intervention, including the criminalisation of malicious deepfakes intended to mislead voters or undermine confidence in democratic institutions.⁵⁶ While the harms associated with deceptive synthetic media are increasingly recognised, the creation of effective legal sanctions presents significant challenges.

One difficulty concerns the definition of harmful deepfakes. GenAI technologies are capable of producing a wide spectrum of synthetic content, much of which is lawful and used for artistic, educational, satirical, or entertainment purposes.⁵⁷ Any attempt to prohibit deepfakes outright would risk interfering disproportionately with freedom of expression.⁵⁸ Consequently, regulatory proposals generally focus on deepfakes created or disseminated with the intention of deceiving the public and causing harm, particularly where the content falsely attributes statements or actions to political candidates during electoral periods.⁵⁹

53 Curt Devine, Donie O'Sullivan and Sean Lyngaas, 'A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning' (CNN, 1 February 2024) <<https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html>> accessed 17 December 2025.

54 Curt Devine, Donie O'Sullivan and Sean Lyngaas, 'A fake recording of a candidate saying he'd rigged the election went viral. Experts say it's only the beginning' (CNN, 1 February 2024) <<https://edition.cnn.com/2024/02/01/politics/election-deepfake-threats-invs/index.html>> accessed 17 December 2025; Lluís de Nadal and Peter Jančárik, 'Beyond the Deepfake Hype: AI, Democracy, and "the Slovak Case"' (Harvard Kennedy School Misinformation Review, 2024) <<https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/>> accessed 27 July 2026.

55 National Cyber Security Centre, *Annual Review 2023* (GCHQ 2023) 40.

56 Shanze Hasan and Abdiaziz Ahmed, 'Gauging the AI Threat to Free and Fair Elections' (Brennan Center for Justice, 6 March 2025) <<https://www.brennancenter.org/our-work/analysis-opinion/gauging-ai-threat-free-and-fair-elections>> accessed 24 July 2026; Phumzile Van Damme, *Future-Proofing Elections Against Deepfake Disinformation* (CIVICUS Digital Democracy Initiative, 2025) <<https://www.civicus.org/documents/ddi/final-deepfakes-elections-report-civicus-ddi-research-2025.pdf>> accessed 24 July 2026.

57 UNESCO, *Synthetic Content and its Implications for AI Policy: A Primer* (UNESCO, 2024) <<https://unesdoc.unesco.org/ark:/48223/pf0000392181>> accessed 24 July 2026; Sam Gregory and others, *JUST JOKING! Deepfakes, Satire, and the Politics of Synthetic Media* (MIT Open Documentary Lab and WITNESS, 2023) <<https://cocreationstudio.mit.edu/just-joking/>> accessed 24 July 2026.

58 Alex Barber, 'Freedom of Expression Meets Deepfakes' (2023) 202 *Synthese* 40 <<https://link.springer.com/article/10.1007/s11229-023-04266-4>> accessed 24 July 2026.

59 Eugen Tomac, 'Use of Deepfakes in the EU's Electoral Processes' (Question for Written Answer E-000462/2024, 12 February 2024) <https://www.europarl.europa.eu/doceo/document/E-9-2024-000462_EN.html> accessed 24 July 2026.

A second challenge relates to the evidential issues associated with proving that content is AI-generated. Although technical tools exist to identify synthetic media, advances in GenAI continue to reduce the reliability of traditional detection methods.⁶⁰ Researchers have found that both human observers and automated systems may struggle to distinguish genuine content from sophisticated AI-generated material.⁶¹ As detection technology and generative technology continue to evolve in parallel, evidential certainty may become increasingly difficult to establish.

Establishing intent may be even more difficult. The distinction between misinformation and disinformation depends substantially on whether the creator intended to deceive.⁶² In many cases, a malicious actor may create a fabricated video while anonymous users subsequently redistribute the material believing it to be genuine.⁶³ While the original creator may have acted with deceptive intent, subsequent distributors may not possess the requisite mental element necessary for criminal liability.⁶⁴ Any legislative response seeking to criminalise harmful deepfakes would therefore need to carefully distinguish between intentional deception and the inadvertent sharing of false information.⁶⁵

Attribution creates an additional challenge, as deepfake content may be generated outside the jurisdiction, distributed through anonymous or pseudonymous accounts, amplified by automated networks, and reposted across multiple platforms within a short period of time.⁶⁶ The decentralised nature of online communication often makes it difficult to identify the original source of content. Even where investigators can trace a deepfake to a particular account, establishing the identity of the individual responsible may require cross-border cooperation involving online platforms, internet service providers, and foreign authorities.⁶⁷

For these reasons, many commentators favour a layered regulatory response rather than reliance solely upon criminal sanctions.⁶⁸ Such an approach combines transparency obligations under Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (the

-
- 60 David Ghiurău and Daniela Elena Popescu, 'Distinguishing Reality from AI: Approaches for Detecting Synthetic Content' (2025) 14(1) Computers <<https://www.mdpi.com/2073-431X/14/1/1>> accessed 24 July 2026.
 - 61 Di Cooke, Abigail Edwards, Sophia Barkoff and Kathryn Kelly, 'As Good as a Coin Toss: Human Detection of AI-Generated Content' (2025) 68(10) Communications of the ACM <<https://cacm.acm.org/research/as-good-as-a-coin-toss-human-detection-of-ai-generated-content/>> accessed 24 July 2026.
 - 62 European Commission, *Strengthened Code of Practice on Disinformation 2022* (2022) <https://disinfocode.eu/assets/pdfs/2022_Strengthened_Code_of_Practice_Disinformation.pdf> accessed 24 July 2026 Preamble defining disinformation as 'verifiably false or misleading information' that is created, presented and disseminated 'to intentionally deceive the public'.
 - 63 European Commission, 'A Strengthened EU Code of Practice on Disinformation' (European Commission, 2022) <https://commission.europa.eu/topics/countering-information-manipulation/strengthened-eu-code-practice-disinformation_en> accessed 24 July 2026.
 - 64 Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026.
 - 65 Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026; Charter of Fundamental Rights of the European Union [2016] OJ C202/389, art 11.
 - 66 US Government Accountability Office, *Science & Tech Spotlight: Combating Deepfakes* (GAO-24-107292, 11 March 2024) <<https://www.gao.gov/products/gao-24-107292>> accessed 24 July 2026; Insikt Group, *2024 Deepfakes and Political Disinformation Report: Emerging Threats & Mitigation Strategies* (24 September 2024) <<https://www.recordedfuture.com/research/targets-objectives-emerging-tactics-political-deepfakes>> accessed 24 July 2026.
 - 67 Europol, Eurojust and the European Judicial Network, *SIRIUS European Union Electronic Evidence Situation Report 2024* (28 November 2024) <<https://www.europol.europa.eu/media-press/newsroom/news/new-sirius-report-%E2%80%93-accessing-electronic-evidence-in-2024>> accessed 24 July 2026; EU CyberNet, 'Cross-Border Access to Electronic Evidence (SIRIUS)' <<https://www.eucybernet.eu/project/sirius/>> accessed 24 July 2026.
 - 68 Jana Kazaz, *Regulating Deepfakes: Global Approaches to Combatting AI-Driven Manipulation* (Centre for Democracy & Resilience, 2024) <<https://www.globsec.org/sites/default/files/2024-12/Regulating%20Deepfakes%20-%20Global%20Approaches%20to%20Combatting%20AI-Driven%20Manipulation%20policy%20paper%20ver4%20web.pdf>> accessed 24 July 2026; Max-Paul Förster, Luca Deck, Raimund Weidlich and Niklas Kühl, 'A Multi-Level Strategy for Deepfake Content Moderation under EU Regulation' (arXiv, 10 July 2025) <<https://arxiv.org/html/2507.08879v1>> accessed 24 July 2026.

EU Artificial Intelligence Act), platform responsibilities under the DSA, fact-checking mechanisms, trusted flagger systems, public awareness initiatives, and media literacy programmes.⁶⁹ Criminal offences may nevertheless play an important role in addressing the most serious cases, particularly where synthetic media are deliberately created or disseminated for the purpose of interfering with elections, defrauding voters, or causing significant public harm.

Disinformation and False Narrative Campaigns

GenAI can be used to generate highly realistic videos that falsely depict political figures saying or doing things that never occurred.⁷⁰ The misuse of AI in this way enables the rapid generation of large amounts of false information, increasing the likelihood that existing misconceptions will be reinforced.⁷¹ Combined with the use of botnets – large networks of bots controlled remotely – which amplify and share false information through the internet, hybrid attacks using GenAI can create the illusion of widespread support or pervasive opposition to political viewpoints in a strategy called ‘political astroturfing’.⁷²

Globally, automated traffic constitutes a significant proportion of internet activity. For example, a 2024 report found that bots accounted for approximately 49.6% of all internet traffic in 2023, highlighting the scale of non-human activity online.⁷³ Not all of this is attributable to malicious botnets; however, the prevalence of automated activity means that some interactions with election-related content on social media may not always reflect solely human participation. This can make it more difficult to accurately determine the extent of genuine public engagement with such content.

The effect of false narratives online is particularly strong among groups that are already wary or distrustful of traditional media.⁷⁴ Following the 2020 US Presidential Election, for instance, Donald Trump made allegations that the election had been rigged. These allegations had a significant effect on a segment of Trump’s core supporter base, some of whom subsequently attempted to uncover evidence of electoral misconduct, highlighting how misinformation can erode public trust in electoral processes.⁷⁵ The European Digital Media Observatory (EDMO) has noted that there is a need for heightened vigilance regarding specific topics such as immigration, for example.⁷⁶ The EDMO also highlighted that, while certain disinformation campaigns originated with foreign actors, their continued spread often depended on local individuals who came to believe and further disseminated the misleading content.⁷⁷ As these narratives circulate more widely, the distinction between

69 European Commission, ‘Trusted Flaggers under the Digital Services Act (DSA)’ (17 June 2026) <<https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>> accessed 24 July 2026; Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts 50 and 52.

70 Ian Sample, ‘What are Deepfakes? And How can You Spot Them’, The Guardian (13 January 2020) <<https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them>> accessed 9 December 2025.

71 Luca Nannini and others, ‘Beyond phase-in: assessing impacts on disinformation of the EU Digital Services Act’ (2025) 5 AI and Ethics 1241.

72 Franziska B Keller and others, ‘Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign’ (2020) 37(2) Political Communication 256, 289.

73 Imperva, 2024 Bad Bot Report (April 2024) <<https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/>> accessed 9 December 2025.

74 Andreas Goldberg and Carolina Plescia, ‘Election integrity across Europe: who thinks elections are held fairly and why?’ (2024) 16(4) European Political Science Review 612, 616.

75 Christine Bohan, ‘The new misinformation around elections’ (The Journal, 14 March 2024) <<https://www.factchecking.ie/articles/the-new-misinformation-around-elections#anchor-2>> accessed 6 January 2026.

76 European Digital Media Observatory, ‘Final Report - Outputs and outcomes of a community-wide effort’ (EDMO, 24 July 2024) 4.

77 European Digital Media Observatory, ‘Propaganda and Disinformation: Lessons from 2024/25 Elections in Europe’ (EDMO, 10 June 2025) <<https://edmo.eu/edmo-news/propaganda-and-disinformation-lessons-from-2024-25-elections-in-europe/>> accessed 26 August 2026.

deliberate disinformation and organically shared misinformation becomes increasingly difficult to draw.

Coordinated attempts of FIMI were identified across multiple elections in Europe during 2024.⁷⁸ For example, false narratives concerning voter fraud, foreign influence, and unfair practices were widespread in at least 11 European countries.⁷⁹ An assessment in Ireland concluded that there was a ‘medium’ level of risk relating to FIMI, which includes misinformation and disinformation, towards election candidates.⁸⁰ By the time the 2024 Irish General Election came around, several instances of false claims about electoral candidates were found by the Institute for Strategic Dialogue.⁸¹

Example: Irish General Election 2024

An example of this arose during Ireland’s general election in 2024. Having failed to secure seats in Dáil Éireann during the election, some independent candidates and political parties distributed false information in the form of conspiracy theories.⁸² In one particular instance, a minor political party suggested that electoral fraud had occurred due to the low number of votes they had received.⁸³

According to The Journal, all major far-right parties in Ireland suggested the 2024 general election was illegitimate.⁸⁴ This suggestion was predicted by the Institute for Strategic Dialogue prior to the general election, indicating the growing narrative of challenging electoral processes.⁸⁵

False narrative campaigns can also have significant consequences for electoral candidates. Research indicates that candidates are frequently targeted by coordinated online attacks and disinformation relating to their personal character and public reputation.⁸⁶ The broader implications of these harms for political participation and representative democracy are discussed later in this Paper.

78 European Digital Media Observatory, ‘Final Report: Outputs and outcomes of a community-wide effort’ (EDMO, 24 July 2024) 5.

79 European Digital Media Observatory, ‘Final Report: Outputs and outcomes of a community-wide effort’ (EDMO, 24 July 2024) 5.

80 National Cyber Security Centre, General Election 2024 Cyber Threat Landscape (Department of the Environment, Climate and Communications, November 2024).

81 Aidan O’Brien, ‘Analysing Claims of Electoral Interference During the Irish Local and European Elections’ (Institute for Strategic Dialogue, 26 November 2024) 6.

82 Sasko Lazarov, ‘Factcheck: Disappointed by Failed Campaigns, Far-Right Candidates Turn to Claims of Election Rigging’ (The Journal, 2 December 2024) <<https://www.thejournal.ie/conspiracy-theories-that-the-n2024-irish-general-election-were-rigged-spread-by-far-right-parties-6560663-Dec2024>> accessed 9 December 2025.

83 *ibid.*

84 *ibid.*

85 Aidan O’Brien, ‘Analysing Claims of Electoral Interference During the Irish Local and European Elections’ (Institute for Strategic Dialogue, 26 November 2024) 16.

86 Coimisiún na Meán, ‘On the digital campaign trail: Election candidates’ online experiences in the 2024 elections’ (Coimisiún na Meán, 3 September 2025) 8.

Coordinated Inauthentic Behaviour and Influence Operations

A growing area of concern for election integrity is the use of CIB to manipulate online discourse.⁸⁷ CIB is commonly used by online platforms, researchers, and regulators to describe organised efforts in which multiple accounts or actors work together to mislead users regarding the origin, popularity, or authenticity of political content. The defining feature of CIB is not necessarily the content itself, but the deceptive methods used to amplify and distribute that content.⁸⁸

CIB frequently involves networks of accounts that appear independent but are in fact controlled by the same organisation, state actor, political movement, or coordinated group.⁸⁹ Such accounts are often used to artificially amplify political messages, create the appearance of widespread public support, or harass opponents. In some instances, these activities form part of broader influence operations designed to shape public perceptions, increase political polarisation, or undermine confidence in democratic institutions.⁹⁰

One common mechanism used in coordinated influence operations is the deployment of fake account networks. These networks may consist of automated accounts (“bots”), accounts operated by individuals using false identities, or a combination of both.⁹¹ By simultaneously liking, sharing, commenting upon, or reposting content, such networks can increase the visibility of particular narratives and exploit platform recommendation algorithms.⁹² The artificial amplification of content can create the misleading impression that a particular viewpoint enjoys substantial public support, even where genuine engagement is relatively limited.

Related practices include ‘troll farms’, whereby organised groups of individuals operate networks of anonymous or misleading online accounts to create, disseminate, and amplify political content while concealing their identities or affiliations.⁹³ Troll farms have frequently been associated with FIMI campaigns and have been identified in several elections and political processes worldwide.⁹⁴ Their activities may include spreading disinformation,

87 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.

88 Institute for Strategic Dialogue, ‘Coordinated Inauthentic Behaviour’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.

89 *ibid.*

90 Institute for Strategic Dialogue, ‘Coordinated Inauthentic Behaviour’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026; Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026.

91 Institute for Strategic Dialogue, ‘Coordinated Inauthentic Behaviour’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026; Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026.

92 Institute for Strategic Dialogue, ‘Coordinated Inauthentic Behaviour’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026; Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026.

93 Stephen Blinder and Jacob Ware, ‘In Sweden, a Domestic Troll Farm Tests Democracy’ (Global Network on Extremism and Technology, 28 October 2024) <<https://gnet-research.org/2024/10/28/in-sweden-a-domestic-troll-farm-tests-democracy/>> accessed 24 July 2026; Institute for Strategic Dialogue, ‘Coordinated Inauthentic Behaviour’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026.

94 European External Action Service, ‘Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)’ (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026; Institute for Strategic Dialogue, ‘Foreign Information Manipulation and Interference’ <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/foreign-information-manipulation-and-interference/>> accessed 24 July 2026.

attacking political candidates, encouraging social division, or amplifying existing societal grievances.⁹⁵ In contrast to traditional political campaigning, such activities are characterised by concealment of sponsorship, coordination between multiple accounts, and efforts to disguise the true source of the information being disseminated.⁹⁶

The threat posed by CIB extends beyond the dissemination of individual pieces of false content. Such operations seek to manipulate the information environment itself. By creating the appearance of consensus, popularity, or controversy, coordinated networks can influence how users perceive public opinion and determine which issues receive attention.⁹⁷ This can distort democratic discourse even where the underlying content would otherwise attract little interest or engagement.

Recent technological developments have increased the sophistication of such operations. GenAI enables the large-scale production of realistic text, images, and videos that can be distributed through coordinated networks of accounts.⁹⁸ AI systems may also facilitate the creation of convincing fictitious online personas, making it increasingly difficult for users, journalists, and regulators to distinguish genuine political participation from organised manipulation.⁹⁹ The convergence of GenAI and coordinated influence operations therefore creates new challenges for election integrity, particularly when false information can be disseminated rapidly across multiple platforms.¹⁰⁰

The DSA addresses some aspects of these risks through its systemic-risk framework. In particular, the European Commission's guidance on elections under the DSA identifies coordinated manipulation, deceptive account behaviour, and threats to civic discourse as risks requiring assessment and mitigation by very large online platforms (VLOPs) and very large online search engines (VLOSEs).¹⁰¹ Similarly, online platforms increasingly publish

- 95 Global Disinformation Index, 'FIMI-ISAC Collective Findings Report on 2024 European Elections' (21 October 2024) <<https://www.disinformationindex.org/research/2024-10-21-fimi-isac-collective-findings-report-on-2024-european-elections/>> accessed 24 July 2026; European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026.
- 96 European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 8 August 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.
- 97 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; Institute for Strategic Dialogue, 'Coordinated Inauthentic Behaviour' <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.
- 98 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 8 August 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.
- 99 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; Institute for Strategic Dialogue, 'Coordinated Inauthentic Behaviour' <<https://www.isdglobal.org/our-expertise/information-warfare-and-online-manipulation/coordinated-inauthentic-behaviour/>> accessed 24 July 2026.
- 100 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026 (noting that evolving technologies can exacerbate information manipulation and create risks for democratic processes and elections); Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.
- 101 European Commission, 'Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes' (26 April 2024) <<https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes>> accessed 24 July 2026 (providing guidance on compliance with Articles 34 and 35 of Regulation (EU) 2022/2065 in relation to risks affecting electoral processes); European Commission, 'Commission Presents New Best-Practice Election Toolkit on the Digital Services Act' (20 February 2025) <<https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-best-practice-election-toolkit-digital-services-act>> accessed 24 July 2026.

transparency reports detailing the removal of coordinated inauthentic behaviour networks and FIMI operations. However, the effectiveness of these measures remains dependent upon platforms' ability to identify such networks and their willingness to take timely action when manipulation is detected.¹⁰²

In the context of election integrity, coordinated inauthentic behaviour represents a significant challenge because it exploits the architecture of digital platforms rather than relying solely on persuasion.¹⁰³ While traditional political debate remains protected as part of democratic discourse, influence operations that depend upon deception regarding identity, coordination, or sponsorship fundamentally undermine transparency and informed democratic participation.¹⁰⁴ Strengthening resilience against these tactics therefore requires a combination of platform accountability, regulatory oversight, transparency measures, independent research, and public awareness initiatives.¹⁰⁵

These false narratives mainly centred around accusations of voter fraud or alleged unfair practices, which were likely attempts to undermine democratically elected representatives' legitimacy and to discredit the elections.¹⁰⁶

102 European Commission, 'Commission Presents New Best-Practice Election Toolkit on the Digital Services Act' (20 February 2025) <<https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-best-practice-election-toolkit-digital-services-act>> accessed 24 July 2026; European Commission, *Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes* (26 April 2024) <<https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes>> accessed 24 July 2026; European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026.

103 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; Ana Romero Vicente, *Coordinated Inauthentic Behaviour Detection Tree* (EU DisinfoLab, 2024) <<https://www.disinfo.eu/publications/coordinated-inauthentic-behaviour-detection-tree/>> accessed 24 July 2026.

104 European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026; Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026.

105 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU's Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 24 July 2026; European Commission, 'Commission Presents New Best-Practice Election Toolkit on the Digital Services Act' (20 February 2025) <<https://digital-strategy.ec.europa.eu/en/news/commission-presents-new-best-practice-election-toolkit-digital-services-act>> accessed 24 July 2026.

106 European Digital Media Observatory, 'Final Report: Outputs and outcomes of a community-wide effort' (EDMO, 24 July 2024) 5.

Election Integrity in a Digital World



E-VOTING



Election Integrity in a Digital World

Malicious actors target elections for various reasons, including to secure geopolitical objectives, disrupt democratic states, push ideologies, or for personal gain.¹⁰⁷ The ability of digital technologies – particularly social media and messaging platforms – to circumvent the regulation of electoral processes and to bypass the gatekeeping role of traditional media has significantly altered the information environment surrounding elections. This can ultimately lead to the erosion of public trust in the outcome of elections.

The European Union Agency for Cybersecurity defines the misuse of information to influence or disrupt elections as Foreign Information Manipulation and Interference (FIMI):

“[FIMI] describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.”¹⁰⁸

As noted above, the pattern of interference often (but not always) uses mechanisms that are not in themselves illegal. In 2024, the European Union’s European External Action Service (EEAS) analysed and identified trends in foreign information manipulations on more than 25 different platforms.¹⁰⁹ Across Europe, the EEAS found disinformation campaigns directed at the French legislative elections, the German coalition government, and interference in Moldovan elections and EU accession.¹¹⁰



In the digital underworld, cyberattacks surge like sinister waves, overshadowing the landscape of election security. (Image: Shutterstock)

107 ENISA, *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape* (European Union Agency for Cybersecurity 2022) 12.

108 ENISA, *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape* (European Union Agency for Cybersecurity 2022) 6.

109 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (European Union, March 2025) 9.

110 *ibid.*

State Actors and False Information

A coordinated approach towards disinformation is particularly impactful when supported by foreign states that have a vested interest in influencing politics for their own benefit. In October 2024, the US Intelligence Community publicly proclaimed that Russia and Iran were attempting to influence the 2024 US presidential campaign, whereas China was determined to be focused on the congressional and other races.¹¹¹ In the same month, the European Parliament adopted a resolution condemning Russia's escalating malicious activity, interference, and hybrid operations. The resolution was issued ahead of Moldovans going to the polls for the country's presidential election and its constitutional referendum on EU integration.¹¹²

In terms of online threats to election integrity within Europe, one of the primary actors has been Russia.¹¹³ The UK's National Cyber Security Centre found that Russia (alongside China and the Democratic People's Republic of Korea) were using Generative AI (GenAI) to engage in social engineering to further their own economic and geopolitical objectives.¹¹⁴ However, in 2019, the UK's Select Committee on Culture, Media and Sport found that, although there was evidence of Russian interference in electoral processes, there was little evidence of this activity having a material impact on the outcome of elections.¹¹⁵

While misinformation, disinformation, and foreign influence operations may affect public discourse, political trust, and perceptions of legitimacy, demonstrating a direct causal effect on electoral outcomes has, however, proven considerably more difficult. Similarly, despite fears of Russian disinformation campaigns in 2026's Hungarian parliamentary election, analysts say the impact was "more limited than feared".¹¹⁶

State actors can increase the threat of election interference by using their vast resources to support campaigns. In particular, large states can more effectively coordinate disinformation campaigns alongside traditional propaganda and financing separatist movements, to create a cascade effect in influencing foreign politics.¹¹⁷

The threat posed by states in sponsoring online election interference is widely recognised internationally. The National Cyber Security Centre considers that there have been numerous state-sponsored attempts at malign election interference in Western democratic nations.¹¹⁸ In *Bradshaw v United Kingdom*, the applicants alleged to the European Court of Human Rights that the UK Government's refusal to investigate claims of election interference by Russia was a breach of the right to free elections.¹¹⁹ The Court in *Bradshaw*

111 Office of the Director of National Intelligence, '30 Day Election Security Update from the Intelligence Community' (US Department of State, 7 October 2024) <<https://2021-2025.state.gov/briefings-foreign-press-centers/2024-elections-fpc/30-day-election-security-update-from-intelligence-community>> accessed 9 December 2025.

112 Resolution on Strengthening Moldova's Resilience against Russian Interference ahead of the Upcoming Presidential Elections and a Constitutional Referendum on EU Integration, European Parliament, 2024/2821 (RSP).

113 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (European Union, March 2025) 22.

114 National Cyber Security Centre (UK), *Annual Review 2025* (GCHQ 2025) 22.

115 Digital, Culture, Media and Sport Committee (UK), *Disinformation and 'fake news': Final Report* (House of Commons 18 February 2019) HC 1791, 70.

116 NewsGuard analyst Alice Lee, quoted in Anna Desmarais, "Fabricating proof": The disinformation tactics that shaped Hungary's election' (Euronews, 13 April 2026) <<https://www.euronews.com/next/2026/04/13/fabricating-proof-the-disinformation-tactics-that-shaped-hungarys-election>> accessed 30 April 2026.

117 Ancuța Hansen, 'How Russia tried to manipulate Moldova's election – and what it reveals' (Lowy Institute, 27 November 2025) <<https://www.lowyinstitute.org/the-interpreter/how-russia-tried-manipulate-moldova-s-election-what-it-reveals>> accessed 9 January 2026.

118 National Cyber Security Centre, *General Election 2024 Cyber Threat Landscape* (Department of the Environment, Climate and Communications, November 2024).

119 *Bradshaw and others v United Kingdom* App no 15653/22 (ECtHR, 22 July 2025).

agreed that State actors have “weaponised” disinformation for the purpose of interfering in elections in order to destabilise democratic nations.¹²⁰

At the same time, unknown hackers, private persons, or splinter groups within countries can also be the architects of disinformation campaigns. In 2020, researchers found disinformation campaigns disseminated via social media by over 80 countries and linked entities.¹²¹ Bolstered by non-affiliated individuals sharing misinformation, online disinformation campaigns targeting elections have become an intrinsic part of the political power struggle across the globe.

Voter Suppression

There have been multiple documented instances of technological innovations being used to facilitate voter suppression. Even before the rise of social media, automated scam calls were deployed in Canada to mislead voters by providing false information about the location of their nearest polling station, as considered in *McEwing v Canada*.¹²²

Example: McEwing v Canada

During the 2011 Canadian General Election, eight citizens in six different electoral districts brought a case against several MPs, the Attorney General, and the Chief Electoral Officer based on an allegation of voter suppression. The complaints centred on misleading telephone calls received that provided incorrect polling station information. On that basis, the eight applicants called for the annulment of election results in their districts.

The Federal Court of Canada held that fraud had occurred during the election campaign, and that the telephone calls were made with the purpose of suppressing voters. However, the court also held that there was no evidence that the telephone calls were successful in suppressing votes and therefore could not be said to have determined the election. Neither was there any evidence that the respondent parties were involved in the commissioning of the fraudulent calls. As such, while there was a fraudulent attempt at voter suppression, it did not meet the threshold of annulment.¹²³

The advent of newer digital technologies amplifies the risk of voter suppression of the type found in *McEwing*. For example, actors may hack an official website or create a spoofed website that appears legitimate to spread false information regarding polling locations, or even fabricate electoral rules.¹²⁴ One notable instance occurred during the 2016 US Presidential election, when online messages falsely claimed that voters could cast their ballots online or via text message.¹²⁵

¹²⁰ *ibid* [134]-[135].

¹²¹ Samantha Bradshaw, Hannah Bailey and Philip N Howard, ‘Industrialised Disinformation: 2020 Global Inventory of Organized Social Media Manipulation’ (University of Oxford 2021) 2.

¹²² *McEwing v Canada* [2013] 433 FTR 59.

¹²³ *McEwing v Canada* [2013] 433 FTR 59 [244]-[249].

¹²⁴ Holly Garnett and Toby James, ‘Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity’ (2020) 19(2) Election Law Journal 111, 117.

¹²⁵ Chelsea Mihelich, ‘Prosecuting Vote Suppression by Misinformation’ (Columbia Law School 2019) <https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1007&context=public_integrity> accessed 18 December 2025.

The misinformation described above was particularly persuasive because it reflected broader trends towards the increased digitalisation of electoral processes. According to the International Institute for Democracy and Electoral Assistance, up to 50% of countries worldwide use some form of electronic voting technology, either to cast votes directly through voting machines or to count paper ballots electronically.¹²⁶ The trend towards electoral digitalisation is particularly evident in Estonia, which has incorporated internet voting into its electoral system. Between 41% and 51% of votes cast in Estonian elections since 2019 have been submitted online.¹²⁷ While Estonia's online voting system has been considered to be more secure than postal voting, concerns have nevertheless been raised that internet voting introduces additional vulnerabilities that could potentially be exploited by malicious actors.¹²⁸ The UK's National Cyber Security Centre stated that the use of paper ballots for voting in elections is beneficial precisely because it significantly reduces the risk of cyber threats.¹²⁹

In a separate development, during the 2025 Irish presidential election, a 'Spoil The Vote' campaign emerged online, promoted by a range of anti-establishment activists and commentators who challenged the legitimacy of the candidate selection process. 'Spoil The Vote' encouraged voters to purposely invalidate their votes for reasons such as the alleged illegitimacy of the candidate selection process.¹³⁰ While spoiling a ballot constitutes a legitimate exercise of an individual's right to vote, its systemic promotion by an online campaign represents a novel tactic by actors engaging in potentially malicious efforts to undermine the legitimacy of election results, through effectively negating cast votes.¹³¹

Cumulatively, these examples illustrate the range of risks to modern elections. Effective responses to misinformation and disinformation in relation to elections are therefore essential to safeguard fundamental democratic processes.

126 International IDEA, 'Use of E-Voting Around the World' (IDEA, 6 February 2023) <<https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world>> accessed 30 April 2026.

127 In the last four elections back to 2019, internet voting has accounted from 41% to 51% of cast votes. Valimised, 'Statistics about Internet voting in Estonia' (Valimised 2025) <<https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia>> accessed 15 April 2026.

128 Jelizaveta Vakariuk, Nikita Snetkov and Jan Willemson, 'Comparing Security Levels of Postal and Internet Voting' (2025) 34(4) Information Security Journal 265, 268.

129 National Cyber Security Centre (UK), *Annual Review 2023* (GCHQ 2023) 39.

130 Hope and Courage Collective and Institute for Strategic Dialogue, 'Irish Presidential Election 2025: Renewed Attacks on Election Integrity and Repeated Platform Failures' (Hope and Courage Collective, 31 October 2025) <<https://hopeandcourage.ie/irish-presidential-election-2025-renewed-attacks-on-election-integrity-and-repeated-platform-failures/>> accessed 18 December 2025.

131 Shane Raymond, 'As Ballots are Counted, Misleading Claims that the Election Was 'Rigged' Spread Online' (The Journal, 25 October 2025) <<https://www.thejournal.ie/misleading-posts-spoilthevote-election-rigged-illegitimate-rerun-low-turnout-factcheck-6855692-Oct2025/>> accessed 18 December 2025.

Combatting False Information

While the pace of regulatory development in response to misinformation and disinformation has attracted criticism,¹³² democratic societies have nevertheless adopted a range of increasingly sophisticated measures aimed at protecting electoral processes from online interference.¹³³ In 2011, Ireland established the National Cyber Security Centre (NCSC) in response to evolving threats to security.¹³⁴ NCSC is responsible for state cyber security measures, and in 2019 the Government highlighted misinformation and disinformation as cyber-related threats to election integrity.¹³⁵ The NCSC is also the National Competent Authority for the EU Network and Information Security Directive in Ireland.¹³⁶ Since 2015, the capacity of the NCSC has expanded in order to fulfil “the full range of cyber security incident response functions”,¹³⁷ with the number of staff increasing from 25 in 2021 to 70 by 2026.¹³⁸ The General Scheme of the National Cyber Security Bill 2024 has proposed to place the NCSC on a statutory footing.¹³⁹

Prior to the 2024 Irish General Election, the NCSC considered that there was a medium level of risk that the election would be targeted by online interference campaigns.¹⁴⁰ However, it also noted that, up to that point, the impact of such campaigns in the past had been low.

The need for vigilance on this front cannot be underestimated. The EU, in an effort to support Member States in safeguarding elections, established the European Cooperation Network on Elections (ECNE) in 2019 to help identify risks to elections and mechanisms to increase democratic resilience.¹⁴¹

Another approach to combatting online election interference has been in the promotion of traditional information sources. The EU Democracy Shield is the European Union’s policy framework for strengthening democratic resilience against threats such as foreign information manipulation and interference (FIMI), disinformation, hybrid threats, and attacks on electoral processes.¹⁴² It adopts a whole-of-society approach combining digital regulation, support for independent media, civil society engagement, public resilience

132 Simon Chesterman, ‘Lawful but Awful: Evolving Legislative Responses to Address Online Misinformation, Disinformation, and Mal-Information in the Age of Generative AI’ (2025) 72(4) *American Journal of Comparative Law* 933, 943-944.

133 Naja Bentzen, *Online Information Manipulation and Information Integrity: An Overview of Key Challenges, Actors and the EU’s Evolving Response* (European Parliamentary Research Service, September 2024) <https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762416/EPRS_BRI%282024%29762416_EN.pdf> accessed 19 January 2026.

134 Established by Government Decision in July 2011. Government of Ireland, *National Cyber Security Strategy 2019-2024* (Government of Ireland 2019) 19.

135 Government of Ireland, *National Cyber Security Strategy 2019-2024* (Government of Ireland 2019) 14-15.

136 National Cyber Security Centre, ‘Home Page’ (NCSC 2025) <<https://www.ncsc.gov.ie/>> accessed 15 April 2026.

137 Government of Ireland, *National Cyber Security Strategy 2019-2024* (Government of Ireland 2019) 20.

138 Department of Climate, Energy and the Environment, ‘Government agrees significant expansion of the National Cyber Security Centre’ (Government of Ireland 2025) <<https://www.gov.ie/en/department-of-climate-energy-and-the-environment/press-releases/government-agrees-significant-expansion-of-the-national-cyber-security-centre/>> accessed 15 April 2026.

139 Department of the Environment, Climate and Communications, General Scheme of the National Cyber Security Bill 2024 (30 August 2024) <<https://assets.gov.ie/static/documents/general-scheme-of-the-national-cyber-security-bill-2024.pdf>>

140 National Cyber Security Centre, ‘General Election 2024 Cyber Threat Landscape’ (Department for the Environment, Climate and Communications 2024).

141 European Commission, ‘European Cooperation Network on Elections’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en> accessed 24 July 2026; European Commission, ‘European Cooperation Network on Elections’ <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en> accessed 20 April 2026.

142 European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *European Democratic Shield: Empowering Strong and Resilient Democracies* (Joint Communication, 12 November 2025); Naja Bentzen, *The European Democracy Shield: An Overview* (European Parliamentary Research Service, January 2026) <<https://epthinktank.eu/2026/01/15/the-european-democracy-shield-an-overview/>> accessed 24 July 2026.

initiatives, and enhanced coordination between Member States and EU institutions.¹⁴³

Michael McGrath, EU Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection, stated that a significant focus of the EU Democracy Shield is on the promotion of trusted media to provide up-to-date and accurate information to inform the public.¹⁴⁴

Previously, broadcast moratoriums had been in place to preserve neutrality and give voters space to decide on their vote without being swayed in any particular direction. In 2013, guidelines by the Broadcasting Authority of Ireland, which at the time was responsible for the regulation of media, stated that media content within an election broadcast moratorium should not include:

“electioneering and/or references to issues linked to the General Election and/or references...to the merits or otherwise of an election candidate(s) and/or their policies shall not be broadcast while the moratorium is in operation.”¹⁴⁵

However, in 2024, Coimisiún na Meán, which replaced the Broadcasting Authority of Ireland with remit over media, abolished the broadcast moratorium on election coverage, instead requiring additional care with information. This was in part due to rising threats to election integrity.¹⁴⁶ Coimisiún na Meán recognised the need for trusted media sources, including traditional news media, in informing the public about the election.¹⁴⁷ This position is reflected by the Irish public, with a higher proportion of Irish citizens trusting the news than those of the US, UK and other European nations.¹⁴⁸ The rescinding of the broadcast moratorium in Ireland was in part based on the need to combat disinformation.¹⁴⁹

The promotion of trusted information sources has therefore become an increasingly important component of modern election integrity strategies. Alongside content moderation and regulatory oversight, policymakers have sought to strengthen democratic resilience by improving public access to reliable and verifiable information.

143 Naja Bentzen, 'The European Democracy Shield: An Overview' (European Parliamentary Research Service, January 2026) 1.

144 Michael McGrath, remarks on the European Democracy Shield, European Committee of the Regions, 'EU's "Democracy Shield" Needs Local Action Against Disinformation and Hate Speech' (10 December 2025) <<https://www.cor.europa.eu/en/news/eus-democracy-shield-needs-local-action-against-disinformation-and-hate-speech>> accessed 24 July 2026.

145 Broadcasting Authority of Ireland, Code of Fairness, Objectivity & Impartiality in News and Current Affairs (April 2013).

146 Coimisiún na Meán, 'Coimisiún na Meán removes traditional broadcast moratorium for election coverage' (1 November 2024) <<https://www.cnam.ie/coimisiun-na-mean-removes-traditional-broadcast-moratorium-for-election-coverage/>> accessed 9 December 2025.

147 *ibid.*

148 Coimisiún na Meán, *Digital News Report Ireland 2025* (Coimisiún na Meán 2025) 11.

149 Coimisiún na Meán's Broadcasting and Video-on-Demand Commissioner Aoife MacEvilly in Coimisiún na Meán, 'Coimisiún na Meán removes traditional broadcast moratorium for election coverage' (1 November 2024) <<https://www.cnam.ie/coimisiun-na-mean-removes-traditional-broadcast-moratorium-for-election-coverage/>> accessed 15 April 2026.

Balancing Election Integrity and Freedom of Expression

A significant proportion of Irish citizens (47% in 2025) now obtain their news from social media.¹⁵⁰ Broadcast media are regulated by the Broadcasting Act 2009, which, amongst other things, prevents broadcasters from undermining the authority of the State or giving unfair preference to any given political party.¹⁵¹ Social media, particularly when individuals post their own opinions and views to a large audience, circumvent these regulations. As a result, regulating online behaviour becomes particularly challenging because individuals can engage in forms of political communication that would breach broadcast regulations if those rules applied to them. Efforts to restrict such activity must also be balanced against the fundamental right to freedom of expression, making regulatory intervention more complex.

This tension between protecting the individual's freedom of expression and regulating online political discourse to preserve the integrity of electoral processes has been considered by the European Court of Human Rights.

*Case: Brzeziński v Poland*¹⁵²

In the case of *Brzeziński v Poland*, the applicant was a local election candidate who produced a booklet that criticised the incumbent local government. The booklet had been shared widely among the applicant's community. The local mayor had been granted an injunction against the applicant by the local Regional Court, which required the applicant to cease sharing the booklet and to correct any untrue statements contained therein.¹⁵³ The case against *Brzeziński* was then upheld at Katowice Court of Appeal.¹⁵⁴

The applicant claimed that the order violated his freedom of expression as guaranteed by Article 10 of the European Convention on Human Rights and appealed to the European Court of Human Rights. The applicant also argued that, while his statements had been critical, they had a factual basis.

At the European Court of Human Rights, it was held that, while Poland had a legitimate aim in following electoral law and protecting the reputation of election candidates, their margin of appreciation for violating the applicant's freedom of expression was limited. The Court found that, as the applicant was himself a candidate in the local election and had been engaging in political debate that was neither deceitful nor vulgar, Poland had disproportionately interfered with the applicant's Article 10 rights.¹⁵⁵

150 Coimisiún na Meán, *Digital News Report Ireland 2025* (Coimisiún na Meán 2025) 24.

151 Broadcasting Act 2009, ss 46J and 46L.

152 *Brzeziński v Poland* App no 47542/07 (ECtHR, 2019).

153 Original judgment in French, *Brzeziński v Poland* App no 47542/07 (ECtHR, 2019). Ronan Ó Fathaigh, 'Brzeziński v. Poland: Fine over 'false' information during election campaign violated Article 10' (Strasbourg Observers, 8 August 2019) <https://pure.uva.nl/ws/files/42454460/Brzezi_ski_v.pdf> accessed 9 December 2025.

154 *ibid.*

155 *ibid.*

The weight placed by the European Court of Human Rights on the Article 10 freedom of expression poses a significant counterbalance to regulatory efforts to combat misinformation and disinformation. In Ireland, the Electoral Reform Act 2022 recognises the safeguards of Article 10 rights and acknowledges the rights of freedom of expression; freedom of association; participation in public affairs; and the obligation of the State to secure the fairness of elections as considerations in the exercise of its powers.¹⁵⁶

However, critics have argued that there is little guidance in respect of how An Coimisiún Toghcháin should balance the right to freedom of expression and its objective of preserving free and fair elections.¹⁵⁷ The EU has provided a Code of Practice on issues relating to disinformation, which cautions Member States from overreaching in efforts to preserve election integrity such that it infringes a right to an opinion.¹⁵⁸ There is a danger that malicious actors seeking to undermine integrity may invoke the freedom of expression to circumvent policy designed to prevent disinformation. These competing considerations are illustrated by the European Court of Human Rights' decision in *Salov v Ukraine*.¹⁵⁹

Case: Salov v Ukraine

The *Salov v Ukraine* case involved the applicant publishing a false newspaper editorial suggesting that the President of Ukraine was an imposter, and that the real President had died. Ukrainian authorities had arrested the applicant but could not identify a criminal offence that had been committed. The applicant therefore challenged the legality of his detention to the European Court of Human Rights, as well as the absence of a fair trial.

Similarly to the case of *Brzeziński*, the Court recognised the legitimate aim of Ukrainian authorities in terms of preserving fair democratic processes by verifying public information. However, the extent to which a Council of Europe Member State may restrict an individual's right to freedom of expression is limited. Additionally, in this particular case the impact of the false information had been limited, as only eight copies of the falsified newspaper had been made. Without direct evidence of whether the applicant had a motive to deceive, or had simply been reiterating rumours he had heard, the Court held that the applicant's right to freedom of expression under Article 10 had been violated.

The cases of *Brzeziński* and *Salov* suggest that the European Court of Human Rights will afford significant protection to political expression under Article 10, including expression in an electoral context that is alleged to be false or misleading.

Academic commentators have argued that restrictions on media content are not justified unless the intent to deceive is apparent.¹⁶⁰ The case of *Salov*, in particular, highlights the

¹⁵⁶ Electoral Reform Act 2022, s152.

¹⁵⁷ Ethan Shattock, 'Knowledge, deception, and freedom of expression: a critical examination of Ireland's approach to disinformation under the Electoral Reform Act 2022' (2025) 39(3) *International Review of Law, Computers and Technology* 344, 350.

¹⁵⁸ Directorate-General for Communications Networks, Content and Technology (European Commission), Code of Conduct on Disinformation (Publications Office of the European Union, 2025) 8.

¹⁵⁹ *Salov v Ukraine* App no 65518/01 (ECtHR, 2005).

¹⁶⁰ Ethan Shattock, 'Knowledge, deception, and freedom of expression: a critical examination of Ireland's approach to disinformation under the Electoral Reform Act 2022' (2025) 39(3) *International Review of Law, Computers and Technology* 344, 366.

need for intent to be established before assessing the proportionality of state interference in the freedom of expression.

The ubiquity of contemporary online content creators underscores the contrast between the digital landscape of today and that of the early 2000s, when *Brzeziński* and *Salov* were decided. The broad reach of digital media, as opposed to traditional newsletters or local publications, means that any restrictions placed on false information are necessarily broader and wider reaching. While in *Salov* the Court found that the impact of the false information on voters had been minimal,¹⁶¹ the same may not be true of a social media influencer or account with thousands or millions of followers. It is plausible that an actor, or foreign state, could resource a disinformation campaign that would have such an impact as to dominate the news surrounding an election, which would have a detrimental impact on election integrity.¹⁶²

An example of social media's impact on elections can be seen in the 2025 Irish Presidential Election, which was targeted by an online campaign encouraging voters to spoil their ballots. In Ireland's 2019 local elections, the approximately 2% of invalid votes cast were primarily caused by improperly completed ballots, with few voters deliberately spoiling their ballots.¹⁶³ This is in direct contrast to the 2025 Presidential Election, in which almost 13% of votes were spoiled, amid claims that online personalities had encouraged voters to spoil their ballots,¹⁶⁴ though the degree to which this contributed to the overall spoilage rate remains uncertain.

The European Digital Media Observatory (EDMO) suggested that some online content creators in Ireland, who were prominent in the 'Spoil The Vote' movement during the Presidential Election, were previously known to violate moderation policies on misinformation.¹⁶⁵

161 Michael Schmitt, 'Foreign Cyber Interference in Elections' (2021) 97 International Law Studies 739, 748.

162 *Salov v Ukraine* App no 65518/01 (ECtHR, 2005).

163 An Coimisiún Toghcháin, 'Let's Have No Repeat of 100,000+ Spoilt Votes in June's Euro & Local Elections' (27 May 2024) <<https://www.electoralcommission.ie/latest-news-and-research/lets-have-no-repeat-of-100000-spoilt-votes-in-junes-euro-amp-local-elections/>> accessed 6 January 2026.

164 Sandra Hurley, 'Deeper reflection' needed after record spoiled votes' (RTÉ News, 25 October 2025) <<https://www.rte.ie/news/presidential-election/2025/1025/1540504-president-ireland-vote/>> accessed 28 July 2026; Jack McCarron and Kate McDonald, 'Who was behind the 'Spoil The Vote' campaign?' (RTÉ News, 25 October 2025) <<https://www.rte.ie/news/primetime/2025/1025/1540566-who-was-behind-the-spoil-the-vote-campaign/>> accessed 6 January 2026.

165 EDMO Ireland, 'Platforms Failing on Electoral Integrity: EDMO Ireland's Initial Findings' (European Digital Media Observatory, 25 October 2025) <<https://edmo.ie/index.php/platforms-failing-on-electoral-integrity-edmo-irelands-initial-findings/>> accessed 15 April 2026.

Interference Targeting Electoral Candidates

Although the growing use of online technologies, particularly social media, has allowed electoral candidates to engage with constituents more effectively than before, it simultaneously exposes them to critics and malicious actors. Coimisiún na Meán found that, in the local and general elections in 2024, 67% of candidates were worried about the threat of negative online behaviour.¹⁶⁶ As a result, 60% of candidates in some way mitigated or reduced their campaigning, in response to (the threat of) negative online behaviour.

AI deepfakes have been used to target female political candidates in Ireland and across Europe by portraying and disseminating generated pornographic imagery of them to cause harm to them.¹⁶⁷ The use of false AI images provides malicious actors with an additional mechanism to attack and harass political candidates in the online sphere. False, digitally created media have a direct impact on candidates' right to freedom of expression, right to participate in public affairs, and the State's election integrity, through deterring prospective candidates or narrowing of their platforms to avoid controversial topics.

The significance of these findings extends beyond the individual candidates affected. When intimidation, harassment, and coordinated disinformation campaigns discourage participation in elections, they can reduce the diversity of candidates willing to seek public office and weaken representative democracy.¹⁶⁸ The protection of candidates from serious online harms should therefore be viewed as an election integrity issue as well as an issue of individual safety and wellbeing.¹⁶⁹

The various mechanisms through which digital technologies can facilitate the spread of disinformation and undermine election integrity present a significant challenge for states and institutions. EU Member States are required to uphold individual rights, including the freedom of expression. However, those same rights can be exploited by malicious actors as a shield against effective regulation. The following chapter examines the current legal framework in the EU and Ireland and assesses how effective it is in addressing these challenges.

¹⁶⁶ Coimisiún na Meán, 'On the Digital Campaign Trail: Election Candidates' Online Experiences in the 2024 Elections' (2025) <https://www.cnam.ie/app/uploads/2025/08/CnaM_On-the-digital-campaign-trail.pdf> accessed 17 December 2025.

¹⁶⁷ Examples discussed in Ellen Coyne and Marie O'Halloran, 'Gráinne Seoige calls on Government to pass law criminalising AI-generated fake nude images' (The Irish Times, 13 January 2026) <<https://www.irishtimes.com/politics/2026/01/13/grainne-seoige-calls-on-government-to-pass-law-criminalising-ai-generated-fake-nude-images/>> accessed 16 April 2026.

¹⁶⁸ OSCE Office for Democratic Institutions and Human Rights (ODIHR), *Addressing Violence against Women in Politics in the OSCE Region: Toolkit* (OSCE 2022).

¹⁶⁹ UNDP and Inter-Parliamentary Union, *Addressing Violence Against Women in Politics: Institutional Responses and Good Practices by Parliaments* (UNDP and IPU 2026).

Legal and Regulatory Framework



Legal and Regulatory Framework

Ireland's legal framework governing election integrity has developed incrementally, combining long-standing rules on political finance with more recent institutional and digital regulatory reforms. Within this evolving framework, the principal legislative instruments governing election integrity and online election interference are the Electoral Reform Act 2022 and the Digital Services Act 2024. The Digital Services Act 2024 gives domestic effect to Regulation (EU) 2022/2065 on a Single Market for Digital Services, commonly referred to as the Digital Services Act (DSA).

This framework can be understood as comprising three interrelated elements: legacy regulation of political finance, more recent institutional reform, and emerging digital regulation.

The Electoral Act 1997

While recent reforms have focused on the regulation of online platforms and digital political advertising, Ireland's legal framework governing elections also includes long-standing legislation addressing political finance, most notably the Electoral Act 1997 (the 1997 Act). The 1997 Act remains a central component of the legal framework regulating elections, particularly in respect of campaign expenditure and political donations.

The 1997 Act established limits on election spending by candidates and political parties, as well as detailed rules governing the acceptance, disclosure, and reporting of political donations. It also introduced transparency requirements through obligations to furnish statements of election expenses and donations, which are subject to oversight by the Standards in Public Office Commission (SIPO). These mechanisms were intended to preserve the principle of electoral fairness by limiting the extent to which financial resources can influence electoral outcomes.

Although the 1997 Act provides an important baseline for regulating political finance, the regulatory model underpinning it was developed in a pre-digital era, where campaign expenditure and political messaging were more readily identifiable and attributable. In contemporary digital environments, however, political content can be disseminated rapidly through decentralised networks, informal actors, and opaque funding structures that may fall outside the scope of traditional campaign finance rules. As a result, the distinction between regulated political advertising and broader political communication becomes increasingly blurred. For example, the use of social media influencers, coordinated networks of user accounts, or indirectly funded content may circumvent the spending thresholds and disclosure requirements provided for in the 1997 Act.

These structural limitations are also reflected in the role of the Standards in Public Office Commission (SIPO), which is responsible for overseeing compliance with rules governing political donations, election expenditure, and financial disclosures by political parties and candidates. While SIPO provides robust oversight of formal financial flows within electoral

politics, its remit is grounded in the same traditional model of political engagement. Consequently, it is less equipped to monitor or regulate newer forms of influence that arise in digital environments. In particular, the indirect promotion of political messages through online networks, third-party content creators, or foreign-backed disinformation campaigns may fall outside SIPO's traditional supervisory scope.

SIPO's role in ensuring financial transparency in elections remains important, even as the mechanisms of influence evolve. A modernised approach to safeguarding election integrity may therefore require closer coordination between SIPO and bodies such as Coimisiún na Meán and An Coimisiún Toghcháin, which are increasingly focused on online harms and false information, to address the intersection between political finance and digital campaigning.

The Electoral Reform Act 2022

Prior to the enactment of the Electoral Reform Act 2022 (the 2022 Act), Ireland's electoral system was criticised as falling short of international practice, owing to its regulation being fragmented across a "clutch of different agencies".¹⁷⁰ Progress towards meaningful electoral reform was regarded as being impeded by the absence of a single body with overarching responsibility for electoral policy and administration.¹⁷¹

A significant step towards addressing this issue was taken with the enactment of the 2022 Act, the majority of which had been commenced by November 2024. It introduced several important changes to safeguard elections. The most significant reforms provided for in the 2022 Act include:

- The establishment of An Coimisiún Toghcháin (the Electoral Commission), Ireland's first statutory, independent Electoral Commission, bringing together a range of previously dispersed electoral functions and providing central oversight of the electoral system;
- The modernisation of the Electoral Register;
- The regulation of online political advertising;
- Measures to protect election integrity;
- Provisions for elections during public health emergencies;
- Island voting reforms; and,
- Strengthened provisions on political donations and political party accounting.

In the period leading up to the enactment of the 2022 Act, a central concern was the growing prevalence of electoral misinformation and disinformation online.¹⁷² Fake accounts frequently circulate unverifiable political content without identifying either the source of the material or the identity of the account holder.¹⁷³ The spread of false political information has the potential to influence voting patterns and threaten the integrity of elections, as

170 David Farrell, 'Conclusion and Reflection: Time for an Electoral Commission for Ireland' (2015) 30(4) Irish Political Studies 641, 642.

171 n 11, 448.

172 Deputy Malcolm Noonan in Dáil Deb 13 July 2022, vol 1024, col 614.

173 Stephen McDermott 'The disinfluencers: How over 150 anonymous 'Irish' accounts are swamping X with extreme views' (theJournal.ie 27 May 2024) <<https://www.factchecking.ie/articles/the-disinfluencers-how-over-150-anonymous-irish-accounts-are-swamping-x-with-extreme-views>> accessed 16 April 2026.

previously discussed in this Paper (for example, in *McEwing v Canada*). Indeed, concerns regarding misleading electoral propaganda during the 2016 US presidential election and during the UK's referendum on EU membership were explicitly discussed during the legislative scrutiny of the 2022 Act.¹⁷⁴

The 2022 Act regulates electoral information by:

- Requiring online platforms to identify adverts that are political in nature;
- Requiring online platforms to verify the creators of online political adverts;
- Placing duties on An Coimisiún Toghcháin to monitor, investigate, and combat disinformation and misinformation campaigns; and
- Empowering An Coimisiún Toghcháin to issue access-blocking, labelling, correction, or take-down notices on identified sources of disinformation

Part 4 of the 2022 Act directly relates to maintaining election integrity by regulating electoral advertising. Section 125 of the 2022 Act restricts actors outside the State from displaying, promoting, or disseminating any online political advertisement relating to Irish elections or elections to the European Parliament. Additional provisions place statutory obligations on online platforms to verify both the source of political advertisements and the veracity of the statements made therein.¹⁷⁵

If commenced, Part 5 of the 2022 Act would deal with misinformation and disinformation by providing for definitions of each type of material. Disinformation would be defined by section 144 as 'false or misleading' information which may cause public harm and is intended to deceive. Part 5 would specifically address the regulation of online information in light of the growing use of disinformation to undermine electoral processes.

In response to the risk of misleading political advertising and disinformation in advance of the General Election 2024 and Presidential Election 2025, An Coimisiún Toghcháin prepared a *Framework on Online Electoral Process Information, Political Advertising and Deceptive AI*. The Framework sets out best-practice principles for online platforms and political parties, operating in tandem with the Electoral Reform Act 2022.¹⁷⁶ For example, it requires political advertisements to be labelled for transparency. The Framework also provides that platforms and candidates should mitigate against any misinformation or disinformation, and that they should highlight and remove deceptive AI-generated video/audio content.¹⁷⁷

Part 5 of the 2022 Act, which empowers An Coimisiún Toghcháin to monitor and investigate disinformation and regulate political advertising, has not yet been commenced, however. Part 4 of the Act was repealed by and replaced with the European Union (Political Advertising) Regulations 2025 (S.I. No. 474 of 2025) (the 2025 Regulations) on 10 October 2025. The 2025 Regulations are discussed in further detail below.

¹⁷⁴ Eoin Ó Bróin, Dáil Deb 13 July 2022, vol 1025, col 4.

¹⁷⁵ Electoral Reform Act 2022, s123.

¹⁷⁶ An Coimisiún Toghcháin, *Framework on Online Electoral Process Information, Political Advertising and Deceptive AI Content 2024* (2024) <<https://cdn.electoralcommission.ie/app/uploads/2024/11/08143237/Framework-on-Online-Electoral-Process-Information-Political-Advertising-and-Deceptive-AI-content-Nov24.pdf>> accessed 6 January 2026.

¹⁷⁷ *ibid* 5.

Online Safety and Media Regulation Act 2022

The objectives of the Online Safety and Media Regulation Act 2022 (the 2022 Act) were to establish Coimisiún na Meán (the Media Commission); dissolve its predecessor, the Broadcasting Authority of Ireland; implement Directive 2010/13/EU as amended by Directive (EU) 2018/1808 (the Audiovisual Media Services Directive); and update the broadcasting and audiovisual regulatory framework.¹⁷⁸

The 2022 Act expanded the Irish media regulatory framework by conferring on Coimisiún na Meán functions relating to online safety and online media services in addition to the broadcasting functions formerly exercised by the Broadcasting Authority of Ireland. Section 45 empowers Coimisiún na Meán to designate online services to which online safety codes apply, and a register of those services is published on the commission's website.¹⁷⁹ The 2022 Act also enables Coimisiún na Meán to investigate persons and platforms for publishing harmful content.¹⁸⁰ In addition, the 2022 Act creates offences for publishing or broadcasting various categories of harmful content online.¹⁸¹

While harmful online content is not necessarily the same as false information or digital election interference, it does provide Coimisiún na Meán with overarching powers to regulate online behaviour. These regulatory, investigative, and prosecutorial powers have since been expanded upon by the Digital Services Act 2024.



Monitoring Election Analytics on Computer. (Image: Shutterstock)

178 Government of Ireland, 'Online Safety and Media Regulation Bill 2022 Explanatory and Financial Memorandum' (2022) <<https://data.oireachtas.ie/ie/oireachtas/bill/2022/6/eng/memo/b0622s-memo.pdf>> accessed 19 January 2026.

179 Online Safety and Media Regulation Act 2022 s 45; Coimisiún na Meán, 'Register of Designated Online Services' (12 September 2025) <<https://www.cnam.ie/industry-and-professionals/online-safety-framework/online-safety-code/register-of-designated-online-services/>> accessed 15 May 2026.

180 Online Safety and Media Regulation Act 2022, s 47.

181 Online Safety and Media Regulation Act 2022, s 46.

The Digital Services Act

The European Union adopted the Digital Services Act (Regulation (EU) 2022/2065) (the DSA) to establish a single, harmonised legislative framework for online and digital services across the EU.¹⁸² The DSA marked a shift from relying on ‘soft law’ instruments – such as the Code of Conduct on Countering Illegal Hate Speech Online – towards a binding regulatory framework governing the dissemination of illegal and harmful content online.

The Code of Conduct on Countering Illegal Hate Speech Online

The Code of Conduct was a shared commitment by the European Commission alongside Facebook, Microsoft, Twitter and YouTube to promote freedom of expression while tackling rising hate speech online.¹⁸³ In 2019, the European Commission reported that the Code of Conduct enhanced transparency among signatory online platforms in how they enforce hate speech standards.¹⁸⁴ The Code of Conduct was also found to have facilitated improved dialogue between online platforms and EU institutions regarding responses to disinformation.¹⁸⁵ However, the Commission also reported that implementation of the Code had been uneven.¹⁸⁶

The level of compliance with the Code of Conduct, as reflected in the removal of flagged illegal content within 24 hours, decreased significantly in the period following its publication, reducing from 90.4% in 2020 to 63.3% in 2022.¹⁸⁷ The European Union Agency for Fundamental Rights identified declining levels of compliance as a key challenge, observing that illegal content remained accessible online for longer periods. Combined with the fact that instances of hate speech and online abuse tend to increase in the periods leading up to elections, the reduction in the level of enforcement was a substantial concern.¹⁸⁸ In response, the European Commission in 2019 stated that if the results of the Code had not proved satisfactory by 2020, then it may propose another regulatory approach.¹⁸⁹

Regulation (EU) 2022/2065: The Digital Services Act

The Digital Services Act (the DSA) creates a regulatory framework aimed at ensuring a safe and accountable online environment. It establishes a system of oversight over online services based on a nested hierarchy of service categories, with obligations increasing according to the nature, size, and societal impact of the service concerned. At its foundation, the DSA regulates intermediary services, comprising mere conduit, caching, and hosting services. Additional obligations apply to specific subsets of those services, including online platforms, online platforms that enable consumers to conclude distance

¹⁸² European Commission, ‘Explanatory Memorandum supplementing Regulation (EU) 2022/2065’ (European Union 2022).

¹⁸³ European Commission, *Code of Conduct on Countering Illegal Hate Speech Online* (European Commission 30 June 2016).

¹⁸⁴ European Commission, ‘Assessment of the Code of Conduct on Hate Speech Online: State of Play’ (27 September 2019) 5.

¹⁸⁵ European Commission, ‘Code of Practice on Disinformation One Year On: Online Platforms Submit Self-Assessment Reports’ (European Union, 29 October 2019) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_19_6166/STATEMENT_19_6166_EN.pdf> accessed 17 December 2025.

¹⁸⁶ *ibid.*

¹⁸⁷ European Union Agency for Fundamental Rights, *Online Content Moderation – Current Challenges in Detecting Hate Speech* (29 November 2023) 24.

¹⁸⁸ European Union Agency for Fundamental Rights, *Online Content Moderation – Current Challenges in Detecting Hate Speech* (29 November 2023) 88.

¹⁸⁹ European Commission, ‘Code of Practice on Disinformation One Year On: Online Platforms Submit Self-Assessment Reports’ (European Union 29 October 2019) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/statement_19_6166/STATEMENT_19_6166_EN.pdf> accessed 17 December 2025.

contracts with traders, and, at the highest tier, very large online platforms (VLOPs) and very large online search engines (VLOSEs), which are subject to enhanced obligations reflecting their scale, potential societal impact and capacity to generate systemic risks.¹⁹⁰

The primary goals of the DSA are to prevent illegal activities, combat disinformation, protect consumer rights, and promote a transparent and fair digital space.¹⁹¹ One risk associated with the proliferation of online information identified by the European Parliament was the increased vulnerability of democratic and electoral processes to attack, which the DSA sought to address by establishing clear response mechanisms for online platforms.¹⁹²

The DSA imposes a range of obligations on online platforms, including an obligation to provide mechanisms to remove illegal content, to provide redress mechanisms for users, to publish transparency reports, to act on complaints in a timely fashion, and to ensure the safety and privacy of children on their platform.

The DSA applies to a wide range of digital service providers, although the obligations imposed by the Regulation vary considerably according to the size and nature of the service concerned. VLOPs and VLOSEs have additional obligations, including to publish their user numbers every six months, conduct annual risk assessments including a review of moderation systems, establish internal compliance procedures, and maintain repositories of all advertisements posted on their platforms.¹⁹³

The European Commission stated that the DSA has a broad range of benefits for both citizens and businesses. For citizens, the DSA improves transparency, supports the labelling and removal of illegal content, and promotes the status of verified sources of information and sellers to increase online safety.¹⁹⁴ For businesses, the DSA is intended to provide a holistic approach towards the regulation of online services, improve the reporting of illegal content, provide for central (non-court) dispute resolution, and enhance online commerce transparency through requiring sellers to list their contact information.¹⁹⁵

Micro and small digital enterprises are excluded from many of the obligations under the DSA, such as the requirement to collect contact information from sellers (Article 30) or the requirement to handle complaints in a timely manner (Article 20).¹⁹⁶ On the other hand, the DSA empowers the European Commission to designate large online services above a defined size as VLOPs or VLOSEs and creates enhanced supervisory powers over these services.¹⁹⁷ The designations of VLOPs and VLOSEs cover online shopping services (e.g., Amazon and AliExpress), social media platforms (e.g., Facebook, LinkedIn, TikTok, and X), service platforms (e.g., Booking.com), and application stores (e.g., Google Play, App Store).¹⁹⁸

190 Regulation (EU) 2022/2065 (Digital Services Act), arts 3 and 33-43.

191 European Commission, 'The Digital Services Act' (22 August 2025) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 11 November 2025.

192 Costica Dumbrava, *Key social media risks to democracy* (European Parliamentary Research Service, 2021); and Regulation 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 (Digital Services Act) [2022] OJ L 277/1, recital 83.

193 Digital Services Act, arts 32-43.

194 European Commission, 'The Digital Services Act' (22 August 2025) <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 11 November 2025.

195 European Commission, 'The Digital Services Act' (European Commission 18 May 2025) <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>> accessed 19 May 2026.

196 Unless said micro or small enterprises are also classified as a VLOP: Digital Services Act, art 19(2).

197 Regulation (EU) 2022/2065, art 33.

198 Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (ACM Conference on Fairness, Accountability and Transparency, Rio de Janeiro, June 2024).

Early litigation under the DSA mainly consisted of challenges by online platforms to their designation as VLOPs or VLOSEs. In *Zalando SE*, the principal issue concerned the methodology used to calculate user numbers for the purposes of VLOP designation.

*Example: Zalando SE v European Commission*¹⁹⁹

In the case of *Zalando SE v European Commission*, the applicant, an online retail platform based in Germany, challenged its designation as a VLOP by the European Commission. The applicant argued that Zalando operates two distinct services on its platform: its own online retail service, which is not an intermediary service, and an online marketplace enabling third-party sellers to transact via the website. On that basis, the applicant contended that the user base of the third-party marketplace alone did not exceed the minimum threshold required for designation as a VLOP.

The General Court of the Court of Justice of the European Union (CJEU) held that, because it was difficult to distinguish between items sold by Zalando itself and those offered by third-party sellers (which were listed side by side on the platform), the entire user base of the website had to be taken into account. Consequently, with 83 million users, Zalando's platform qualified as a VLOP.

The supervisory role over VLOPs and VLOSEs is a shared regulatory model where the European Commission has powers to enforce the DSA with the support of organisations designated by national governments as Digital Services Coordinators.²⁰⁰ Under the DSA, the Commission has direct investigative and enforcement powers over VLOPs and VLOSEs, enabling it to initiate investigations ex officio where it suspects infringements, and to make use of tools such as requests for information, interviews, on-site inspections, and access to platforms' data and internal systems. In respect of enforcement mechanisms, non-compliance with the DSA may result in fines of up to 6% of a provider's global annual turnover.²⁰¹ Interim measures can also be utilised to address urgent risks. Additionally, the Commission can impose periodic penalties and, in extreme cases, request temporary service suspensions.²⁰²

In addition to its supervisory and enforcement framework, the DSA imposes extensive transparency obligations in relation to content moderation decisions.

As part of the DSA's transparency framework, Article 17 requires providers of hosting services to provide a statement of reasons where they impose restrictions on content or on a recipient's account because they consider content posted by that recipient to be illegal or incompatible with the provider's terms and conditions. Article 24(5) further requires online platform providers to submit those decisions and statements of reasons to the European Commission for inclusion in a publicly accessible and machine-readable database maintained by the Commission.

¹⁹⁹ Case T-348/23 *Zalando SE v European Commission* (General Court, 2025).

²⁰⁰ Regulation (EU) 2022/2065, arts 64-83.

²⁰¹ Regulation (EU) 2022/2065, art 52(3).

²⁰² Regulation (EU) 2022/2065, art 23.

The operation and proportionality of the enhanced obligations imposed on designated VLOPs have been considered by the General Court in *Amazon EU Sàrl v European Commission*.

*Case example: Amazon EU Sàrl v European Commission Case T-367/23*²⁰³

In this case, the applicant, Amazon EU Sàrl (Amazon), challenged the obligations imposed on it arising from its designation as a VLOP by the European Commission.

Amazon argued that, while the objective purpose of preventing illegal content (including false or misleading content relating to elections) was legitimate, the obligations on it by the DSA infringed its freedom to conduct a business under Article 16 of the EU Charter of Fundamental Rights. Amazon contended that the objectives could have been achieved through less intrusive means, and that the obligations imposed therefore constituted a disproportionate interference with its business activities.

While the General Court of the CJEU acknowledged that designation as a VLOP entails an interference with the freedom to conduct a business under Article 16 of the Charter, it held that this interference is provided for by law, pursues legitimate objectives of general interest, and does not constitute a manifestly disproportionate means of achieving the objectives of the DSA.

The Court endorsed the legislature's choice to use a quantitative threshold (45 million average monthly active recipients) as a proxy for scale, societal reach, and the capacity to amplify systemic risks (including exposure to illegal content). The Court expressly rejected Amazon's argument that marketplaces are structurally incapable of generating systemic risks, emphasising that large marketplaces can concentrate consumers and traders, facilitate largescale dissemination of illegal products or content, and therefore justify heightened regulatory scrutiny.

The establishment of national Digital Services Coordinators (DSCs) forms part of the DSA's decentralised enforcement framework, enabling national authorities to supervise compliance and exercise investigatory powers, while supporting a complementary system in which the Commission exercises exclusive supervisory authority over key obligations applying to VLOPs and VLOSEs. DSCs are also responsible for granting trusted flagger status to eligible entities. Trusted flaggers are organisations with recognised expertise in identifying illegal content and notices submitted by them must be prioritised by online platforms under Article 22 of the DSA. Article 22 also sets out trusted flaggers' obligations, which include the requirement to publish annual reports on their activities.²⁰⁴

In advance of the European Parliament elections in 2024, the European Commission adopted guidelines under the DSA to assist VLOPs in mitigating systemic risks to electoral processes, thereby supporting compliance with Articles 34 and 35 of the DSA and the protection of democratic processes and public discourse.²⁰⁵

²⁰³ Case T-367/23 *Amazon EU Sàrl v European Commission* (General Court, 2025).

²⁰⁴ Regulation (EU) 2022/2065, art 23.

²⁰⁵ European 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' (Communication) COM C/2024/3014.

Under the DSA, VLOPs and VLOSEs are required to mitigate systemic risks, including negative effects on public discourse and electoral processes. To support compliance with these obligations, the Commission's election guidelines recommend that platforms tailor risk mitigation measures to local contexts and cooperate with independent experts and relevant stakeholders to strengthen election-related content governance, including in areas such as disinformation and hate speech. The guidelines apply throughout all stages of elections and are relevant to national, regional, local, and European Parliament elections.

To prepare for elections, the guidelines recommend that platforms should set up a dedicated internal team before each election period.²⁰⁶ This team should be appropriately staffed based on the risks identified and should include experts in areas such as content moderation, fact-checking, cybersecurity, and disinformation. Platforms should clearly define in their terms and conditions the timeframe during which these special measures and resources will be in place.

Although many of the obligations discussed above apply specifically to VLOPs and VLOSEs, Article 25 of the DSA imposes a separate obligation on providers of online platforms generally to ensure that their online interfaces do not deceive, manipulate, or otherwise materially distort users' ability to make free and informed decisions. The European Commission's investigation into X was initiated on the basis of suspected non-compliance with Article 25.

Example: European Commission investigation into X

In December 2025, the European Commission adopted a non-compliance decision against X (formerly Twitter) under the DSA, finding that the platform's 'verified' (blue checkmark) function breached DSA transparency obligations. The Commission concluded that, because the 'verified' status could be obtained through payment without any meaningful verification of its user's identity, its design was deceptive. According to the Commission, this deception exposed users to risks including "impersonation frauds" and "other forms of manipulation by malicious actors".²⁰⁷

The Commission described this as the first non-compliance decision adopted under the DSA. It imposed a fine of €120 million on X and required X to adopt specific remedial measures to bring an end to the deceptive practice and ensure compliance with the DSA.²⁰⁸

Broader content and AI investigations into X by the European Commission are ongoing. However, in July 2026, the Commission accepted a formal action plan from X to resolve the transparency failures that led to the original €120 million fine.²⁰⁹ Under this legally binding plan, X is under an enhanced supervision regime to overhaul its advertising registry, grant data access to eligible researchers, and formally allow data scraping for academic purposes.²¹⁰

²⁰⁶ *ibid* para 22.

²⁰⁷ European Commission, 'Commission fines X €120 million under the Digital Services Act' (5 December 2025) <http://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934> accessed 15 December 2025.

²⁰⁸ *ibid*.

²⁰⁹ European Commission, 'Commission accepts X's action plan to comply with Digital Services Act' (16 July 2026) <<https://digital-strategy.ec.europa.eu/en/news/commission-accepts-xs-action-plan-comply-digital-services-act>> accessed 28 July 2026.

²¹⁰ European Commission, 'Commission accepts X's action plan to comply with Digital Services Act' (16 July 2026) <<https://digital-strategy.ec.europa.eu/en/news/commission-accepts-xs-action-plan-comply-digital-services-act>> accessed 28 July 2026.

The Commission’s decision against X (the first non-compliance decision under the DSA) exemplifies the DSA’s hybrid governance model. This model combines platformled risk assessment with centralised public enforcement, rather than creating a system of enforced selfregulation. Under the DSA’s model of riskbased regulation, platforms retain discretion over service design but are subject to ex-post scrutiny and enforcement by the Commission where those design choices infringe statutory obligations.²¹¹ The DSA requires VLOPs and VLOSEs to have appropriate risk assessments, a “crisis response mechanism” to deal with threats to either “public security or public health”, and independent audits of the online platforms’ compliance with the Regulation.²¹²



European Parliament in Brussels, Belgium. (Image: Shutterstock)

211 Marie-Therese Sekwenz and Rita Gsenger, ‘The Digital Services Act: Online Risks, Transparency and Data Access’ in Rita Gsenger and Marie-Therese Sekwenz (eds), *Digital Decade: How the EU Shapes Digitalisation Research* (Nomos 2025) 115, 119.

212 Regulation (EU) 2022/2065, arts 33 – 37.

Ireland's Digital Services Act 2024

While the DSA is a regulation and therefore has direct effect in all EU Member States without requiring domestic implementation, the Digital Services Act 2024 (the 2024 Act) was enacted in Ireland to give it further effect, as well as to amend the Broadcasting Act 2009 and the Consumer Protection Act 2014. The 2024 Act was enacted to give effect to the EU DSA in Ireland and establish the national enforcement framework. In doing so, the 2024 Act designated Coimisiún na Meán (the Media Commission) as the competent DSC for Ireland.²¹³ The 2024 Act also designated the Competition and Consumer Protection Commission (CCPC) as a second authority with respect to online marketplaces.²¹⁴

As the Digital Services Coordinator, Coimisiún na Meán has broad powers to investigate and enforce compliance with the DSA. In addition, the CCPC, as a competent authority with responsibility for Articles 30-32 of the Regulation, possesses investigative and enforcement powers within its designated remit. Between them, these authorities have powers to issue compliance notices, impose financial sanctions for non-compliance, and, in the case of the CCPC, disclose personal data to An Garda Síochána where necessary and proportionate for the prevention or investigation of a criminal offence.²¹⁵

Coimisiún na Meán may, in certain circumstances, require intermediary service providers to address illegal content and, as a matter of last resort, seek court orders requiring providers to block access to non-compliant services. It is also empowered to award 'trusted flagger' status to designated organisations, whose notices of illegal content must be given priority by online platforms.²¹⁶ Coimisiún na Meán also has the power to refuse to grant trusted flagger status, or to revoke such status where the relevant criteria are no longer met.²¹⁷ According to its published activity reporting, Coimisiún na Meán did not initiate any formal investigations under the DSA in response to complaints during 2024.²¹⁸ As 2024 represented the first year of operation of the DSA framework in Ireland, this position should be viewed in its initial implementation context. By 2025 and continuing into 2026, Coimisiún na Meán had commenced a number of investigations under the DSA and was actively cooperating with the European Commission and other Digital Services Coordinators in the enforcement of the DSA, including matters involving VLOPs.²¹⁹

Trusted flagger status is entrusted to organisations that are independent from VLOPs and that possess the expertise necessary to identify illegal content online.²²⁰ Until June 2026, the Central Bank of Ireland was the only organisation in Ireland to hold trusted flagger status, with a remit focused on financial fraud and financial scam-related issues.²²¹ As

213 Digital Services Act 2024, s 44.

214 Department of Enterprise, Tourism and Employment, 'Digital Services Act (DSA)' (Government of Ireland, no date) <<https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/>> accessed 3 December 2025.

215 Digital Services Act 2024, ss 49, 78, 47, and 72, respectively.

216 Broadcasting Act 2009 s 190, as amended by Digital Services Act 2024, s 41.

217 Broadcasting Act 2009 ss 188 and 189.

218 Coimisiún na Meán, 'Annual Activity Report Pursuant to art. 55 of the Digital Services Act' (no date) <https://www.cnam.ie/app/uploads/2025/04/20250319_Art-55-Dsa-report_VFfinal.pdf> accessed 17 December 2025.

219 Coimisiún na Meán, 'Coimisiún na Meán Commences Investigations into TikTok and LinkedIn' (2 December 2025) <https://www.cnam.ie/coimisiun-na-mean-commences-investigations-into-tiktok-and-linkedin/> accessed 24 July 2026; Coimisiún na Meán, 'Two Investigations Commenced into Meta, in Respect of Facebook & Instagram' (5 May 2026) <<https://www.cnam.ie/two-investigations-commenced-into-meta-in-respect-of-facebook-instagram/>> accessed 24 July 2026; Liz Carolan, 'Ireland Moves Deeper into DSA Oversight with New Meta Dark Patterns Probe' (Tech Policy Press, 6 May 2026) <<https://www.techpolicy.press/ireland-moves-deeper-into-dsa-oversight-with-new-meta-dark-patterns-probe/>> accessed 27 August 2026.

220 Coimisiún na Meán, Article 22 Trusted Flaggers: Guidance Document (16 February 2024) 8.

221 Granted until 2028. Coimisiún na Meán, 'Trusted flaggers' (2025) <<https://www.cnam.ie/industry-and-professionals/online-safety-framework/certifications-schemes/trusted-flaggers/>> accessed 3 December 2025.

a financial regulator, the Central Bank has limited involvement in matters pertaining to election interference.

On 25 June 2026, however, Coimisiún na Meán granted trusted flagger status to three additional organisations: the Irish Internet Hotline (IIH), the Irish Music Rights Organisation (IMRO), and the Jewish Representative Council of Ireland (JRCI).²²² These organisations have been accredited for three-year periods and bring specialised expertise in a range of areas, including child sexual abuse material, non-consensual intimate image sharing, racism, xenophobia, financial scams and fraud, copyright infringement, and illegal antisemitic material. As a result, Ireland now has four accredited trusted flaggers operating across a broader range of illegal online content categories.

While these additional designations strengthen Ireland's implementation of Article 22 of the Digital Services Act (DSA), none of the newly appointed trusted flaggers has a specific remit relating to election integrity, political disinformation, or foreign information manipulation and interference. By contrast, Belgium, Greece, and Lithuania have each designated multiple trusted flaggers, including organisations with specific expertise relevant to election integrity.²²³ Given the growing threat posed by digital disinformation, there remains a strong case for Ireland to consider designating additional trusted flaggers with specialist expertise in safeguarding the integrity of elections.

Because many major online platforms base their European headquarters in Ireland, Coimisiún na Meán is responsible for conducting a high number of investigations compared to other Digital Services Coordinators. In January 2026, for example, Coimisiún na Meán was conducting 19 separate investigations pursuant to the DSA.²²⁴ The designation of three additional trusted flaggers therefore represents a significant expansion of the State's capacity to support the identification and reporting of illegal content, while also assisting Coimisiún na Meán in its wider supervisory role.

Trusted flaggers form one element of the DSA's multi-pronged approach to regulating illegal content online. Reports submitted by trusted flaggers receive priority consideration from online platforms and can also assist Coimisiún na Meán in identifying emerging trends and risks across the digital environment. As noted by Digital Services Commissioner John Evans, trusted flagger reports will be "instrumental in establishing an informed, evidence-based approach to [Coimisiún na Meán's] supervision of online platforms."²²⁵ The DSA framework combines these mechanisms with obligations on online platforms (particularly VLOPs and VLOSEs) to address illegal content.²²⁶ These measures are complemented by a hierarchy of content notices, compliance procedures, regulatory guidance, and enforcement mechanisms, designed to respond to the scale of the systemic risks associated with the dissemination of illegal content.²²⁷

222 Coimisiún na Meán, 'Trusted Flagger status granted to three new organisations' <<https://www.cnam.ie/trusted-flagger-status-granted-to-three-new-organisations/>> accessed 7 July 2026.

223 European Commission, 'Trusted flaggers under the Digital Services Act (DSA)' (European Union, 16 December 2025) <<https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa>> accessed 16 December 2025.

224 European Digital Rights (EDRI), 'Coimisiún na Meán' *Digital Services Coordinators Database* <<https://dscdb.edri.org/DigitalServicesCoordinators/Ireland>> accessed 7 January 2026.

225 Coimisiún na Meán, 'Trusted Flagger status granted to three new organisations' <<https://www.cnam.ie/trusted-flagger-status-granted-to-three-new-organisations/>> accessed 7 July 2026.

226 European Commission, 'DSA: Very Large Online Platforms and Search Engines' (European Commission) <<https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>> accessed 23 July 2026.

227 Asha Allen and Ophélie Stockhem, 'A Series on the EU Digital Services Act: Tackling Illegal Content Online' (Center for Democracy and Technology, 2 August 2022) <<https://cdt.org/insights/a-series-on-the-eu-digital-services-act-tackling-illegal-content-online/>> accessed 21 May 2026.

Application of the Digital Services Act

The DSA primarily targets the regulation of *intermediary services* (online platforms that facilitate the sharing of harmful content) rather than directly regulating the malicious actors responsible for generating the harmful content. These actors, who may seek to undermine election integrity, range from foreign states and ideological groups to individuals seeking to suppress opposing voters. Other risks include challenges to the legitimacy of election results (as illustrated in *McEwing v Canada*).

The approach adopted by both the European Union and Ireland, which places stricter obligations on intermediary services, is grounded in the “significant influence” that these online platforms exert over public discourse.²²⁸ In *Amazon EU Sàrl*, the General Court observed that the largest online platforms have, by virtue of their extensive userbases, effectively become public spaces.²²⁹ Although the protection of fundamental rights is traditionally a function of the state, the risks that online misinformation and disinformation pose to the freedom of expression, as well as to democratic processes, justify placing corresponding obligations on platforms to help preserve and protect those rights and processes.²³⁰

The DSA therefore imposes legal obligations on VLOPs and VLOSEs to adopt systematic measures that limit the spread of illegal or harmful content on their services. Under Article 36 of the DSA, for example, the European Commission can, where a crisis occurs, adopt a decision to require VLOPs and VLOSEs to establish crisis response mechanisms. Article 36(2) defines a crisis for the purposes of the Article, as having occurred “where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it.” The response mechanisms are intended to ensure that VLOPs and VLOSEs respond effectively when their services risk amplifying a crisis. The rationale is that online platforms play a decisive role in how information spreads during emergencies. In Ireland, no extraordinary circumstances have arisen to date which would require the implementation of the crisis response mechanism.

However, issues were identified with online content relating to Ireland’s 2024 local and European Parliament elections. The compliance teams established by VLOPs and VLOSEs under EU law, and the methods they used to verify election-related information, lacked transparency, both in their composition and in their procedures. Following the European elections, this opacity prompted the Irish Government to call for greater transparency in the measures adopted by VLOPs and VLOSEs.²³¹

Transparency regarding the seriousness of a threat, the urgency of a situation, and the potential impact on the rights and interests of all affected parties is essential for developing effective counterstrategies. Such transparency is best supported through strong public-private partnerships, particularly between regulators and VLOPs, where information sharing and coordinated responses can be systematically embedded. However,

228 Marie-Therese Sekwenz and Rita Gsenger, ‘The Digital Services Act: Online Risks, Transparency and Data Access’ in Rita Gsenger and Marie-Therese Sekwenz (eds), *Digital Decade: How the EU Shapes Digitalisation Research* (Nomos 2025) 115, 118.

229 Case T-367/23 *Amazon EU Sàrl v European Commission* (General Court, 2025) para 156.

230 Marie-Therese Sekwenz and Rita Gsenger, ‘The Digital Services Act: Online Risks, Transparency and Data Access’ in Rita Gsenger and Marie-Therese Sekwenz (eds), *Digital Decade: How the EU Shapes Digitalisation Research* (Nomos 2025) 115, 131.

231 Joint Committee on EU Affairs, ‘Report on EU Elections, Voting Rights and Disinformation’ (Houses of the Oireachtas, May 2024) 6.

commercial interests compete with the additional obligations placed on platforms in regulating the online space, complicating efforts to build effective cooperation. In an example, X challenged Coimisiún na Meán's decision to implement the Online Safety Code, the purpose of which was to implement the Audiovisual Media Services Directive.²³²

*Example: X v Coimisiún na Meán*²³³

In *X v Coimisiún na Meán*, social media platform X sought judicial review of Coimisiún na Meán's decision to create and adopt the Online Safety Code as being *ultra vires*.²³⁴ X argued that the Online Safety Code went further than what was permitted under the Audiovisual Media Services Directive (Directive (EU) 2018/1808) (the 2018 Directive), and that in any case the Code was precluded by the implementation of the DSA.²³⁵ In particular, X contended that the Code imposes measures restricting not only illegal content, but also legal content deemed to be potentially harmful, which exceeds Coimisiún na Meán's powers under Article 28b of the 2018 Directive.

The High Court interpreted the 2018 Directive and the DSA by giving the statutory provisions their ordinary meaning, informed by the broader legislative context described by the respective explanatory memorandums. The Court held that, while the Code went beyond the requirements of the DSA, this did not constitute an impermissible overreach on the part of the regulator.²³⁶ Rather, the Code's objective of protecting minors from harmful content was considered to be complementary to the regulatory framework established by the DSA. Accordingly, the Court dismissed the application for judicial review.²³⁷

X v Coimisiún na Meán clarified the complementary role of the regulatory frameworks, emphasising the multi-pronged approach envisaged by the DSA in regulating the online space.²³⁸ The 2018 Directive permits the regulation of content, particularly concerning access to content by minors, by the potential harm caused rather than the legality of the content itself.²³⁹ By finding the 2018 Directive complementary to the DSA, *X v Coimisiún na Meán* sets a precedent that the DSA's harmonisation of online content regulation includes and is supported by more specific legislation that informs the types of content which may be harmful. Thus, the impact of *X v Coimisiún na Meán* extends to clarifying the scope of Coimisiún na Meán's role, and by extension other Digital Services Coordinators across the EU, in applying the DSA's framework beyond minimum compliance.

232 Coimisiún na Meán, *Online Safety Code* (Coimisiún na Meán, October 2024) 6; and Directive (EU) 2018/1808 (Audiovisual Media Services Directive), section 139K.

233 [2025] IEHC 442.

234 *X Internet Unlimited Company v Coimisiún na Meán* [2025] IEHC 442, [9] and [87].

235 *ibid* [61] and [82].

236 *ibid* [186].

237 *ibid* [186]-[191].

238 *ibid*.

239 Audiovisual Media Services Directive, art 6a.

The emerging body of jurisprudence under the Digital Services Act (at both the EU level and within Ireland) is being shaped primarily through investigations into VLOPs and VLOSEs. As the first entities designated under the DSA and the earliest subjects of regulatory scrutiny, these services are generating the foundational interpretations that will guide future enforcement and judicial review. In April 2026, the European Commission issued preliminary findings that Meta's Facebook and Instagram services were in breach of the DSA, concluding that Meta had failed to adequately identify, assess, and mitigate the risks associated with users under the age of 13 accessing its platforms.²⁴⁰ On 10 July 2026, the Commission issued a separate set of preliminary findings against Meta, concluding that Facebook and Instagram's "addictive design" features (including infinite scroll, autoplay, push notifications, and highly personalised recommender systems) breached the DSA because Meta had not adequately assessed or mitigated the risks posed to users, particularly minors and vulnerable adults.²⁴¹

Towards the end of 2025, Coimisiún na Meán launched an investigation into X's compliance with Article 20 of the DSA, focusing on the platform's complaints handling procedures.²⁴² This investigation has been suspended pending the determination of X's ongoing High Court proceedings against the regulator.²⁴³ Coimisiún na Meán is simultaneously pursuing additional investigations into other VLOPs, including TikTok and LinkedIn and is collaborating with the European Commission in a coordinated inquiry concerning Grok and X.²⁴⁴ The investigations currently being pursued by the European Commission and Coimisiún na Meán demonstrate how the DSA is evolving from a legislative framework into an active system of regulatory oversight. In particular, the investigation concerning Grok and X highlights the extent to which the DSA focuses on platform accountability for systemic risks arising from the design and operation of online services. It also illustrates the central role played by Irish regulators in the supervision of major online platforms established in Ireland.

²⁴⁰ European Commission, 'Commission preliminarily finds Meta in breach of Digital Services Act for failing to prevent minors under 13 from using Instagram and Facebook' (European Commission, 29 April 2026) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_26_920/IP_26_920_EN.pdf> accessed 21 May 2026.

²⁴¹ European Commission, 'Commission Preliminarily Finds the Addictive Design of Instagram and Facebook in Breach of the Digital Services Act' (10 July 2026) <<https://digital-strategy.ec.europa.eu/en/news/commission-preliminarily-finds-addictive-design-instagram-and-facebook-breach-digital-services-act>> accessed 24 July 2026.

²⁴² John Evans in Coimisiún na Meán, 'Coimisiún na Meán Investigation into X' (12 November 2025) <<https://www.cnam.ie/coimisiun-na-mean-investigation-into-x/>> accessed 15 December 2025.

²⁴³ Paul Neilan, 'Elon Musk and X granted High Court permission to challenge Coimisiún na Meán investigation' (The Irish Times, 9 December 2025) <<https://www.irishtimes.com/business/2025/12/09/elon-musk-and-x-granted-high-court-permission-to-challenge-coimisiun-na-mean-investigation/>> accessed 18 December 2025.

²⁴⁴ Coimisiún na Meán, 'Coimisiún na Meán commences investigations into TikTok and LinkedIn' (2 December 2025) <<https://www.cnam.ie/coimisiun-na-mean-commences-investigations-into-tiktok-and-linkedin/>> accessed 15 December 2025.

Example: European Commission investigation into Grok and X²⁴⁵

Grok is an AI model that is deployed directly within the social media platform X. Following widespread reports that Grok's AI-driven image-generation tools had been used to create sexually explicit images of women and children, the European Commission opened a formal investigation into Grok and X. The Commission considered that the misuse of Grok to generate illegal content constituted a serious harm to EU citizens. If X was found to have failed to meet its obligations under Articles 34, 35, and 42 of the DSA – in particular its duties to as a VLOP to assess systemic risk, implement effective mitigation measures, and cooperate with oversight – it could be held in breach of the DSA. In other words, X's potential liability would arise not from the creation of the illegal content, but from any failure to identify and mitigate the risks associated with the misuse of Grok on its platform. Once a formal investigation has commenced, the Commission is empowered to take further enforcement action against the notice parties to ensure compliance.

As the designated Digital Services Coordinator responsible for oversight of X, Coimisiún na Meán is working closely with the European Commission in this investigation in accordance with Article 66 of the DSA.

Ireland hosts the European headquarters of many online services that have been designated as VLOPs and VLOSEs. Indeed, ten of the 20 designated services have their European headquarters in Ireland.²⁴⁶ As a result, Coimisiún na Meán, in its capacity as Ireland's national Digital Services Coordinator, is the *de facto* regulatory authority responsible for overseeing these services, notwithstanding their global operations. One of the core purposes of the DSA is to reduce systemic risks to public security and to safeguard the integrity of electoral processes.²⁴⁷ Given the scale of information disseminated and consumed through VLOPs and VLOSEs, Ireland's regulatory institutions are positioned at the forefront of the European Union's efforts to address the broad societal risks identified in the DSA, including online threats to election integrity.

²⁴⁵ European Commission, 'Commission Investigates Grok and X's recommender systems under the Digital Services Act' (26 January 2026) <https://ec.europa.eu/commission/presscorner/detail/en/ip_26_203> accessed 27 January 2026.

²⁴⁶ European Commission, 'Supervision of the designated very large online platforms and search engines under DSA' (European Union, 5 December 2025) <<https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>> accessed 16 December 2025.

²⁴⁷ European Commission, 'The Digital Services Act' (12 December 2025) <<https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>> accessed 15 December 2025.

Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)

The emergence of GenAI has prompted the European Union to adopt a dedicated regulatory framework governing the development and deployment of AI systems.²⁴⁸ Regulation (EU) 2024/1689 (the Artificial Intelligence Act or AI Act) entered into force in August 2024 and establishes a risk-based framework for the regulation of artificial intelligence across the European Union. While the AI Act is not specifically directed towards election integrity, several of its provisions are directly relevant to the risks posed by AI-generated misinformation, disinformation, and synthetic media during electoral periods.

Unlike the Digital Services Act, which regulates online platforms and the dissemination of content, the AI Act regulates the creation and deployment of AI systems themselves. In so doing, it addresses concerns that advances in GenAI have significantly lowered the barriers to producing convincing but fabricated images, audio recordings, and video content capable of misleading voters or damaging public confidence in democratic institutions.

Of particular relevance is the AI Act's treatment of so-called "deepfakes". Article 3(60) defines a deepfake as AI-generated or manipulated image, audio, or video content that resembles existing persons, objects, places, entities, or events and would falsely appear to a person to be authentic or truthful. The AI Act does not generally prohibit the creation or dissemination of deepfakes. Instead, it adopts a transparency-based approach by requiring, in specified circumstances, that AI-generated or manipulated content be clearly disclosed as such.

Article 50(4) of the AI Act requires deployers of AI systems that generate or manipulate content constituting a deepfake to disclose that the content has been artificially generated or manipulated. The disclosure must be presented in a clear and distinguishable manner and should remain accessible to the recipient of the content. Similar obligations apply under Article 50(4a) to certain AI-generated or AI-manipulated text published for the purpose of informing the public on matters of public interest. The purpose of these transparency measures is to enable individuals to make informed assessments regarding the authenticity and reliability of information they encounter online.

The significance of these obligations for election integrity lies in their preventative character. Rather than prohibiting synthetic media, the AI Act seeks to improve transparency by ensuring that recipients can identify when content has been artificially generated or manipulated.

The AI Act's transparency obligations complement the Digital Services Act. Whereas the AI Act seeks to ensure that synthetic content is identifiable at the point of creation or deployment, the DSA places obligations on online platforms to assess and mitigate the systemic risks associated with the dissemination of such content. Together, the two regimes establish a layered regulatory framework addressing both the production and distribution of AI-generated media.

²⁴⁸ European Commission, 'AI Act' (European Commission) <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 23 July 2026.

The AI Act represents a significant regulatory development in the governance of synthetic media.²⁴⁹ However, it should not be viewed as a complete solution to the risks associated with AI-enabled disinformation. The AI Act does not impose a blanket prohibition on deceptive political deepfakes. Nor does it create a comprehensive, AI-specific regime for the rapid removal of such content disseminated online. Instead, it primarily requires transparency and disclosure for AI-generated or AI-manipulated content, including deepfakes.²⁵⁰

Practical enforcement may also prove challenging. Electoral disinformation campaigns frequently originate outside the European Union or involve anonymous actors operating across multiple online services simultaneously.²⁵¹ Consequently, identifying the original creator of synthetic media may be difficult, even where the content itself can be shown to be AI-generated.²⁵² The effectiveness of the AI Act will therefore depend, at least in part, upon effective cooperation between AI providers, online platforms, national regulators, and law enforcement authorities.²⁵³

Furthermore, the AI Act does not entirely eliminate tensions with fundamental rights. As with the DSA, regulatory interventions directed at misleading content must be balanced against the rights to freedom of expression and political participation protected by both the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.²⁵⁴ The transparency-focused model adopted by the AI Act reflects an attempt to mitigate electoral and informational harms associated with synthetic media while avoiding disproportionate interference with lawful political expression and democratic participation.²⁵⁵

In addition to its deepfake transparency obligations, the AI Act imposes requirements on providers of general-purpose AI models, including obligations relating to technical documentation, transparency, and compliance with copyright rules.²⁵⁶ Certain providers of general-purpose AI models presenting systemic risks are subject to enhanced obligations, including risk assessment and mitigation measures.²⁵⁷ While these provisions are not directed specifically at elections, they may indirectly contribute to election integrity by encouraging greater oversight of the AI systems capable of generating large volumes of synthetic content.

249 European Commission, 'AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 24 July 2026; Freshfields, 'EU AI Act Unpacked #8: New Rules on Deepfakes' (25 June 2024) <<https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-ai-act-unpacked-8-new-rules-on-deepfakes-102jb19>> accessed 24 July 2026.

250 Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts 50(4) and 50(4a); European Commission, 'AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 24 July 2026; Freshfields, 'EU AI Act Unpacked #8: New Rules on Deepfakes' (25 June 2024) <<https://www.freshfields.com/en/our-thinking/blogs/technology-quotient/eu-ai-act-unpacked-8-new-rules-on-deepfakes-102jb19>> accessed 24 July 2026.

251 European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 24 July 2026.

252 Europol, Eurojust and the European Judicial Network, *SIRIUS European Union Electronic Evidence Situation Report 2024* (reported in Europol, 'New SIRIUS Report: Accessing Electronic Evidence in 2024' (28 November 2024)) <<https://www.europol.europa.eu/media-press/newsroom/news/new-sirius-report-%E2%80%93-accessing-electronic-evidence-in-2024>> accessed 24 July 2026.

253 EU CyberNet, 'Cross-Border Access to Electronic Evidence (SIRIUS)' <<https://www.eucybernet.eu/project/sirius/>> accessed 24 July 2026.

254 Charter of Fundamental Rights of the European Union [2016] OJ C202/389, art 11; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) art 10.

255 European Commission, 'AI Act' <<https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>> accessed 24 July 2026.

256 Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) arts 53 and 55.

257 Artificial Intelligence Act, art 56.

The Regulation of Artificial Intelligence Act 2026

The Regulation of Artificial Intelligence Act 2026 (the 2026 Act), enacted in July 2026, provides for the domestic enforcement and implementation of aspects of the AI Act in Ireland. Among other measures, the 2026 Act establishes Oifig IS na hÉireann (the AI Office of Ireland), an independent statutory body responsible for coordinating Ireland's AI governance framework (sections 8 and 9 of the 2026 Act). Oifig IS na hÉireann also serves as the State's designated single point of contact for AI regulatory matters pursuant to the EU AI Act (section 42 of the 2026 Act).²⁵⁸

The 2026 Act further establishes the institutional arrangements necessary for the supervision and enforcement of the AI Act in Ireland. In particular, Part 4 of the 2026 Act sets out the functions and powers of relevant market surveillance authorities and relevant competent authorities, including powers relating to the testing of AI systems, access to information, and the reporting and investigation of serious incidents (sections 57 to 59 of the Act).²⁵⁹ The authorities responsible for carrying out these functions have been designated by the European Union (Artificial Intelligence Act) (Designation of Market Surveillance Authorities and Notification of Competent Authorities) Regulations 2025 (S.I. No. 366 of 2025) (the 2025 Designation Regulations). The 2025 Designation Regulations allocate supervisory responsibilities across a number of sectoral regulators, reflecting the distributed enforcement model adopted under the AI Act. The market surveillance authorities that have been designated include the Central Bank of Ireland, the Data Protection Commission, Coimisiún na Meán, Oifig IS na hÉireann, and the Commission for Regulation of Utilities.²⁶⁰ The national competent authorities that have been designated include the Competition and Consumer Protection Commission, the Health and Safety Authority, and the Commission for Communications Regulation.²⁶¹

The 2026 Act also prescribes offences for breaches of obligations arising under the AI regulatory framework relating to the misuse of AI and sets out the remedies and enforcement mechanisms available in cases of alleged infringement.²⁶²

A notable feature of the 2026 Act is the allocation of a formal coordinating role to Oifig IS na hÉireann. Under section 9 of the 2026 Act, Oifig IS na hÉireann is responsible for coordinating the activities of relevant competent authorities, facilitating information sharing, and supporting joint investigation and enforcement activities. This coordinating function may be particularly significant in the context of addressing AI-generated misinformation, disinformation, and synthetic media, where regulatory issues may engage several bodies simultaneously, including Coimisiún na Meán, the Data Protection Commission, and An Coimisiún Toghcháin. Such coordination may become increasingly important where AI-generated content simultaneously engages electoral law, online platform regulation, data protection obligations, and AI-specific transparency requirements.

²⁵⁸ Regulation of Artificial Intelligence Act 2026.

²⁵⁹ Regulation of Artificial Intelligence Act 2026, Part 4.

²⁶⁰ Designated under regulation 4 of and Schedules 2 and 3 to the 2025 Designation Regulations.

²⁶¹ Designated under regulation 3 of and Schedule 1 to the 2025 Designation Regulations.

²⁶² Regulation of Artificial Intelligence Act 2026, Part 6.

The significance of these arrangements for election integrity lies less in the creation of new substantive obligations than in the establishment of a domestic enforcement structure capable of responding to AI-related harms. Through the investigative, reporting, and co-operation mechanisms established under the 2026 Act, Irish authorities are placed in a stronger position to monitor compliance with AI transparency obligations, investigate suspected breaches, and coordinate responses where AI-generated or manipulated content is disseminated during electoral periods. The 2026 Act's provisions concerning inter-agency co-operation, incident reporting, and regulatory coordination are likely to assume particular importance during electoral periods, where large volumes of AI-generated or manipulated content may engage multiple regulatory regimes simultaneously.

Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising

Aware of the risks posed by foreign states and other malicious actors to electoral processes, the European Parliament sought to harmonise the regulation of political advertising by adopting Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising (the 2024 Regulation).²⁶³ The objective of the 2024 Regulation is to enhance transparency regarding the source and sponsorship of political advertising and provide a common minimum standard to which providers of political advertising must adhere.²⁶⁴

Given domestic implementation in Ireland by the European Union (Political Advertising) Regulations 2025 (S.I. No. 474 of 2025) (the 2025 Regulations) in October 2025, Regulation (EU) 2024/900 establishes harmonised rules for sponsors and providers of political advertising services, including political advertising publishers, and applies to any message prepared, placed, promoted, published, delivered, or disseminated – directly or indirectly – by, for, or on behalf of a political actor.

The 2024 Regulation applies to political advertising sponsored by or on behalf of a political actor, including content produced in-house or disseminated as part of a broader political advertising campaign.²⁶⁵ It does not apply to political information published by Member States for the purpose of informing the public about participation in elections or referendums.²⁶⁶

It requires all political advertisements to be clearly labelled as such and accompanied by information identifying the sponsor, the amount paid, and any criteria used to target certain group(s). The 2024 Regulation also extends to posts by influencers who have received payment or other benefits for content that supports a party, candidate, or political position.

The 2024 Regulation applies broadly to the preparation, placement, promotion, and publication of political advertising by any means, a scope which also includes the co-ordinated posting of messages through fake accounts or pre-designed bots. In effect, where a message is of a kind that would usually be paid for, any form of sponsored political media content falls within the definition of political advertising.²⁶⁷

²⁶³ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, para 19.

²⁶⁴ *ibid.*

²⁶⁵ Regulation 2024/900, art 3.

²⁶⁶ *ibid.*

²⁶⁷ *ibid.*

Microtargeting and Election Integrity

A central concern underlying Regulation (EU) 2024/900 is the increasing use of microtargeting techniques in political campaigning.²⁶⁸ Online political advertising differs significantly from traditional forms of political communication because digital platforms possess extensive amounts of personal data relating to their users.²⁶⁹ These data can be used to segment audiences and deliver highly tailored political messages to specific groups of voters.²⁷⁰

Microtargeting generally refers to the practice of directing political advertisements towards narrowly defined groups of individuals on the basis of personal characteristics, interests, behaviours, demographics, or inferred preferences.²⁷¹ Online platforms are capable of creating detailed profiles of users by analysing browsing histories, engagement patterns, location data, purchasing behaviour, and other forms of online activity.²⁷² These profiles may then be used to determine which political content is shown to particular individuals.²⁷³

Several forms of microtargeting have become common within the digital advertising ecosystem. Behavioural targeting utilises information about a person's online activities and interactions to predict interests or political preferences.²⁷⁴ Profiling involves the creation of detailed assessments regarding an individual's characteristics, attitudes, or likely behaviour.²⁷⁵ Lookalike audience techniques enable advertisers to target individuals who share characteristics with existing groups of supporters, while voter segmentation permits campaigns to create customised messages for different demographic or social groups.²⁷⁶ These practices can significantly increase the effectiveness of political advertising by tailoring messages to the concerns or vulnerabilities of specific audiences.²⁷⁷

The use of microtargeting in political campaigns has attracted increasing scrutiny because it reduces the transparency traditionally associated with electoral debate.²⁷⁸ In

²⁶⁸ Regulation (EU) 2024/900, recitals 1-2; European Commission, 'Transparency and Targeting of Political Advertising' (European Commission, 2025) <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en> accessed 24 July 2026.

²⁶⁹ Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-356; Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-8.

²⁷⁰ European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3; Council of Europe, 'Tackling the Risks for Democracy of Digital Political Campaigning: Council of Europe Issues Guidelines' (6 April 2022).

²⁷¹ Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-8; Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-353.

²⁷² Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-356; Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-7.

²⁷³ European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3; Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, recitals 1, 2, and 14.

²⁷⁴ Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-354; Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-8.

²⁷⁵ Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-8; Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, recitals 14-18.

²⁷⁶ Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-356; European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3.

²⁷⁷ European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3; Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-9.

²⁷⁸ European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3; Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, recitals 2-8.

contrast to broadcast media, where political messages are visible to the general public, targeted online advertisements may only be seen by a small subset of voters.²⁷⁹ This allows campaigns to present different messages to different audiences with limited public scrutiny.²⁸⁰ Critics have argued that such practices may undermine democratic accountability by fragmenting public debate and making it more difficult for journalists, regulators, and opposing political actors to monitor electoral communications.²⁸¹

Microtargeting has also generated concerns regarding the potential manipulation of voters. Regulatory and academic commentary has suggested that highly personalised political communications may exploit individuals' biases, susceptibilities, or emotional responses in ways that are not possible through traditional forms of political communication.²⁸²

These concerns are particularly significant where targeting relies on sensitive personal data, including data relating to political opinions, racial or ethnic origin, religious or philosophical beliefs, health information, or other special categories of personal data protected under data protection law.²⁸³ The Cambridge Analytica scandal increased international concern regarding the use of personal data, profiling, and psychological techniques in electoral campaigns. It prompted extensive regulatory and parliamentary investigations into the use of data analytics for political influence.²⁸⁴

In response to these concerns, the 2024 Regulation imposes significant restrictions on the targeting and amplification of political advertisements.²⁸⁵ It generally prohibits the use of special categories of personal data for political advertising purposes except in narrowly defined and strictly regulated circumstances, and it establishes specific transparency requirements regarding the targeting techniques employed.²⁸⁶ Political advertisements must be clearly labelled and accompanied by information identifying the sponsor, explaining why the advertisement has been shown to a particular audience, and disclosing the principal parameters used for targeting.²⁸⁷ These requirements seek to balance the legitimate role of political communication in a democratic society with the protection of personal data, electoral fairness, and democratic transparency.²⁸⁸

279 Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-9; Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 350-356.

280 European Parliamentary Research Service, *Towards New Rules on Transparency and Targeting of Political Advertising* (PE 733.592, April 2024) 1-3; Council of Europe, 'Tackling the Risks for Democracy of Digital Political Campaigning: Council of Europe Issues Guidelines' (6 April 2022).

281 Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2022) 5-9; Maja Brkan, 'The Regulation of Data-Driven Political Campaigns in the EU: From Data Protection to Specialized Regulation' (2022) 41 *Yearbook of European Law* 348, 356-365.

282 European Data Protection Board, *Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns* (13 March 2019) 1-2; Council of Europe, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (Council of Europe 2022) 6-8.

283 European Data Protection Board, *Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns* (13 March 2019) 2-3.

284 Information Commissioner's Office, *Investigation into the Use of Data Analytics in Political Campaigns: A Report to Parliament* (6 November 2018) 7-12; House of Commons Digital, Culture, Media and Sport Committee, *Disinformation and 'Fake News': Interim Report* (HC 2017-19, 363) paras 92-94.

285 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025) <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en> accessed 27 July 2026.

286 Regulation (EU) 2024/900, arts 18-20; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

287 Regulation (EU) 2024/900, arts 11-12 and 19; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

288 Regulation (EU) 2024/900, recital 1 and art 1 (stating that the Regulation aims to support open and fair political debate while protecting personal data and addressing information manipulation concerns); European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

As regards election integrity, the significance of these measures extends beyond protecting personal data to preserving open and transparent democratic debate.²⁸⁹ Democratic elections function most effectively where political arguments can be publicly scrutinised, challenged, and debated by voters, political opponents, journalists and civil society actors.²⁹⁰ Restrictions on political microtargeting therefore reflect a broader concern that democratic discourse should not become fragmented into opaque and highly personalised communications that are visible only to select audiences.²⁹¹ By increasing transparency regarding targeting and advertising practices, the 2024 Regulation seeks to enhance accountability in political advertising and to enable oversight by voters, regulators, journalists, researchers, and civil society organisations.²⁹²

The 2024 Regulation does not prohibit political advertising; rather, it introduces enhanced transparency and reporting obligations on those who sponsor and disseminate it.

Regulation 36(2) of the European Union (Political Advertising) Regulations 2025 (the 2025 Regulations) repealed Part 4 of the Electoral Reform Act 2022. According to the Minister for Housing, Local Government and Heritage, the 2025 Regulations replace the provisions of Part 4 of the 2022 Act by maintaining its substantive scope while ensuring full alignment with the 2024 Regulation.²⁹³ The 2025 Regulations also expand the legal framework by extending its application to all forms of political advertising, not only to online content.²⁹⁴

The scope of the 2025 Regulations has attracted criticism, with several VLOPs - including Meta, TikTok, and X – arguing that the new requirements are excessively restrictive.²⁹⁵ Indeed, several VLOPs responded by prohibiting all political advertising on their platforms. The response by the largest social media platforms to ban political advertising, rather than implement the transparency and flagging mechanisms that the 2025 Regulations require, has had the practical effect of removing political advertisements of even mainstream and established political parties. Commentators have argued that the removal of mainstream political party advertisements from social media platforms makes it easier for malicious actors to mislead potential voters.²⁹⁶

In the absence of political advertising on these platforms, political actors have increasingly relied on organic reach, with campaign-trail videos gaining traction and going viral in place of sponsored media campaigns.

289 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, recital 1 and art 1; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025) <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en> accessed 27 July 2026.

290 Consultative Committee of Convention 108, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (Council of Europe 2022) 6-8.

291 Consultative Committee of Convention 108, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (Council of Europe 2022) 7-9; European Data Protection Board, *Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns* (13 March 2019) 1-2.

292 Regulation (EU) 2024/900, arts 11-13 and 19; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

293 Dáil Deb 2 December 2025, Question 318.

294 European Union (Political Advertising) Regulations 2025 s 9.

295 Meta, 'Ending Political, Electoral, and Social Issue Advertising in the EU in Response to Incoming EU Legislation' (25 July 2025) <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>> accessed 11 November 2025; and Anette Kroeber-Riel, 'An Update on Political Advertising in the European Union' (Google Blog, 14 November 2024) <<https://blog.google/company-news/inside-google/around-the-globe/google-europe/political-advertising-in-eu/>> accessed 11 November 2025.

296 Liz Carolan quoted in Conor O'Carroll and Maria Delaney, 'Political ad ban by social media companies leaves elections 'susceptible to bad actors'' (The Journal, 23 October 2025) <<https://www.thejournal.ie/investigates-social-media-political-ad-ban-6851352-Oct2025/>> accessed 20 May 2026.

The extent of the criticism of the regulatory obligations under the 2024 Regulation prompted the European Commission to issue a new set of guidelines intended to simplify compliance with the Regulation and to support both platforms and regulatory authorities in implementing it.²⁹⁷ However, at the time of writing (October 2026), it remains unclear whether these guidelines will encourage VLOPs and VLOSEs to reintroduce political advertising, as none of the platforms has yet reversed its decision to prohibit such content.

The restrictions on political microtargeting introduced by the 2024 Regulation represent a significant development in the regulation of digital political campaigning.²⁹⁸

Whereas previous regulatory approaches largely focused on ensuring transparency regarding the identity of those sponsoring political advertisements, the 2024 Regulation also imposes obligations concerning the targeting and advertising techniques used to disseminate political messages,²⁹⁹ as discussed. This reflects growing concern that electoral influence may be exercised not only through the substance of political messages but also through the profiling, algorithmic systems, and data processing techniques used to determine which individuals receive them.³⁰⁰ The 2024 Regulation therefore extends the concept of electoral transparency beyond the source and funding of political advertising to encompass the mechanisms through which audiences are identified and reached.³⁰¹

297 Commission, 'Guidelines to Support the Implementation of Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising' COM (2025) 6829 final.

298 Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L 2024/900, recital 1 and art 1; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025) <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/transparency-and-targeting-political-advertising_en> accessed 27 July 2026.

299 Regulation (EU) 2024/900, arts 11-13 and arts 18-20; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

300 European Data Protection Board, *Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns* (13 March 2019) 1-2; Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (Council of Europe 2022) 6-9.

301 Regulation (EU) 2024/900, arts 11-13 and 19; European Commission, *Transparency and Targeting of Political Advertising* (updated 10 October 2025).

Assessing the Regulatory Framework





Assessing the Regulatory Framework

This chapter examines the effectiveness of the legal and regulatory framework outlined in the previous chapter. It considers both the strengths and limitations of the Digital Services Act (DSA), analyses the implications of the continued non-commencement of Part 5 of the Electoral Reform Act 2022, and evaluates the balance struck between combating information disorders and protecting the freedom of expression. The chapter also considers alternative approaches, including media literacy and public resilience initiatives, before assessing the overall effectiveness of the current regulatory model.

Challenges within the DSA Framework

While the obligations imposed on very large online platforms (VLOPs) and very large online search engines (VLOSEs) under the DSA can be justified by the effectively public role these platforms play, it is worth noting that, due to their scale, they face significant regulatory cost and administrative burden that do not apply to platforms with fewer than 45 million users. In *Amazon EU Sàrl*, Amazon argued that this differential treatment constituted a breach of the principle of equal treatment. However, the General Court rejected that argument, identifying justifiable reasons for treating a VLOP differently from a small online business based on the systemic risks posed to their large audiences by the spread of illegal content.³⁰² In any case, the Court found that Amazon was being treated in the same manner as all other VLOPs.

The DSA has also faced criticism regarding its treatment of illegal content and of harmful content. Although the DSA is described as a harmonising framework across the EU, the definition of illegal content remains imprecise. This is particularly problematic given that EU Member States maintain differing (and sometimes conflicting) definitions and legal standards. For example, defamation of religion constitutes a criminal offence in Germany and would therefore qualify as illegal content, whereas the same expression is lawful in neighbouring Denmark.³⁰³ Research indicates that VLOPs and VLOSEs frequently remove content on the basis of their own terms and conditions rather than pursuant to the DSA's illegal content provisions, in part due to ongoing uncertainty in respect of whether the material in question would qualify as harmful or illegal under EU law.³⁰⁴

³⁰² Case T-367/23 *Amazon EU Sàrl v European Commission* (General Court, 2025) paras 156-157.

³⁰³ Aina Turillazzi and others, 'The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15(1) *Law, Innovation and Technology* 83, 94.

³⁰⁴ Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (ACM Conference on Fairness, Accountability and Transparency, Rio de Janeiro, June 2024); Aina Turillazzi and others, 'The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15(1) *Law, Innovation and Technology* 83, 94-96.

Similar issues have been identified in the UK, where the Online Safety Act has been criticised for having a “loose definition” of harmful content.³⁰⁵ Both the DSA framework and the UK’s Online Safety Act regulate illegal content, but leave the scope of harmful – but not necessarily illegal – content unclear.³⁰⁶ In the DSA’s case, this was in part due to concerns raised by the European Parliament’s Committee on Civil Liberties, Justice and Home Affairs on the impact that limiting potentially harmful, but legal, content would have on the right to freedom of expression.³⁰⁷ Consequently, it will be for test cases to establish a precise definition of what is harmful content, and the extent to which it is covered by the regulatory framework.



Data analytics, compiling complex information (Image: Shutterstock)

305 Kir Nuthi and Mella Tesfagzi, ‘Reforming the UK Online Safety Bill to Protect Legal Free Expression and Anonymity’ (Center for Data Innovation, 29 August 2022) <<https://www2.datainnovation.org/2022-uk-online-safety-bill.pdf>> accessed 17 December 2025.

306 Albeit in the DSA’s case, harmful but not illegal content is left to other mechanisms such as the Audiovisual Media Services Directive and domestic codes of conduct.

307 Committee on Civil Liberties, Justice and Home Affairs, ‘Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the Proposal for a Regulation of the European Parliament and of the Council Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC’ (19 June 2021) 5. <https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf> accessed 17 December 2025.

Statutory Definitions and the Non-Commencement of Part 5 of the Electoral Reform Act 2022

A further issue arising within Ireland's regulatory framework concerns the continued non-commencement of Part 5 of the Electoral Reform Act 2022. Part 5 was introduced in response to concerns regarding the role of misinformation and disinformation in electoral processes and provides a statutory framework empowering An Coimisiún Toghcháin to monitor, investigate, and respond to such activity. Significantly, Part 5 would also introduce statutory definitions of both misinformation and disinformation. However, at the time of writing (October 2026), those provisions have not been commenced.

The non-commencement of Part 5 creates a degree of uncertainty within the Irish legal framework. While online political advertising is now regulated through the DSA, Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising, and the supervisory functions of Coimisiún na Meán, the specific election integrity provisions envisaged by Part 5 remain dormant. As a result, Ireland relies primarily on the DSA's systemic risk model and broader platform governance obligations to address election-related misinformation and disinformation. This raises the question of whether the absence of commenced provisions creates a regulatory gap in Ireland's approach to protecting the integrity of elections.

There are arguments that the delay in commencing Part 5 does create such a gap. The current framework contains no operative statutory definitions of misinformation or disinformation, despite both concepts being used extensively in policy documents, regulatory guidance, and public discourse.³⁰⁸ Nor does An Coimisiún Toghcháin currently possess the full suite of powers originally envisaged by Part 5 to address false electoral information. In particular, the absence of a dedicated legislative framework may make it more difficult to clearly delineate responsibilities between electoral authorities and digital regulators, potentially creating uncertainty regarding institutional mandates and accountability.

However, there are equally persuasive arguments against immediate commencement in its current form. Since the enactment of the Electoral Reform Act 2022, the regulatory landscape has changed significantly. The DSA has entered into force, Coimisiún na Meán has assumed responsibility as Ireland's Digital Services Coordinator (DSC), the Artificial Intelligence Act has introduced obligations regarding synthetic media, and Regulation (EU) 2024/900 has established a harmonised framework for political advertising. Consequently, Part 5 was designed for a regulatory environment that differs substantially from that which now exists at both Irish and European Union level.

³⁰⁸ European Commission, *Guidelines for Providers of VLOPs and VLOSEs on the Mitigation of Systemic Risks for Electoral Processes* (26 April 2024) <<https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes>> accessed 24 July 2026; Coimisiún na Meán, 'Digital Services' <<https://www.cnam.ie/category/digital-services/>> accessed 24 July 2026.

The Case for and Against Statutory Definitions

The question of whether misinformation and disinformation should be defined in legislation remains particularly contentious. A principal advantage of statutory definitions is that they provide legal certainty and transparency regarding the conduct that may trigger regulatory intervention. Clear definitions may assist regulators, courts, online platforms, and members of the public in understanding the scope of state action and the distinction between intentional deception and innocent error. The proposed definitions contained within Part 5 seek to distinguish misinformation from disinformation primarily by reference to intent, reflecting a distinction that is widely adopted in both academic literature and European policy instruments.³⁰⁹

However, the adoption of statutory definitions raises important freedom of expression concerns. Broadly drafted definitions risk capturing legitimate political speech, satire, opinion, journalistic error, or contested statements made during the course of democratic debate.³¹⁰ Such an approach could create tensions with the right to freedom of expression protected by Article 10 of the European Convention on Human Rights (ECHR) and Article 11 of the Charter of Fundamental Rights of the European Union. As demonstrated by the decisions of the European Court of Human Rights in *Salov v Ukraine* and *Brzeziński v Poland*,³¹¹ states possess a legitimate interest in protecting the integrity of electoral processes, but restrictions on political expression must satisfy the requirements of legality, necessity, and proportionality under Article 10 ECHR. The Court has consistently afforded a high level of protection to political speech, particularly during electoral periods when public debate is at its most important.

Accordingly, any attempt to introduce statutory definitions of misinformation or disinformation should be approached with caution. Definitions that are vague, overly broad, or based solely on the falsity of information may create legal uncertainty and risk chilling lawful democratic participation.³¹² A more defensible approach would be to ensure that any statutory definitions are narrowly drafted, clearly targeted at demonstrably false or misleading information, and incorporate elements such as intent to deceive, recklessness, or the likelihood of causing significant public harm.³¹³ Such safeguards would better distinguish malicious information manipulation from legitimate political discourse, good faith error, or opinion.

309 Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026; EU Code of Practice on Disinformation, Preamble (defining disinformation as verifiably false or misleading information created, presented and disseminated in order to intentionally deceive the public or secure economic gain).

310 Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026.

311 *Salov v Ukraine* App no 65518/01 (ECtHR, 6 September 2005); *Brzeziński v Poland* App no 47542/07 (ECtHR, 25 July 2019).

312 Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026.

313 European Commission, *Strengthened Code of Practice on Disinformation* (June 2022) Preamble (defining disinformation as verifiably false or misleading information disseminated with the intention of deceiving the public and capable of causing public harm).

The Digital Service Act's Alternative Risk-Based Model

Although the EU Code of Practice on Disinformation adopts a definition of disinformation based on falsity, intent to deceive, and public harm, the DSA deliberately avoids defining either misinformation or disinformation.³¹⁴ Instead, it adopts a systemic risk-based approach that focuses on broader harms to civic discourse, electoral processes, and fundamental rights rather than attempting to categorise individual items of content. This model places emphasis on patterns of manipulation, amplification mechanisms, coordinated campaigns, and systemic risks to democratic processes, while reducing the need for regulators to make case-by-case determinations regarding the truthfulness of political speech.

The risk-based approach adopted by the DSA offers a degree of flexibility that may be better suited to emerging technologies and novel forms of online manipulation.³¹⁵ Rather than requiring regulators to determine whether a given statement falls within a fixed statutory definition of misinformation or disinformation, the DSA focuses on assessing and mitigating risks arising from the dissemination of harmful content. This approach may be particularly advantageous in circumstances where generative artificial intelligence (GenAI), synthetic media, and foreign information manipulation continue to evolve rapidly. However, the advantages of flexibility must be balanced against the benefits of legal certainty. If Part 5 is to be commenced, there is a strong case for ensuring that any statutory definitions are carefully aligned with existing European regulatory frameworks, are rights compliant, and contain sufficient safeguards to protect freedom of expression under both Article 10 of the ECHR and Article 11 of the EU Charter of Fundamental Rights.³¹⁶



Vote Election Document Filling. (Image: Shutterstock)

³¹⁴ *ibid.*

³¹⁵ European Commission and the Board for Digital Services, *Second Report on Systemic Risks on Very Large Online Platforms and Search Engines under the Digital Services Act* (2 July 2026) <<https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services>> accessed 27 August 2026; Sally Broughton Micova and Andrea Calef, *Elements for Effective Systemic Risk Assessment under the DSA* (CERRE, 17 July 2023) <<https://cerre.eu/publications/elements-for-effective-systemic-risk-assessment-under-the-dsa/>> accessed 24 July 2026.

³¹⁶ Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026.

Regulatory Coherence and Divergent National Implementation

The debate surrounding statutory definitions of misinformation and disinformation illustrates a broader regulatory challenge. Even if Part 5 were commenced, its operation would not occur in isolation but within an established European framework that already addresses many of the same concerns through the DSA's systemic risk model. Accordingly, assessing whether the non-commencement of Part 5 creates a genuine regulatory gap requires consideration of how the DSA is functioning in practice and whether it adequately addresses threats to electoral integrity.

There are notable divergences in how the DSA is being implemented across Member States. Although the DSA prohibits national authorities from requiring VLOPs and VLOSEs to deploy general monitoring systems for illegal content,³¹⁷ it leaves the regulation of online content to national DSCs. This decentralised model creates the potential for inconsistent approaches to identifying and addressing illegal or harmful content, depending on which national regulatory authority a VLOP or VLOSE falls under.

Anticipating the risk of divergent national practices, the European Commission has issued guidance publications to aid in the harmonisation of national approaches. In relation to elections, the European Commission has published the DSA Elections Toolkit to assist Digital Services Coordinators on approaches to preserving election integrity under the DSA.³¹⁸ The DSA Elections Toolkit recommends early engagement with online platforms by DSCs, well in advance of any electoral period, to support a coordinated approach towards minimising and regulating disinformation.³¹⁹ In addition to the measures aimed at mitigating the risks associated with disinformation, the Toolkit suggests that cooperation with VLOPs and VLOSEs should also focus on promoting trusted and official sources of information.³²⁰ However, the DSA Elections Toolkit ultimately encourages DSCs to “establish basic protocols and procedures”, rather than providing standardised template protocols that would enable a more fully harmonised approach across Member States.³²¹

Freedom of Expression and the Risk of Over Removal

As already described, the principal aim of the DSA (to prevent the spread of illegal and harmful content) inevitably intersects with the freedom of expression. The boundary between sharing information believed to be true and disseminating misinformation or disinformation is often difficult to draw.³²² Several commentators suggest that the DSA's practical orientation leans more toward the removal of content than restoration of material taken down in error, raising concerns that VLOPs and VLOSEs may over-remove content in an effort to ensure compliance, thereby undermining the freedom of expression.³²³

³¹⁷ Caroline Cauffman and Catalina Goanta, 'A New Order: The Digital Services Act and Consumer Protection' (2021) 12(4) European Journal of Risk Regulation 758, 765.

³¹⁸ European Board for Digital Services and the European Commission, *DSA Elections Toolkit for Digital Services Coordinators* (European Union 2025).

³¹⁹ *ibid* 10-11.

³²⁰ *ibid* 12.

³²¹ *ibid* 16.

³²² As seen in *Salov v Ukraine App No 65518/01 (ECtHR, 6 September 2005)*.

³²³ Aina Turillazzi and others, 'The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15(1) Law, Innovation and Technology 83, 95.

The possibility of significant financial penalties for non-compliance may create incentives for platforms to adopt a precautionary approach to content moderation. Evidence from Article 17 Statements of Reasons suggests that content removal or concealment remains the predominant response to potentially problematic content, accounting for approximately 93% of reported moderation actions.³²⁴ Although such interventions are often justified on safety grounds, critics argue that the prominence of removal-based remedies may contribute to the risk of over-enforcement and the restriction of lawful expression.³²⁵

Regulatory Spillover and the Chilling Effect on Political Speech

The issues identified in this section could, in combination, produce a compliance environment in which freedom of expression is restricted to an unintended degree. Where content shared on a VLOP is considered illegal in one Member State, the VLOP may, in the interest of easing the administrative burden, opt to remove that content from all regional or even global versions of its service.

The same dynamic may also arise in relation to content that is not illegal in any Member State but is regulated so strictly that compliance is burdensome. This has been evident in the context of the EU's recent regulation of political advertising, which prompted Meta and Google to withdraw all political advertising from their platforms on the basis of 'unworkable requirements'.³²⁶ Critics of those decisions, including politicians and campaigners, have argued that the removal of political advertising from large online platforms may reduce transparency and limit opportunities for democratic engagement by shifting campaign activity to less visible channels.³²⁷ Whether these effects materialise in practice remains contested. However, this illustrates how regulatory obligations may inadvertently incentivise platforms to completely withdraw certain categories of speech rather than assume the associated compliance burden.

Further, EU regulation can become a *de facto* standard, affecting free speech beyond the EU's jurisdictional borders.³²⁸ Research shows, for example, that location-based approaches to content moderation frequently extended beyond the borders of the EU. Approximately 73% of remedies for illegal or harmful content were applied across the European Economic Area, rather than solely within the Member State in which the content is deemed illegal or harmful, or even strictly within the EU's own jurisdiction.³²⁹

Concerns regarding interference with the right to freedom of expression were central to the debate preceding the adoption of the DSA. An opinion by the Committee on Civil

324 Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (ACM Conference on Fairness, Accountability and Transparency, Rio de Janeiro, June 2024).

325 Aina Turillazzi and others, 'The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications' (2023) 15(1) Law, Innovation and Technology 83, 95.

326 As detailed in the respective news bulletins. Meta, 'Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation' (25 July 2025) <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>>; and Google, 'Update to Political Content Policy' (September 2025) <<https://support.google.com/adspolicy/answer/16409999?hl=en>>.

327 Ellen O'Regan and Eliza Gkritsi, 'Backlash as new EU political ad rules kick' (Politico, 10 October 2025) <<https://www.politico.eu/article/eu-political-ad-rules-google-meta-microsoft-big-tech-kick-in/>> accessed 6 January 2026.

328 Richard Wennberg, 'Does the EU's Digital Services Act Violate Freedom of Speech?' (Center for Strategic and International Studies, 22 September 2025) <<https://www.csis.org/blogs/europe-corner/does-eus-digital-services-act-violate-freedom-speech>> accessed 16 December 2025.

329 Kaushal and others, 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database' (ACM Conference on Fairness, Accountability and Transparency, Rio de Janeiro, June 2024).

Liberties, Justice and Home Affairs criticised the effective outsourcing of decisions as to whether content is illegal or harmful to the online platforms themselves, rather than to an independent judicial authority.³³⁰ The Committee further argued that responsibility should lie with the Commission and the Member States to ensure that illegal content is removed only within the territory in which it is illegal.³³¹

Beyond Content Moderation: Building Societal Resilience

The concerns outlined above have led some commentators to question whether content moderation and regulatory enforcement alone are sufficient to address misinformation and disinformation.³³² In particular, the risk of over-removal and the potential impact on freedom of expression have prompted consideration of alternative or complementary approaches that focus on strengthening societal resilience to information manipulation rather than restricting access to content.³³³ Such approaches may be especially relevant within the DSA framework, which seeks to mitigate systemic risks while preserving fundamental rights.³³⁴

Several academics have suggested that an ‘inoculation’ approach to public education may be a more effective strategy for countering misinformation and disinformation. In the context of climate-related misinformation and disinformation, for example, research has shown that educational interventions can positively influence public understanding, even among groups that are initially sceptical.³³⁵

More recently, these educational approaches have been reflected in the development of ‘prebunking’ strategies. Prebunking seeks to expose individuals to common manipulation techniques before they encounter them in real-world information environments. The intention is to increase their ability to recognise and resist misleading content when subsequently encountered.³³⁶ Rather than attempting to correct false information after it has spread, prebunking aims to build psychological resilience in advance through public awareness campaigns, media literacy initiatives, and explanatory content highlighting common disinformation tactics (including emotional manipulation, conspiracy narratives, impersonation, and the use of fabricated evidence).³³⁷ Research suggests that prebunking interventions may improve an individual’s ability to identify misleading information and

330 Committee on Civil Liberties, Justice and Home Affairs, ‘Draft Opinion of the Committee on Civil Liberties, Justice and Home Affairs for the Committee on the Internal Market and Consumer Protection on the Proposal for a Regulation of the European Parliament and of the Council Single Market for Digital Services (Digital Services Act) and Amending Directive 2000/31/EC’ (19 June 2021) 12. <https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf> accessed 17 December 2025.

331 *ibid* amendment 8.

332 Aina Turillazzi and others, ‘The Digital Services Act: An Analysis of its Ethical, Legal, and Social Implications’ (2023) 15(1) *Law, Innovation and Technology* 83.

333 Sander van der Linden, Jon Roozenbeek and Josh Compton, ‘Inoculating Against Fake News About COVID-19’ (2020) *Frontiers in Psychology* 11, 2928; Sander van der Linden and others, ‘Inoculating the Public Against Misinformation About Climate Change’ (2017) 2(1) *Global Challenges* 1600008.

334 Digital Services Act recitals 3, 9, 81, and art 34.

335 Sander van der Linden and others, ‘Inoculating the Public Against Misinformation About Climate Change’ (2017) 2(1) *Global Challenges* 1, 5.

336 Sander van der Linden and Jon Roozenbeek, ‘“Inoculation” to Resist Misinformation’ (2024) 331(22) *Journal of the American Medical Association* 1961, 1961–1962; Jon Roozenbeek, Thomas Nygren, and Sander van der Linden, ‘Prebunking Interventions Based on Psychological Inoculation Can Reduce Susceptibility to Misinformation Across Cultures’ (2020) 1(2) *Harvard Kennedy School Misinformation Review*.

337 Trisha Harjani and others, *A Practical Guide to Prebunking Misinformation* (University of Cambridge, Jigsaw and BBC Media Action 2022); Mikey Biddlestone and others, ‘Tune in to the Prebunking Network! Development and Validation of Six Inoculation Videos that Prebunk Manipulation Tactics and Logical Fallacies in Misinformation’ (2025) 46 *Political Psychology* 1858.

reduce their susceptibility to manipulation. Prebunking is therefore a potentially valuable complement to regulatory and platform-based responses during electoral periods.³³⁸

Research also suggests that individuals with some level of media literacy training are better able to verify information and are less likely to share misinformation as a result.³³⁹

Consistent with these findings, the United Nations Office on Drugs and Crime has recommended public education regarding misinformation and disinformation as an effective tool for mitigating the impact of false information by strengthening people's ability to recognise when they are being misled.³⁴⁰

Persistent Challenges in Platform Enforcement

The issues outlined above suggest that the harmonised regulation of online content may be more fragmented than it appears. Although the DSA envisages a harmonised system of platform accountability, the reliance on first-line moderation by online platforms has not yet resulted in the level of legal certainty and consistency anticipated by the framework.³⁴¹ Different platforms have adopted varying approaches to the handling of illegal and harmful content. Investigations into TikTok's moderation practices, for example, identified 'significant failings' in its handling of disinformation in the Irish language and further found that the platform approved 20% of English-language advertisements containing disinformation.³⁴² In October 2025, the European Commission found that TikTok and Meta had breached their obligations to notify illegal content and to provide effective mechanisms for challenging content moderation decisions.³⁴³

Strengths of the Multi-Layered Regulatory Model

While the preceding analysis identifies a number of unresolved questions within the current regulatory framework, these concerns should not obscure the significant strengths of the DSA's regulatory model. The framework introduces multiple layers of oversight, combines platform responsibility with regulation, and provides mechanisms capable of adapting to evolving forms of online harm. Against that background, it is important to consider those aspects of the framework that appear to be functioning effectively, and which may provide a foundation for future regulatory development.

The regulatory framework established by the DSA demonstrates the potential effectiveness of a multilayered approach to online content moderation. The DSA establishes a hierarchy of oversight mechanisms. The first level consists of online service

338 Jon Roozenbeek, Thomas Nygren, and Sander van der Linden, 'Prebunking Interventions Based on Psychological Inoculation Can Reduce Susceptibility to Misinformation Across Cultures' (2020) 1(2) *Harvard Kennedy School Misinformation Review*; Sander van der Linden and others, 'Misinformation: Susceptibility, Spread, and Interventions to Immunize the Public' (2022) 28 *Nature Medicine* 460.

339 Theodora Dame Adjin-Tettey, 'Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education' (2022) 9(1) *Cogent Arts & Humanities* 1, 12.

340 UNODC, 'Information Warfare, Disinformation and Electoral Fraud' (June 2019) <<https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare-disinformation-and-electoral-fraud.html#top>> accessed 17 December 2025.

341 Charis Papaevangelou and Fabio Votta, 'Trading Nuance for Scale? Platform Observability and Content Governance under the DSA' (2025) 14(3) *Internet Policy Review* <<https://policyreview.info/articles/analysis/platform-observability-and-content-governance>> accessed 27 July 2026.

342 Global Witness, 'TikTok Still Approving Election Disinformation Ads in Ireland' (27 November 2024) <<https://globalwitness.org/en/campaigns/digital-threats/tiktok-still-approving-election-disinformation-ads-in-ireland/>> accessed 18 December 2025.

343 European Commission, 'Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act' (European Union, 24 October 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503> accessed 18 December 2025.

providers' content moderation practices, followed by trusted flaggers, the DSCs, and finally the European Commission. Each of these actors exercises a distinct regulatory role. This creates a system of cumulative oversight, whereby content that falls through one layer of moderation is then (ideally) identified and remedied by the next. The importance of test cases and investigations by the DSCs and the European Commission will serve to refine the edges of the regulatory framework, enabling a more coherent, holistic approach by the different actors.

The advantage of this model is that it utilises a wide range of capabilities in terms of tackling disinformation under the DSA. Given the volume of misinformation and disinformation disseminated through VLOPs and VLOSEs, assigning initial responsibility to platforms through existing content moderation and risk management systems represents a logical starting point for intervention under the DSA.³⁴⁴ Leveraging the large-scale moderation systems already operated by VLOPs and VLOSEs, which review content at the earliest stages of dissemination, offers the earliest practical opportunity to identify and address illegal content before it achieves significant reach.³⁴⁵

The system is then supported by the sector-specific expertise of trusted flaggers, the supervisory and investigatory powers of the DSCs, and the European Commission's capacity for addressing systemic risks through investigations and resolving high-level clarifications of the regulatory framework.³⁴⁶

However, critics have argued that, rather than enhancing transparency around the origins of online political content, the current regulatory framework may have had the opposite effect. As discussed, faced with what they considered difficult compliance requirements under Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising, several major platforms removed political advertising in its entirety, including advertisements from recognised and trusted sources.³⁴⁷ Although these developments arose in the context of Regulation (EU) 2024/900 rather than the DSA itself, they illustrate a broader challenge that also exists within the DSA framework: where regulatory obligations are perceived as excessively burdensome, platforms may choose to remove or restrict categories of content rather than assume the associated compliance costs. Consequently, improved cooperation between online platforms and regulatory authorities operating within the DSA framework is essential.³⁴⁸

³⁴⁴ European 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* (26 April 2024); Niklas Eder, 'Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation' (2024) 25(7) *German Law Journal* 1197.

³⁴⁵ European 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* (26 April 2024) paras 21-31; Niklas Eder, 'Making Systemic Risk Assessments Work: How the DSA Creates a Virtuous Loop to Address the Societal Harms of Content Moderation' (2024) 25(7) *German Law Journal* 1197, 1199-1202.

³⁴⁶ Simona Veleva, 'Digital Services Act: Anticipating Challenges in Regulatory Implementation' (2025) *ELTE Law Journal* 143, 150.

³⁴⁷ Ellen O'Regan and Eliza Gkritsi, 'Backlash as new EU political ad rules kick' (Politico, 10 October 2025) <<https://www.politico.eu/article/eu-political-ad-rules-google-meta-microsoft-big-tech-kick-in/>> accessed 6 January 2026.

³⁴⁸ Simona Veleva, 'Digital Services Act: Anticipating Challenges in Regulatory Implementation' (2025) *ELTE Law Journal* 143, 158.

The Future of Election Integrity





The Future of Election Integrity

Emerging Threats and the Evolving Information Environment

Recent reforms in the regulation of digital technologies reflect a growing recognition that legal frameworks must adapt more effectively to the challenges created by rapid technological change, even if they cannot realistically keep pace with that change. The Digital Services Act (DSA) forms part of this broader regulatory response and was designed to operate alongside sector-specific EU and national legislation.³⁴⁹ The spread of illegal content and other systemic online risks, including misinformation and disinformation, prompted the adoption of the DSA, which establishes a harmonised framework for online platform regulation throughout the European Union.³⁵⁰

However, the implementation of the broader DSA framework has brought to the surface difficulties in precisely defining the type of content which is to be moderated. The removal of political advertising from several very large online platforms (VLOPs) such as Meta and X is, in Meta's words, a decision of operational complexity.³⁵¹ This highlights the difficulty in designing regulatory measures that are both effective and workable in fast-moving digital ecosystems.

A related example may be found in how legal frameworks governing political financing, which were designed to prevent unfair advantages in election campaigns, have proven to be less effective in the digital space.³⁵² Online platforms can obscure the origins of both funding and information behind politically aligned content, allowing actors to circumvent campaign finance restrictions. Through abstracting or anonymising material sources and exploiting the speed and scale at which information circulates online, certain actors can launch targeted political campaigns on a scale previously unattainable.

A useful illustration of the regulatory challenges posed by digital communication is the shift in approach to broadcast moratoriums. These rules, which restricted political coverage in the immediate period before elections, required compliance by traditional media such as newspapers, radio, and television.³⁵³ However, the limitations of the moratorium were circumvented by the use of online platforms, where individual users and decentralised actors on online platforms could share misinformation and disinformation which could not

349 European Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Article 33 of Regulation (EU) 2022/2065 and the interaction of that Regulation with other legal acts' COM (2025) 708 final, 2.

350 *ibid* 1.

351 Meta, 'Ending Political, Electoral, and Social Issue Advertising in the EU in Response to Incoming EU Legislation' (25 July 2025) <<https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>> accessed 11 November 2025.

352 Catherine Lynch, 'The Regulation of Online Political Advertising' (Houses of the Oireachtas Library and Research Service, 4 February 2021) 13-14.

353 Broadcasting Act 2009 (as enacted), ss 42 and 48.

then be debunked by traditional media.³⁵⁴ The subsequent revocation of the broadcast moratorium rules in Ireland was therefore welcomed as a pragmatic step, enabling trusted traditional media to operate on a more level playing field with fewer verifiable online sources.³⁵⁵

While the right to free elections by secret ballot has been protected under the European Convention on Human Rights for more than 70 years,³⁵⁶ contemporary threats to election integrity increasingly arise from disinformation and foreign information manipulation and interference (FIMI). Unlike traditional forms of election interference, these activities do not typically target the mechanics of voting itself. Rather, they seek to influence voters indirectly by shaping perceptions, distorting public debate, and attempting to undermine trust in democratic institutions.³⁵⁷

This new dynamic risks undermining the ‘principle of political equality’, which assumes that electoral competition should not be distorted by opaque or disproportionate influence.³⁵⁸

An example of the risk that digital interference can pose to electoral behaviour emerged during the 2024 Romanian Presidential Election, where allegations of foreign influence through social media platforms played a significant role.



A person actively participates in online voting, using a laptop to submit their ballot while preparing necessary documents for the election. (Image: Shutterstock)

354 As several broadcasters such as RTÉ and Virgin Media responded to a Coimisiún na Meán consultation. Martin Wall, ‘Broadcasters Told Media Regulator They Backed Abolishing the Pre-Election Moratorium’ (The Irish Times, 28 November 2024) <<https://www.irishtimes.com/politics/2024/11/28/broadcasters-told-media-regulator-they-backed-abolishing-the-pre-election-moratorium/>> accessed 22 May 2026.

355 An Coimisiún Toghcháin, ‘Election Broadcast Moratorium Removal Welcomed’ (1 November 2024) <<https://www.electoralcommission.ie/latest-news-and-research/election-broadcast-moratorium-removal-welcomed/>> accessed 15 December 2025.

356 Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms 1952, art 3.

357 Christine Bohan, ‘The new misinformation around elections’ (The Journal, 14 March 2024) <<https://www.factchecking.ie/articles/the-new-misinformation-around-elections#anchor-2>> accessed 7 January 2026.

358 Holly Garnett and Toby James, ‘Cyber Elections in the Digital Age: Threats and Opportunities of Technology for Electoral Integrity’ (2020) 19(2) Election Law Journal 111, 118.

Example: Romanian Presidential Election 2024

During Romania's 2024 presidential election, Călin Georgescu, a relative newcomer to national politics, secured the highest number of votes in the first round of voting. His unexpected success drew scrutiny from Romanian intelligence agencies, which reported concerns about campaign irregularities, particularly the lack of transparency surrounding funding sources. Amplified by an extensive social media campaign, Georgescu's support had increased from an initial polling level of 5% to 23% in the first round of voting.³⁵⁹

These concerns were ultimately referred to the Romanian Constitutional Court. Pursuant to its constitutional mandate to safeguard the integrity of presidential elections in Romania,³⁶⁰ the Court was tasked with determining whether electoral law had been violated and whether any such violations were sufficiently grave to warrant the annulment of the election.³⁶¹ The argument for annulment centred on claims that misinformation disseminated through social media had interfered with the Romanian voters' freedom to form an opinion and with the principle of universal direct suffrage.

The Court ultimately held that the lack of transparency surrounding Georgescu's campaign, coupled with the dissemination of misleading information regarding other candidates, had compromised the election. On that basis, it exercised its constitutional power to annul the result and ordered that a new election be held.³⁶²

The constitutional power of the Romanian Constitutional Court acted as a final lever to combat malign threats to elections. Experts have argued that the outcome of the Romanian presidential election case demonstrates the democratic resilience of implementing institutional safeguards for election integrity.³⁶³

359 Claudia Bădulescu and Barry Colfer, 'Romania's 2024–2025 Presidential Election Crisis and Its Aftermath' (IIEA, 9 December 2025) <<https://www.iiia.com/blog/romania-20242025-presidential-election-crisis-and-its-aftermath>> accessed 6 January 2026.

360 Constitution of Romania 1991, art 146(f).

361 Ruling No 32, Romanian Constitutional Court (6 December 2024).

362 Ruling No 32, Romanian Constitutional Court (6 December 2024) [16].

363 Claudia Bădulescu and Barry Colfer, 'Romania's 2024–2025 Presidential Election Crisis and Its Aftermath' (IIEA, 9 December 2025) <<https://www.iiia.com/blog/romania-20242025-presidential-election-crisis-and-its-aftermath>> accessed 6 January 2026.

European and International Responses

The European Union's 'European Democracy Shield' is an example of this new strategy of implementing several layers of safeguards to counteract rising FIMI and the attempted dismantling of democratic processes.³⁶⁴

A key component of the European Democracy Shield is the European Centre for Democratic Resilience (ECDR), which commenced operations in 2026. The ECDR serves as a framework for cooperation between EU institutions, Member States, candidate countries, researchers, civil society organisations, fact-checkers, and other stakeholders.³⁶⁵ Its objectives include improving situational awareness, strengthening early warning and rapid response capabilities, supporting resilience against FIMI and disinformation, and facilitating information exchange regarding threats to democratic processes.³⁶⁶

The Democracy Shield places particular emphasis on countering FIMI, building upon existing EU mechanisms such as the European External Action Service (EEAS) Rapid Alert System and the FIMI Toolbox. The framework seeks to improve the collective capacity of EU Member States to identify, attribute, and respond to coordinated information manipulation campaigns targeting democratic institutions and electoral processes.³⁶⁷

While the European Democracy Shield focuses on democratic resilience and coordinated responses to foreign interference, the European Union has also pursued regulatory measures aimed at the online environment in which disinformation spreads. In particular, the DSA places additional obligations on online platforms rather than attempting to regulate malicious foreign actors directly. This is a pragmatic choice due to the difficulties in identifying or constraining actors operating outside EU jurisdiction, while enabling platforms to implement systematic safeguards that can reduce the spread of misinformation and disinformation.

While there have been attempts in other jurisdictions to regulate online behaviour directly, such as in France and the United Kingdom where the intentional distribution of disinformation has been criminalised, it is debatable what effect, if any, such measures have had on the broader disinformation landscape.³⁶⁸ The cross-border nature of online information flows, combined with the difficulty of identifying anonymous actors and attributing coordinated campaigns, creates significant challenges for enforcement and limits the effectiveness of purely national regulatory responses.

The difficulty of attributing coordinated online influence operations, coupled with the limited reach of national legal frameworks, creates significant accountability gaps. This underscores the need for a broader range of responses, particularly in the context

364 Heather Burke, *European Democracy Shield Explored* (IIEA 2025) 2.

365 European Commission, 'European Centre for Democratic Resilience' (European Commission) <https://commission.europa.eu/european-centre-democratic-resilience_en> accessed 25 May 2026.

366 European Parliament, 'Legislative Train Schedule: European Democracy Shield (EDS)' (European Parliament 20 April 2026) <<https://www.europarl.europa.eu/legislative-train/package-european-democracy-action-plan/file-european-democracy-shield>> accessed 25 May 2026.

367 European Commission, 'European Democracy Shield and EU Strategy for Civil Society pave the way for stronger and more resilient democracies' (Press Release IP/25/2660, 12 November 2025) <https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_2660/IP_25_2660_EN.pdf> accessed 22 July 2026.

368 UNODC, 'Information Warfare, Disinformation and Electoral Fraud' (UNODC, June 2019) <<https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/information-warfare--disinformation-and-electoral-fraud.html>> accessed 17 December 2025.

of coordinated disinformation campaigns, to mitigate wider societal and political consequences. The EEAS, in its role of collating and analysing examples of FIMI, recommends stronger cooperation between EU Member States and the increased use of independent fact-checking organisations to counter online disinformation narratives.³⁶⁹ Establishing clear links between covert channels and the actions of a foreign state enables institutions such as the Council of the European Union to impose sanctions and pursue public attribution, thereby providing more direct accountability for orchestrated disinformation efforts.³⁷⁰

While attribution and sanctions can provide mechanisms for accountability, the transnational nature of modern information ecosystems means that no single jurisdiction can address these challenges in isolation.

Election integrity is increasingly being viewed internationally through the broader lens of democratic resilience. NATO has highlighted the growing threat posed by hybrid activities, including disinformation campaigns, cyber-enabled interference, and hostile influence operations targeting democratic institutions.³⁷¹ Similarly, the Organisation for Economic Cooperation and Development's (OECD) work on information integrity emphasises the importance of transparency, media literacy, independent journalism, public trust, and evidence-based policymaking in strengthening democratic resilience.³⁷² These developments suggest that protecting elections requires a holistic approach extending beyond traditional electoral regulation to include institutional preparedness, international cooperation, and the resilience of the wider information environment.

Ireland's participation in EU initiatives, its engagement with OECD work on information integrity, and its cooperation with international partners therefore represent important components of a broader strategy for safeguarding democratic processes in an increasingly interconnected digital environment.

Alongside these broader resilience-based approaches, there are also strong arguments for the removal of demonstrably false information as part of a wider regulatory toolkit. Social media platforms remain among the most widely used channels for spreading misinformation and disinformation, and evidence indicates that content moderation can successfully slow the spread of false narratives.³⁷³ The role of the DSA, together with Ireland's national implementing legislation, in imposing heightened obligations on social media platforms to monitor and address false information is therefore well founded. The EU-level framework establishes the overarching regulatory requirements, while the Irish legislation operationalises these obligations domestically. The combined approach is justified both by the scale of social media platforms' influence and by evidence that effective content moderation can reduce the dissemination of false and misleading information.

369 European External Action Service, *3rd EEAS Report on Foreign Information Manipulation and Interference Threats* (European Union March 2025) 38.

370 *ibid.*

371 NATO, 'Countering Hybrid Threats' (NATO, 29 January 2026) <<https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats>> accessed 23 July 2026.

372 OECD, Recommendation of the Council on Information Integrity (OECD/LEGAL/0505, 17 December 2024) <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0505>> accessed 24 July 2026.

373 Sandra González-Balión and others, 'The Diffusion and Reach of (Mis)Information on Facebook During the U.S. 2020 Election' (2020) 11 Sociological Science 1124.

A clear example of how misinformation spreads online emerged during the 2025 Irish Presidential election, when false claims regarding the scope of presidential powers circulated widely on X, reaching more than 108 million users. The purpose of this content was to undermine confidence in the electoral process.³⁷⁴ In parallel, domestic actors created and disseminated AI-generated videos targeting the two final candidates, aiming to spread false information, such as falsified videos of Catherine Connolly announcing her withdrawal from the presidential race.³⁷⁵

The disinformation campaign surrounding the Irish Presidential election highlights the need for a cohesive and well-calibrated response. Addressing disinformation requires a broader democratic resilience approach. This includes the removal of demonstrably false content, the active promotion and amplification of verified information, support for independent journalism, media literacy initiatives, institutional cooperation, and public trust-building measures.³⁷⁶

In practice, however, major platforms have tended to prioritise content removal and risk avoidance over investing in the systems and expertise necessary to verify and amplify trustworthy information. In the Irish political context, this approach ultimately resulted in the widespread suspension of online political advertising on most of the major platforms. This preference for risk avoidance became particularly apparent in relation to political advertising. Rather than investing in compliance systems capable of meeting new transparency obligations, several major platforms chose to suspend political advertising altogether.

Therefore, efforts to regulate political advertising with the aim of increasing transparency and safeguarding electoral fairness and integrity have, in practice, been undermined by the response of most of the major platforms. Rather than implementing the measures necessary to comply with the regulatory framework, several platforms chose to suspend political advertising completely, limiting the ability of established political parties to campaign online.

The effective removal of political advertising from online platforms is not the only challenge facing election integrity, as candidates themselves remain vulnerable to harassment and the circulation of false narratives about their characters. Coimisiún na Meán conducted research into election candidates' online experiences during the 2024 elections and found that more than 95% of candidates used some form of social media campaigning.³⁷⁷ Candidates surveyed as part of An Coimisiún na Meán's study observed that online harassment was prevalent during the 2024 elections. They also noted that it remains essential to distinguish between genuine political criticism (which should be protected) and abusive or harmful behaviour online.³⁷⁸

374 Aidan O'Brian and Eileen Culloty, 'From Free Speech to Violent Rhetoric: Elon Musk's X as a Threat to Election Integrity: How Conor McGregor's Irish Presidential Ambitions Unfolded on X' (EDMO, September 2025) <<https://edmo.ie/wp-content/uploads/2025/09/Elon-Musk-X-as-a-Threat-to-Election-Integrity.pdf>> accessed 17 December 2025.

375 Kate McDonald, 'AI-Generated Deepfake Videos Target Presidential Election' (RTÉ News, 22 October 2025) <<https://www.rte.ie/news/2025/1022/1539967-ai-generated-presidential-election/>> accessed 11 November 2025; Shane Raymond, 'Convincing AI-Generated Videos and Images Are Flooding Social Media Ahead of the Election' (The Journal, 22 October 2025) <<https://www.thejournal.ie/factcheck-ai-generated-videos-and-images-irish-presidential-race-atas-2025-catherine-connolly-heather-humphreys-6850517-Oct2025/>> accessed 25 May 2026.

376 OECD, *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity* (OECD 2024) 30.

377 Coimisiún na Meán, 'On the Digital Campaign Trail: Election Candidates' Online Experiences in the 2024 Elections' (2025) <https://www.cnam.ie/app/uploads/2025/08/CnaM_On-the-digital-campaign-trail.pdf> accessed 17 December 2025.

378 *ibid* 12.

Academics have cautioned that excessive regulation may risk constraining the public's ability to participate in political debate.³⁷⁹ At the same time, however, insufficient regulation leaves political candidates vulnerable to harassment and disinformation, conditions that may discourage individuals from standing for election. Such outcomes can lead to candidates withdrawing from campaigns, undermining both their individual right to participate in political life and the broader democratic objective of fostering inclusive and representative political engagement.³⁸⁰ Crucially, the public also has a right to be accurately and adequately informed so that they can meaningfully exercise their right to vote, a cornerstone of democratic society. Coimisiún na Meán found that 2% of local election and 5% of general election candidates indicated they would not run again due to the online harassment they suffered during their campaigning.³⁸¹

Discouraging individuals from standing for election is particularly problematic for candidates who are female or from minority backgrounds, as they tend to be disproportionately targeted by sexist or racist harassment.³⁸² An absence of female candidates, or candidates from minority backgrounds, would have serious implications for representative democracy. Research indicates that immigrant populations tend to have lower voter turnout than native populations, with the lack of political representation for their own group being identified as a significant contributing factor.³⁸³ Protecting candidates from harmful online behaviour is therefore essential to ensuring effective political representation across diverse demographic groups.

These experiences demonstrate that the effectiveness of DSA mechanisms depends not only on the design of the regulatory framework but also on the willingness of platforms to invest in meaningful compliance measures.

In response to the growing threat of disinformation, the Irish Government announced plans in 2025 for a national strategy designed to support trustworthy media and counter false or misleading information. The resulting National Counter Disinformation Strategy, published in April 2025, sets out a principled and coordinated approach, recognising that effective counter-disinformation efforts require multiple, mutually reinforcing measures. The strategy aims to address disinformation through a combination of public education initiatives, robust implementation of existing legislation, and enhanced cross-sectoral collaboration. In its first Implementation Update, the National Counter-Information Strategy reported substantive early progress, including the rollout of media literacy training for librarians, Ireland's participation in an OECD Steering Group on information integrity, and cooperation with EU Member States.³⁸⁴

379 Elena Abrusci, 'The UK Online Safety Act, the EU Digital Services Act and Online Disinformation: Is the Right to Political Participation Adequately Protected?' (2024) 16(2) *Journal of Media Law* 440, 447.

380 *ibid* 449; and Coimisiún na Meán, 'On the Digital Campaign Trail: Election Candidates' Online Experiences in the 2024 Elections' (2025) 9.

381 Coimisiún na Meán, 'On the Digital Campaign Trail: Election Candidates' Online Experiences in the 2024 Elections' (2025) 9.

382 Coimisiún na Meán, 'On the Digital Campaign Trail: Election Candidates' Online Experiences in the 2024 Elections' (2025) <https://www.cnam.ie/app/uploads/2025/08/CnaM_On-the-digital-campaign-trail.pdf> accessed 17 December 2025.

383 Lucas Geese, 'Does Descriptive Representation Narrow the Immigrant Gap in Turnout? A Comparative Study across 11 Western European Democracies' (2023) 71(4) *Political Studies* 1277.

384 Department of Culture, Communications and Sport, 'National Counter Disinformation Strategy Implementation Update' (Government of Ireland December 2025) 2.

Election Coordination, Regulatory Preparedness, and Democratic Resilience

A recurring theme within international approaches to safeguarding elections is the recognition that responsibility for protecting electoral processes cannot rest with any single institution.³⁸⁵ Election interference campaigns frequently involve multiple overlapping elements, including misinformation and disinformation, FIMI, cybersecurity threats, AI-generated content, political finance concerns, and attempts to undermine public confidence in electoral administration.³⁸⁶ As a result, several democratic states have adopted coordinated election integrity response mechanisms that bring together regulators, electoral authorities, cybersecurity agencies, law enforcement bodies, online platforms, and civil society organisations.³⁸⁷

One model that has emerged internationally is the establishment of election security or election integrity task forces (EITFs), often supported by election-specific monitoring centres or operational coordination hubs.³⁸⁸ Activated in advance of major electoral events, these structures serve as central points for situational awareness, information exchange, and incident management throughout the electoral period.³⁸⁹ Drawing information from electoral authorities, cybersecurity agencies, online platforms, trusted flaggers, fact-checking organisations, and civil society groups, they enable responsible agencies to assess emerging threats rapidly and coordinate appropriate responses.³⁹⁰ Their purpose is not to moderate political discourse or determine the accuracy of political opinions, but to facilitate timely responses to coordinated attempts to interfere with electoral processes.

Examples of this approach can be observed in a number of jurisdictions. The United States, for example, established extensive election security coordination mechanisms involving the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, intelligence agencies, state election officials, and local election administrators. These arrangements facilitate the sharing of threat intelligence and coordinated responses to election-related cyber and information threats. Similarly, following Russian interference efforts during the 2017 presidential election, France established Viginum, a specialised government body tasked with detecting, monitoring, and analysing foreign digital interference campaigns affecting democratic processes.

At the EU level, similar principles underpin the work of the European Cooperation Network on Elections (ECNE), which promotes cooperation and information exchange between EU Member States in responding to risks to election integrity.

385 European Commission, *Election Integrity Checklist* (European Cooperation Network on Elections 2025) 1, stating that safeguarding electoral integrity requires “a whole-of-government approach” and engagement with “a wide range of stakeholders”.

386 European External Action Service, ‘Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)’ (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 23 July 2026; Council of the European Union, ‘Disinformation and Democratic Resilience’ <<https://www.consilium.europa.eu/en/policies/disinformation-and-democratic-resilience/>> accessed 23 July 2026.

387 Cybersecurity and Infrastructure Security Agency, ‘Election Security is a Partnership’ <<https://www.cisa.gov/election-security-partnership>> accessed 23 July 2026; Fondation Hirondelle, ‘Election Integrity Task Force (EITF) – Côte d’Ivoire/Bangladesh/Peru’ <<https://www.hirondelle.org/en/our-work/projects/topical/governance/election-integrity-task-force-eitf-cote-divoire-bangladesh-peru>> accessed 23 July 2026.

388 Global Media Registry, ‘The Election Integrity Task Force (EITF)’ <<https://www.mediaregistry.org/eitf>> accessed 23 July 2026; Fondation Hirondelle, ‘Election Integrity Task Force (EITF) – Côte d’Ivoire/Bangladesh/Peru’ <<https://www.hirondelle.org/en/our-work/projects/topical/governance/election-integrity-task-force-eitf-cote-divoire-bangladesh-peru>> accessed 23 July 2026.

389 *ibid.*

390 *ibid.*

Beyond these institutional coordination mechanisms, several EU Member States, including France,³⁹¹ Lithuania,³⁹² and the Netherlands,³⁹³ have also developed broader national frameworks to address foreign information manipulation, election interference, and online disinformation. These approaches combine institutional coordination, public resilience measures, media literacy initiatives, and support for trusted sources of information as part of broader efforts to strengthen democratic resilience.³⁹⁴

The principal value of such arrangements lies in their ability to reduce institutional fragmentation and facilitate timely interventions during electoral periods. Election-related misinformation and foreign interference frequently engage the responsibilities of multiple organisations simultaneously,³⁹⁵ and without established coordination mechanisms, information may remain siloed, delaying responses during critical periods.³⁹⁶ Several jurisdictions have therefore adopted expedited response protocols, incorporating designated contact points, information-sharing arrangements, escalation procedures, and agreed thresholds for action.³⁹⁷ These mechanisms support the timely identification of false information relating to voting procedures, candidate eligibility, election results, or AI-generated content, and the dissemination of verified information to mitigate its impact.³⁹⁸

Many of the features evident in these international models are already reflected in Ireland's approach.³⁹⁹ The National Cyber Security Centre conducts election-related risk assessments, while Coimisiún na Meán, An Coimisiún Toghcháin, and the Department of the Taoiseach each have responsibilities relevant to election integrity and counter-disinformation efforts. The National Counter Disinformation Strategy further promotes a whole-of-society approach involving government, regulators, academia, media organisations, and civil society.⁴⁰⁰

However, the current framework remains distributed across multiple institutions. While this reflects the complexity of the issues involved, greater formalisation of coordination arrangements during electoral periods may warrant consideration. A structured election integrity coordination framework could improve information exchange, enable earlier

391 Service de Vigilance et de Protection contre les Ingérences Numériques Étrangères (VIGINUM), 'Viginum' <<https://www.sgdsn.gouv.fr/viginum>> accessed 23 July 2026.

392 Nerijus Maliukevičius, *Fortifying Democracies: Lithuania's Comprehensive Approach to Counter Disinformation and Propaganda* (Geopolitics and Security Studies Center 2024) <https://www.gssc.lt/wp-content/uploads/2024/04/v05_Maliukevicius_Fortifying-Democracies_EN_A4.pdf> accessed 23 July 2026.

393 Government of the Netherlands, 'Tackling Disinformation: Actions and Measures' (12 August 2024) <<https://www.nldigitalgovernment.nl/overview/digitalisation-policy/dossierpostcontext/tackling-disinformation-actions-and-measures/>> accessed 23 July 2026.

394 Nerijus Maliukevičius, *Fortifying Democracies: Lithuania's Comprehensive Approach to Counter Disinformation and Propaganda* (Geopolitics and Security Studies Center 2024) <https://www.gssc.lt/wp-content/uploads/2024/04/v05_Maliukevicius_Fortifying-Democracies_EN_A4.pdf> accessed 23 July 2026; Government of the Netherlands, 'Tackling Disinformation: Actions and Measures' (12 August 2024) <<https://www.nldigitalgovernment.nl/overview/digitalisation-policy/dossierpostcontext/tackling-disinformation-actions-and-measures/>> accessed 23 July 2026.

395 European Commission, 'European Cooperation Network on Elections' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en> accessed 23 July 2026.

396 European Commission, 'European Cooperation Network on Elections' <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en> accessed 23 July 2026.

397 Transparency Centre, Code of Conduct on Disinformation, 'Elections' <<https://disinfocode.eu/elections>> accessed 23 July 2026.

398 US Alliance for Election Excellence, 'Checklist for Combating Election Misinformation' <<https://electionexcellence.org/resources/checklist-for-combating-election-misinformation/>> accessed 23 July 2026.

399 Department of Culture, Communications and Sport, *National Counter Disinformation Strategy* (Government of Ireland 2025) <<https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/national-counter-disinformation-strategy-working-group/>> accessed 23 July 2026.

400 Department of Culture, Communications and Sport, *National Counter Disinformation Strategy* (Government of Ireland 2025) <<https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/national-counter-disinformation-strategy-working-group/>> accessed 23 July 2026; Department of Culture, Communications and Sport, 'Minister O'Donovan Welcomes Publication of National Counter Disinformation Strategy' (17 April 2025) <<https://www.gov.ie/en/department-of-culture-communications-and-sport/press-releases/minister-odonovan-welcomes-publication-of-national-counter-disinformation-strategy/>> accessed 23 July 2026.

identification of emerging threats, support engagement with online platforms, and strengthen the State's ability to respond rapidly to incidents capable of undermining confidence in democratic processes.

Such an approach would be consistent with broader developments across the European Union, where increasing emphasis is being placed on democratic resilience, coordinated risk mitigation, and whole-of-government responses to foreign information manipulation and interference.⁴⁰¹ Given Ireland's prominent role in the implementation and enforcement of the DSA, the development of formal election response mechanisms would further strengthen the State's capacity to address evolving risks while respecting fundamental rights and democratic freedoms.

The State's efforts to counter online election interference across multiple fronts are encouraging. Although available evidence suggests that online false information has not materially altered electoral outcomes in Ireland, its continued proliferation risks weakening public confidence in democratic institutions and electoral processes.⁴⁰² From targeted disinformation campaigns to the erosion of trust in traditional media and official sources, and the harassment of electoral candidates, malicious actors continue to exploit digital technologies in new and evolving ways.⁴⁰³ Maintaining electoral integrity therefore requires not only effective regulation, but also sustained coordination, institutional preparedness, and investment in democratic resilience.



Leinster House, Dublin. Both the lower (Dail) and higher (Seanad) chamber meet here. (Image: Shutterstock)

401 Council of the European Union, 'Disinformation and Democratic Resilience' <<https://www.consilium.europa.eu/en/policies/disinformation-and-democratic-resilience/>> accessed 23 July 2026; European External Action Service, 'Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)' (17 March 2026) <https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en> accessed 23 July 2026.

402 Department of Culture, Communications and Sport, 'National Counter Disinformation Strategy Working Group' <<https://www.gov.ie/en/department-of-culture-communications-and-sport/publications/national-counter-disinformation-strategy-working-group/>> accessed 23 July 2026; Department of Housing, Local Government and Heritage, 'Minister O'Brien and Minister Noonan Welcome the Publication of New Electoral Commission Guide on Disinformation' (24 April 2024) <<https://www.gov.ie/en/department-of-housing-local-government-and-heritage/press-releases/minister-obrien-and-minister-noonan-welcome-the-publication-of-new-electoral-commission-guide-on-disinformation/>> accessed 23 July 2026.

403 EDMO Ireland, 'Platforms Failing on Electoral Integrity: EDMO Ireland's Initial Findings' (EDMO, 25 October 2025) <<https://edmohub.ie/index.php/platforms-failing-on-electoral-integrity-edmo-irelands-initial-findings/>> accessed 19 January 2026.

Data Access, Research Capacity, and Election Monitoring

Effective responses to misinformation and disinformation depend not only on regulation and institutional coordination, but also on access to reliable evidence regarding how information spreads through online platforms.⁴⁰⁴ Historically, researchers, regulators, journalists, and civil society organisations have faced significant difficulties in assessing the scale and impact of online election interference due to limited access to platform data.⁴⁰⁵ Much of the information necessary to understand how content is amplified, targeted, or recommended remains under the control of private technology companies, creating challenges for independent scrutiny and evidence-based policymaking.⁴⁰⁶

The DSA represents a significant development in this regard. Recognising the importance of independent oversight, Articles 40 and 41 establish mechanisms intended to provide qualified researchers with access to data held by VLOPs and very large online search engines (VLOSEs). This framework enables researchers, subject to appropriate safeguards, to obtain access to platform data for the purpose of investigating systemic risks, including risks to civic discourse, electoral processes, public security, and fundamental rights.

The researcher access provisions reflect an important shift in regulatory philosophy. Rather than relying exclusively upon information disclosed voluntarily by platforms, the DSA seeks to facilitate independent examination of online systems and their effects on democratic processes. By enabling academic institutions and approved researchers to analyse platform data, policymakers may obtain a more comprehensive understanding of issues such as disinformation campaigns, coordinated inauthentic behaviour, algorithmic amplification, political advertising practices, and foreign information manipulation and interference.⁴⁰⁷

In relation to election integrity, access to platform data is particularly valuable because many forms of online interference are not fully visible through publicly available information. Electoral misinformation campaigns may rely on recommendation systems, targeted advertising, coordinated networks of accounts, and private forms of online coordination.⁴⁰⁸ Access to relevant platform data therefore assists researchers in assessing the scale of such activity and evaluating the effectiveness of regulatory interventions designed to address it.⁴⁰⁹

404 Yasmin Green and others, *Evidence-Based Misinformation Interventions: Challenges and Opportunities for Measurement and Collaboration* (Carnegie Endowment for International Peace 2023) <<https://carnegieendowment.org/research/2023/01/evidence-based-misinformation-interventions-challenges-and-opportunities-for-measurement-and-collaboration>> accessed 23 July 2026.

405 Philipp Darius and others, 'Election Research in the Age of Regulated Data Access under the EU Digital Services Act' (2026) 15(1) Internet Policy Review <<https://policyreview.info/articles/analysis/election-research-data-access-dsa>> accessed 23 July 2026.

406 John Albert, 'A Guide to the EU's New Rules for Researcher Access to Platform Data' (AlgorithmWatch, 7 December 2022) <<https://algorithmwatch.org/en/dsa-data-access-explained/>> accessed 23 July 2026.

407 Anna Liesenfeld, Herwig CH Hofmann, and Felix Pflücke, 'The Legal Significance of Independent Research based on Article 40 DSA for the Management of Systemic Risks in the Digital Services Act' (2025) 16(1) European Journal of Risk Regulation 184 <<https://doi.org/10.1017/err.2024.61>> accessed 23 July 2026.

408 John Albert, 'A Guide to the EU's New Rules for Researcher Access to Platform Data' (AlgorithmWatch, 7 December 2022) <<https://algorithmwatch.org/en/dsa-data-access-explained/>> accessed 23 July 2026.

409 Philipp Darius and others, 'Election Research in the Age of Regulated Data Access under the EU Digital Services Act' (2026) 15(1) Internet Policy Review <<https://policyreview.info/articles/analysis/election-research-data-access-dsa>> accessed 23 July 2026; European Commission Joint Research Centre, 'FAQs: DSA Data Access for Researchers' (3 July 2025) <https://algorithmic-transparency.ec.europa.eu/news/faqs-dsa-data-access-researchers-2025-07-03_en> accessed 23 July 2026.

The DSA framework also highlights the growing importance of independent election-monitoring infrastructure. Traditionally, election monitoring focused primarily on polling stations, counting procedures, campaign finance reporting, and electoral administration.⁴¹⁰ Contemporary threats increasingly occur in digital environments, requiring new forms of monitoring and analysis. Independent monitoring of online information environments can assist in identifying emerging disinformation narratives, coordinated influence operations, deceptive AI-generated content, and threats to public confidence in electoral processes.⁴¹¹ Such monitoring can also support rapid-response frameworks by providing early warning of emerging risks.⁴¹²

Academic institutions have an important role to play within this ecosystem. Universities and research organisations frequently possess expertise in areas including digital communications, political behaviour, cybersecurity, artificial intelligence, and information integrity.⁴¹³ Partnerships between regulators, electoral authorities, research institutions, and civil society organisations can strengthen analytical capacity while maintaining appropriate independence from both government and industry.⁴¹⁴ Such partnerships may also facilitate the development of evidence-based responses to emerging threats and improve understanding of the effectiveness of existing regulatory measures.⁴¹⁵

Ireland is particularly well positioned to benefit from this approach given its central role in European digital regulation. As many of the world's largest online platforms maintain their European headquarters within the State, Irish institutions occupy a unique position in the implementation and oversight of the DSA framework. Coimisiún na Meán, universities, research centres, and initiatives such as the European Digital Media Observatory (EDMO) already contribute to understanding the evolving information environment.⁴¹⁶ However, the long-term effectiveness of election integrity policies will depend upon sustained investment in research capability and access to reliable data regarding the operation of digital platforms.

Evidence-based policymaking is especially important in the field of election integrity because many assumptions regarding misinformation and disinformation remain contested.⁴¹⁷ While concerns regarding online manipulation are well founded, the precise

410 OSCE Office for Democratic Institutions and Human Rights, *Handbook for the Observation of Election Administration* (OSCE 2023) <<https://odihr.osce.org/sites/default/files/f/documents/0/4/544240.pdf>> accessed 23 July 2026.

411 International IDEA, 'The Information Environment Around Elections' <<https://www.idea.int/theme/information-communication-and-technology-electoral-processes/information-environment-around-elections>> accessed 23 July 2026.

412 David Levine and others, *Building Resilience Against Election Influence Operations: Preparing for the European Elections in 2024 and Beyond* (IFES 2024) <<https://www.ifes.org/pub/building-resilience-against-election-influence-operations/-case-studies>> accessed 23 July 2026.

413 UNESCO, *Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multi-Stakeholder Approach* (UNESCO 2023) <<https://www.unesco.org/en/internet-trust/guidelines>> accessed 23 July 2026.

414 *ibid*; Craig Matasick, Carlotta Alfonsi and Alessandro Bellantoni, 'Governance Responses to Disinformation: How Open Government Principles Can Inform Policy Options' (OECD Working Papers on Public Governance No 39, OECD Publishing 2020) <<https://doi.org/10.1787/d6237c85-en>> accessed 23 July 2026.

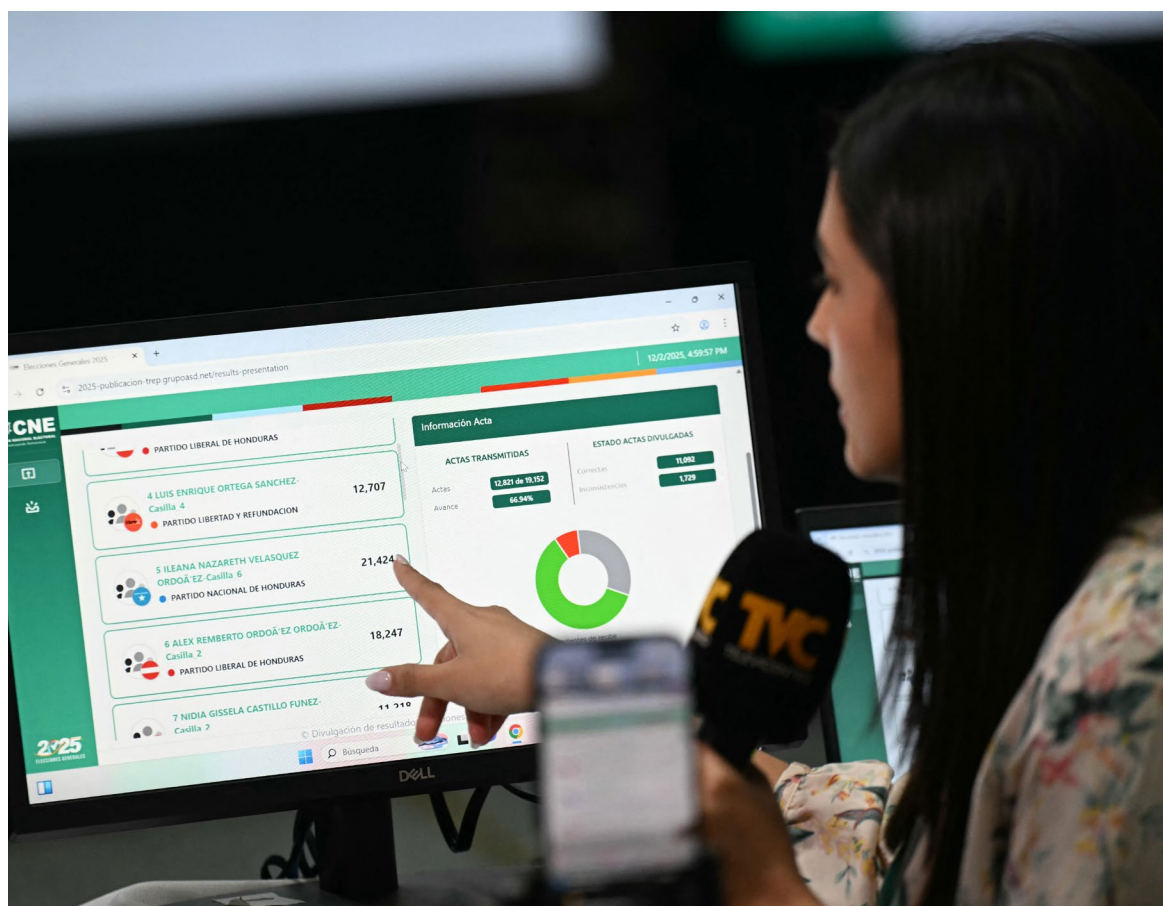
415 Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Carnegie Endowment for International Peace 2024) <<https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide>> accessed 23 July 2026.

416 European Commission, 'European Digital Media Observatory (EDMO)' <<https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>> accessed 23 July 2026; European Digital Media Observatory, 'Our Vision and Mission' <<https://edmo.eu/about-us/edmoeu/our-vision-and-mission/>> accessed 23 July 2026.

417 Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Carnegie Endowment for International Peace 2024) <<https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide>> accessed 23 July 2026; Yasmin Green and others, *Evidence-Based Misinformation Interventions: Challenges and Opportunities for Measurement and Collaboration* (Carnegie Endowment for International Peace 2023) <<https://carnegieendowment.org/research/2023/01/evidence-based-misinformation-interventions-challenges-and-opportunities-for-measurement-and-collaboration>> accessed 23 July 2026.

impact of different forms of online content on electoral outcomes remains the subject of ongoing research.⁴¹⁸ Policies that are not supported by robust evidence may risk either overestimating or underestimating particular threats. Strengthening research capacity therefore contributes not only to regulatory effectiveness but also to ensuring that interventions remain proportionate, targeted, and consistent with fundamental rights.

As digital technologies continue to evolve, the ability of researchers and independent institutions to examine online information ecosystems will become increasingly important. Access to reliable platform data, robust election monitoring infrastructure, and sustained cooperation between regulators and academic institutions should therefore be regarded as essential components of long-term democratic resilience and election integrity.



A member of the media looks at the screen showing the official recount in a presidential election. (Photo by Marvin RECINOS / AFP via Getty Images)

418 Jon Bateman and Dean Jackson, *Countering Disinformation Effectively: An Evidence-Based Policy Guide* (Carnegie Endowment for International Peace 2024) <<https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide>> accessed 23 July 2026; Matthew Leake, 'Are Fears About Online Misinformation in the US Election Overblown? The Evidence Suggests They Might Be' (Reuters Institute for the Study of Journalism, 24 October 2024) <<https://reutersinstitute.politics.ox.ac.uk/news/are-fears-about-online-misinformation-us-election-overblown-evidence-suggests-they-might-be>> accessed 23 July 2026.

Strengthening Democratic Resilience

Media Pluralism and the Democratic Function of Journalism

While considerable attention has been devoted to regulating online platforms and addressing misinformation and disinformation, independent journalism remains a central institution within democratic societies. Independent journalism performs a critical democratic function by investigating public affairs, scrutinising political actors, verifying claims, and providing voters with information necessary for informed participation in elections.⁴¹⁹

The role of journalism in protecting election integrity extends beyond the verification of individual claims. Independent news organisations perform a vital democratic function by scrutinising government and political actors, facilitating informed public debate, and ensuring that citizens have access to the information necessary to participate meaningfully in democratic processes. In so doing, journalism contributes not only to information accuracy but also to transparency, accountability, and public trust in democratic institutions.⁴²⁰

Media pluralism is an important safeguard against information manipulation.⁴²¹ Where citizens have access to a diverse range of independent and pluralistic media sources, it becomes more difficult for any individual actor (whether governmental, political, commercial, or foreign) to dominate public discourse, shape electoral narratives unchallenged, or manipulate the information environment without scrutiny and contestation.⁴²²

The sustainability of journalism has become an increasingly significant policy concern in the digital era.⁴²³ Traditional revenue models that supported investigative and local journalism have been disrupted by the growth of digital platforms, which now capture a substantial share of advertising revenues.⁴²⁴ This creates a significant democratic paradox: at precisely the moment when societies are facing increasing volumes of misinformation, disinformation, and information manipulation, many of the institutions responsible for independent verification, investigative reporting, and public interest journalism are experiencing growing economic and financial pressures.⁴²⁵

419 UNESCO, 'Media and Elections' <<https://www.unesco.org/en/freedom-expression-rule-law/media-elections>> accessed 23 July 2026; UNESCO, World Trends Report on Freedom of Expression and Media Development 2022–2025: Journalism, Shaping a World at Peace (UNESCO 2025) <<https://www.unesco.org/en/world-media-trends>> accessed 23 July 2026.

420 UNESCO, World Trends Report on Freedom of Expression and Media Development 2022–2025: Journalism, Shaping a World at Peace (UNESCO 2025) <<https://www.unesco.org/en/world-media-trends>> accessed 23 July 2026; Council of Europe, 'Media - Freedom of Expression' <<https://www.coe.int/en/web/freedom-expression/media>> accessed 23 July 2026.

421 UNESCO, 'Media Pluralism' <<https://www.unesco.org/en/media-pluralism-diversity/media-pluralism>> accessed 23 July 2026; UNESCO, 'Media Pluralism and Diversity' <<https://www.unesco.org/en/media-pluralism-diversity>> accessed 23 July 2026.

422 Steering Committee on Media and Information Society, *Resisting Disinformation: Ten Building Blocks to Strengthen Information Integrity* (Council of Europe, 2026) <<https://edoc.coe.int/en/media/12547-resisting-disinformation-ten-building-blocks-to-strengthen-information-integrity.html>> accessed 23 July 2026; UNESCO, 'Media Pluralism' <<https://www.unesco.org/en/media-pluralism-diversity/media-pluralism>> accessed 23 July 2026.

423 UNESCO, 'Media Viability' <<https://www.unesco.org/en/international-programme-development-communication/media-viability>> accessed 23 July 2026; European Commission, 'Media Freedom and Pluralism' <<https://digital-strategy.ec.europa.eu/en/policies/media-freedom>> accessed 23 July 2026.

424 UNESCO, 'Media Viability' <<https://www.unesco.org/en/international-programme-development-communication/media-viability>> accessed 23 July 2026; European Commission, 'Media Freedom and Pluralism' <<https://digital-strategy.ec.europa.eu/en/policies/media-freedom>> accessed 23 July 2026.

425 UNESCO, 'Media Viability' <<https://www.unesco.org/en/international-programme-development-communication/media-viability>> accessed 23 July 2026; UNESCO, 'UNESCO Works to Counter Mis- and Disinformation' (2022) <<https://unesdoc.unesco.org/ark:/48223/pf0000382385.locale=en>> accessed 23 July 2026; UN News, 'UNESCO Launches Consultation on Fair Payment for News in the Digital Age' (19 June 2026) <<https://news.un.org/en/story/2026/06/1167771>> accessed 23 July 2026.

Such pressures have been directly acknowledged by Coimisiún na Meán, most recently in its revised Media Pluralism Policy, published in August 2026.⁴²⁶ Recognising the importance of a diverse, inclusive, and trusted media ecosystem in the context of rapid technological change, the revised policy focuses on measures designed to support editorial independence, enhance media transparency, facilitate regulatory compliance, and protect the right to freedom of expression.⁴²⁷ It further emphasises the importance of sustaining local, community, and independent media services, recognising that media pluralism strengthens social inclusion, enriches public debate, and supports effective democratic participation.⁴²⁸

Supporting a sustainable, independent, and pluralistic media sector should be regarded as a core element of democratic resilience.⁴²⁹ Efforts to safeguard election integrity are unlikely to succeed if the institutions responsible for informing the public, scrutinising power, and facilitating democratic debate are themselves weakened. Election integrity depends not only on protecting elections from interference, but also on maintaining the wider democratic ecosystem within which elections take place.⁴³⁰

Media Literacy and Public Resilience

Regulatory interventions and platform governance measures alone cannot fully address the challenges posed by misinformation, disinformation, and FIMI. Democratic resilience also depends on the capacity of citizens to critically evaluate information, identify misleading content, and engage effectively with increasingly complex digital information environments.⁴³¹ Consequently, media literacy has emerged as an important component of contemporary election integrity strategies.

In Ireland, Coimisiún na Meán has been assigned a central role in promoting media literacy and supporting public understanding of the digital information environment.⁴³² Through its Media Literacy Ireland initiative and broader public awareness activities, it seeks to enhance citizens' capacity to critically assess online content, recognise manipulative information practices, and engage safely in digital spaces.⁴³³ Such initiatives recognise that resilience to misinformation cannot be achieved solely through content moderation or legal enforcement, but also requires strengthening the public's ability to evaluate information independently.

Similar objectives can be observed at the European level. The EDMO coordinates cooperation between researchers, fact-checkers, media organisations, and other

426 Coimisiún na Meán, *Media Pluralism Policy* (Coimisiún na Meán 2026) <https://www.cnam.ie/app/uploads/2026/07/23227-CnaM-Media-Pluralism-Policy_ENG_FINAL_web.pdf> accessed 14 August 2026.

427 *ibid.*

428 *ibid.* 10.

429 UNESCO, 'Media Viability' <<https://www.unesco.org/en/international-programme-development-communication/media-viability>> accessed 23 July 2026; United Nations, 'United Nations Global Principles for Information Integrity' <<https://www.un.org/en/information-integrity/global-principles>> accessed 23 July 2026; Council of Europe, *Resisting Disinformation: Ten Building Blocks to Strengthen Information Integrity* (2026) <<https://edoc.coe.int/en/media/12547-resisting-disinformation-ten-building-blocks-to-strengthen-information-integrity.html>> accessed 23 July 2026.

430 International IDEA, 'Electoral Processes' <<https://www.idea.int/theme/electoral-processes>> accessed 23 July 2026.

431 UNESCO, 'Media and Information Literacy' <<https://www.unesco.org/en/media-information-literacy>> accessed 23 July 2026; UNESCO, *Media and Information Literate Citizens: Think Critically, Click Wisely!* (UNESCO 2021) <<https://www.unesco.org/en/articles/media-and-information-literate-citizens>> accessed 23 July 2026.

432 Coimisiún na Meán's media literacy mandate is derived from the Broadcasting Act 2009, as amended by the Online Safety and Media Regulation Act 2022, which empowers the Commission to undertake, encourage and foster research and activities promoting media literacy.

433 Media Literacy Ireland, 'What is Media Literacy Ireland?' <<https://www.medialiteracyireland.ie/>> accessed 24 July 2026; Coimisiún na Meán, 'Understanding Media' <<https://www.cnam.ie/general-public/guides-resources/understanding-media/>> accessed 24 July 2026.

stakeholders to monitor disinformation trends, support media literacy initiatives, and improve understanding of evolving information threats.⁴³⁴ By combining research, fact-checking, and public education, EDMO seeks to strengthen societal resilience against disinformation while respecting freedom of expression and democratic values.⁴³⁵

Increasing attention has also been given to so-called “prebunking” strategies.⁴³⁶ Drawing upon the psychological theory of inoculation, prebunking seeks to expose individuals to common manipulation techniques before they encounter misleading content in practice.⁴³⁷ Research suggests that such interventions can improve resilience to misinformation by helping users to recognise tactics such as emotional manipulation, false dichotomies, scapegoating, and conspiracy-based narratives before they are exposed to them in real-world contexts.⁴³⁸ Rather than correcting false claims after they have spread, prebunking aims to equip individuals with the skills necessary to identify and resist manipulation in advance.⁴³⁹

Public awareness initiatives similarly form part of a broader resilience-based approach to election integrity.⁴⁴⁰ Campaigns designed to increase public understanding of disinformation techniques, AI-generated content, foreign influence operations, and deceptive online practices can reduce the effectiveness of attempts to manipulate public opinion during electoral periods.⁴⁴¹ While no single intervention can eliminate the risks posed by misinformation and disinformation, media literacy, prebunking, and public awareness measures contribute to a more informed electorate and a more resilient democratic environment.⁴⁴²

These initiatives reflect a growing recognition that election integrity depends not only on regulating platforms and responding to harmful content, but also on empowering citizens to navigate the digital information ecosystem. Strengthening public resilience through media literacy and civic awareness therefore represents an increasingly important complement to legal, regulatory, and institutional responses to contemporary information threats.

434 European Commission, ‘European Digital Media Observatory (EDMO)’ (Shaping Europe’s Digital Future) <<https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>> accessed 24 July 2026; European Digital Media Observatory, ‘Homepage’ <<https://edmo.eu/>> accessed 24 July 2026.

435 European Commission, ‘European Digital Media Observatory (EDMO)’ (Shaping Europe’s Digital Future) <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory> accessed 24 July 2026.

436 Joint Research Centre, ‘Misinformation and Disinformation: Both Prebunking and Debunking Work for Fighting It’ (25 October 2024) <https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-both-prebunking-and-debunking-work-fighting-it-2024-10-25_en> accessed 24 July 2026.

437 Joint Research Centre, ‘Misinformation and Disinformation: Both Prebunking and Debunking Work for Fighting It’ (25 October 2024) <https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-both-prebunking-and-debunking-work-fighting-it-2024-10-25_en> accessed 24 July 2026.

438 Jon Roozenbeek, Thomas Nygren, and Sander van der Linden, ‘Prebunking Interventions Based on the Psychological Theory of “Inoculation” Can Reduce Susceptibility to Misinformation Across Cultures’ (2020) *Harvard Kennedy School Misinformation Review* <<https://misinfreview.hks.harvard.edu/article/global-vaccination-badnews/>> accessed 24 July 2026; Truth Labs for Education, ‘Inoculation Science: Video Resources’ <<https://inoculation.science/inoculation-videos/>> accessed 24 July 2026.

439 Jon Roozenbeek, Thomas Nygren, and Sander van der Linden, ‘Prebunking Interventions Based on the Psychological Theory of “Inoculation” Can Reduce Susceptibility to Misinformation Across Cultures’ (2020) *Harvard Kennedy School Misinformation Review* <<https://misinfreview.hks.harvard.edu/article/global-vaccination-badnews/>> accessed 24 July 2026; Truth Labs for Education, ‘Inoculation Science: Video Resources’ <<https://inoculation.science/inoculation-videos/>> accessed 24 July 2026.

440 Alexander Románishyn, ‘Enhancing Election Integrity by Strengthening EU Defences Against Disinformation’ (Martens Centre, 26 June 2024) 17 <<https://www.martenscentre.eu/publication/enhancing-election-integrity-by-strengthening-eu-defences-against-disinformation/>> accessed 24 July 2026.

441 *ibid.*

442 European Commission, ‘EU Funding of €5 Million to Strengthen Media Literacy and Resilience to Disinformation’ (30 April 2025) <<https://digital-strategy.ec.europa.eu/en/news/eu-funding-eu5-million-strengthen-media-literacy-and-resilience-disinformation>> accessed 24 July 2026; European Digital Media Observatory, ‘Media Literacy’ <<https://edmo.eu/areas-of-activities/media-literacy/>> accessed 24 July 2026; Joint Research Centre, ‘Misinformation and Disinformation: Both Prebunking and Debunking Work for Fighting It’ (25 October 2024) <https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/misinformation-and-disinformation-both-prebunking-and-debunking-work-fighting-it-2024-10-25_en> accessed 24 July 2026.

Recommendations





Recommendations

This Discussion Paper examines threats to election integrity arising from coordinated disinformation campaigns by malicious actors, the rapid spread of false information through digital technologies, AI-generated misleading content, limited transparency and accountability for creators of illegal content, and the algorithmic amplification of deceptive material.

In addition, the analysis considers the current legal framework at both European Union and national (Irish) levels for tackling the rise of false information online. While not specific to election-related content, this broader framework provides an important backdrop to efforts aimed at protecting election integrity.

The EU Digital Services Act (DSA), together with Ireland's national implementing legislation, has significantly strengthened the regulation of very large online platforms (VLOPs) and very large online search engines (VLOSEs) by imposing heightened obligations to address illegal and misleading content shared on their platforms. As Ireland hosts the European headquarters of many services that have been designated as VLOPs and VLOSEs, it is well placed to demonstrate strategic leadership in the regulation of harmful and misleading online content, with countering online election interference representing a critical component of this broader role. The designation of Coimisiún na Meán as Digital Services Coordinator (DSC) positions it as the *de facto* regulatory authority for those platforms within the EU.

The recent establishment of Oifig IS na hÉireann (the AI Office of Ireland) under the Regulation of Artificial Intelligence Act 2026 further strengthens Ireland's institutional capacity in this area. Given the increasing role of AI-generated content, synthetic media, and automated information manipulation in electoral contexts, effective cooperation between Coimisiún na Meán, An Coimisiún Toghcháin, and Oifig IS na hÉireann will be an important component of Ireland's broader election integrity framework.

Building on this analysis, the following recommendations are informed by identified gaps in the implementation of the DSA, the evolving nature of online electoral risks, and the current institutional landscape in Ireland. They are designed to be operationally deliverable within existing mandates, with clearly defined responsibilities and implementation pathways.

Recommendation 1: Expansion of the Trusted Flagger Network

Lead Authority: Coimisiún na Meán

Key Stakeholders: Oifig IS na hÉireann, An Coimisiún Toghcháin

Coimisiún na Meán should, in its capacity as Digital Services Coordinator, continue to expand the number and diversity of the entities designated as trusted flaggers under Article 22 of the DSA, with particular emphasis on areas relevant to election integrity, digital disinformation, and foreign information manipulation and interference (FIMI).

This should include:

- The publication of targeted calls for applications from organisations with expertise in election integrity, digital misinformation, and AI-generated content;
- The development of specialist accreditation pathways for organisations operating in areas of public interest, including elections and civic participation;
- The provision of guidance and technical support to applicants to facilitate compliance with the statutory criteria for trusted flagger status;
- The introduction of periodic transparency reporting on the operation, performance, and impact of the trusted flagger system; and
- The regular review of sectoral coverage to identify gaps in expertise and to ensure that emerging online harms are adequately addressed.

In identifying gaps in trusted flagger coverage, Coimisiún na Meán should consult with Oifig IS na hÉireann regarding emerging risks associated with AI systems, synthetic media, and AI-enabled information manipulation.

This measure is intended to build upon the recent expansion of Ireland's trusted flagger network and to ensure that appropriate expertise exists across all significant categories of illegal and harmful online content and emerging digital risks.

Explanation and Rationale

The effectiveness of the DSA, and of Ireland's national framework for implementing and enforcing it, remains to be fully tested. Many of the legal challenges to date (such as those initiated by *Amazon EU Sàrl* and *Zalando*) have focused on contesting the designation of certain services as VLOPs or VLOSEs rather than on compliance with the substantive obligations imposed by the DSA. Because the DSA imposes enhanced obligations on designated services, concerns remain that influential but non-designated services may continue to play a significant role in shaping public discourse while being subject to less demanding regulatory requirements. The existing framework also places

the initial responsibility for addressing disinformation on VLOPS and VLOSEs, with regulatory authorities performing oversight and enforcement functions. The trusted flagger mechanism is intended to support this arrangement by enabling independent expert organisations to assist in the identification of illegal content and to provide regulators with valuable information regarding emerging risks.

Recent developments have strengthened Ireland's implementation of the trusted flagger mechanism. As already discussed, in June 2026, Coimisiún na Meán granted trusted flagger status to the Irish Internet Hotline, the Irish Music Rights Organisation, and the Jewish Representative Council of Ireland, significantly expanding the range of expertise available within the trusted flagger network. The network now encompasses areas including child sexual abuse material, non-consensual intimate image sharing, racism, xenophobia, copyright infringement, financial fraud, and illegal antisemitic content.⁴⁴³

However, an important gap remains. Ireland does not yet have an accredited trusted flagger that has a specific remit relating to election integrity, political disinformation, or FIMI. Given the increasing use of digital platforms, algorithmic amplification, and AI-generated content in electoral contexts, there is a compelling case for accrediting organisations with specialist expertise in protecting democratic processes and identifying content that may undermine election integrity.

The case for specialist election integrity trusted flaggers is strengthened further by the growing use of generative AI (GenAI) and synthetic media during electoral campaigns. As discussed previously, malicious actors can now produce highly convincing AI-generated images, audio recordings, and videos that falsely depict candidates saying or doing things that never occurred. While the AI Act introduces transparency obligations requiring certain AI-generated content and deepfakes to be disclosed as such, significant challenges remain regarding the identification, attribution, and verification of deceptive synthetic media. Organisations possessing specialist expertise in AI-enabled misinformation, digital forensics, and synthetic media analysis may therefore provide valuable support to both online platforms and regulators in identifying malicious deepfakes and other forms of AI-generated electoral manipulation before they achieve significant reach or influence.

Continued expansion of the trusted flagger network should therefore be pursued as a means of strengthening Ireland's capacity to support the implementation of the DSA. Trusted flaggers should also operate with a high degree of transparency regarding the content they report and the outcomes of those reports.⁴⁴⁴ Increased transparency would enable Coimisiún na Meán to provide meaningful public scrutiny of DSA implementation, assess how online services are responding to trusted flagger reports, and identify emerging risks within the online information environment.

443 Coimisiún na Meán, 'Trusted Flagger Status Granted to Three New Organisations' (Coimisiún na Meán, 25 June 2026 <<https://www.cnam.ie/trusted-flagger-status-granted-to-three-new-organisations/>> accessed 7 July 2026).

444 Jacob van de Kerkhof, 'Article 22 Digital Services Act: Building trust with trusted flaggers' (2025) 14(1) Internet Policy Review 1, 9.

Recommendation 2: Structured Engagement with Online Platforms on Political Advertising

Lead Authority: Coimisiún na Meán

Key Stakeholders: An Coimisiún Toghcháin, Data Protection Commission, relevant Government Departments

Coimisiún na Meán, working in close cooperation with An Coimisiún Toghcháin and other competent authorities, should establish a formalised engagement mechanism with VLOPs and VLOSEs headquartered in Ireland to support compliance with obligations relating to political advertising under the DSA and the EU Political Advertising framework.

This should include:

- The establishment of a standing regulatory platform forum on election integrity;
- The issuance of clear guidance on transparency requirements for political advertising;
- The development of standardised compliance templates, including political advertising repositories; and
- The facilitation of a phased reintroduction of political advertising, subject to demonstrable compliance.

The objective of this engagement is to ensure the availability of transparent, verifiable political information online while maintaining the integrity of regulatory safeguards.

Explanation and Rationale

Ensuring that the public has access to information directly from political parties, together with clear context and disclosure of sponsors of political advertising, is an important safeguard against the spread of false or misleading narratives about political figures in the digital space.⁴⁴⁵ Although a 2020 consultation conducted by the UK Government found that voters value transparency regarding the source of political information,⁴⁴⁶ the applicability of these findings to the Irish context is necessarily limited, given differences in electoral regulation, media ecosystems, and public attitudes. Nevertheless, the underlying principle, that transparency supports informed decision making, remains relevant.

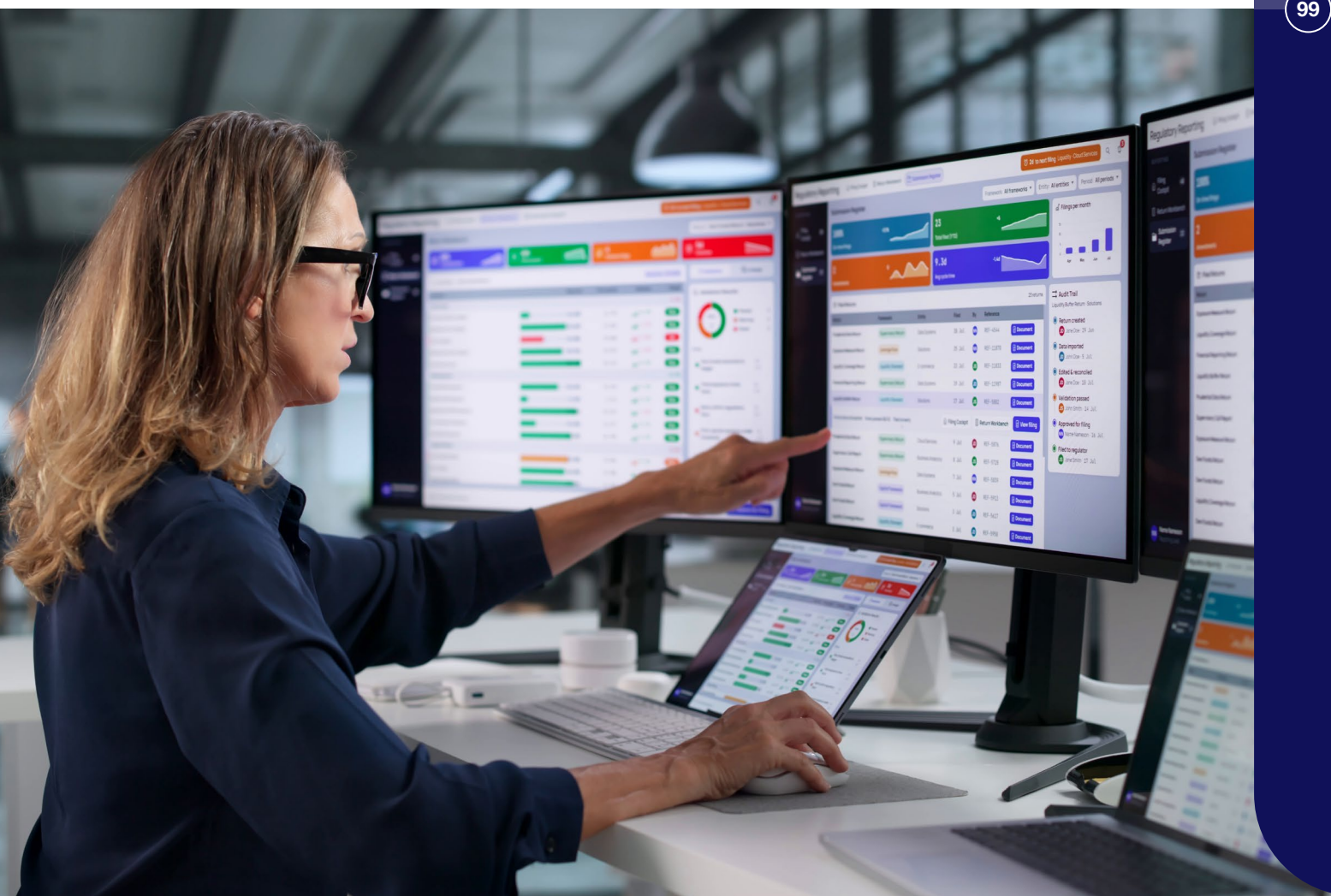
⁴⁴⁵ Cabinet Office, 'Transparency in digital campaigning' (UK Government, 12 August 2020) <<https://www.gov.uk/government/consultations/transparency-in-digital-campaigning-technical-consultation-on-digital-imprints>> accessed 19 January 2026.

⁴⁴⁶ Cabinet Office, Digital Imprints: Government Consultation Response (UK Government, 15 June 2021) 8-9, noting broad support for measures designed to improve transparency in online political campaigning and help voters identify the source of political material, available at <<https://www.gov.uk/government/consultations/transparency-in-digital-campaigning-technical-consultation-on-digital-imprints>> accessed 24 July 2026.

In the Irish context, the suspension of political advertising by several VLOPs and VLOSEs has restricted the availability of verified political information online. While platforms have cited administrative complexity in complying with the DSA, such concerns cannot outweigh their legal obligations, particularly given the scale, resources, and systemic influence that these platforms have.

Coimisiún na Meán should lead structured engagement with platforms to clarify compliance expectations and reduce procedural ambiguity, drawing on support from relevant Government Departments where necessary, while fully upholding the integrity of the DSA's transparency and accountability requirements. This approach would support the responsible restoration of political advertising without compromising the regulatory standards designed to protect the public from harmful or misleading content.

Given the overlap between platform regulation, election integrity, and political advertising transparency, implementation should be coordinated through the existing statutory cooperation arrangements between Coimisiún na Meán, An Coimisiún Toghcháin, and the Data Protection Commission.



Recommendation 3: Alignment of Part 5 of the Electoral Reform Act 2022 with the Digital Services Act

Lead Authorities: Department of Housing, Local Government and Heritage and Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media

Key Stakeholders: An Coimisiún Toghcháin, Coimisiún na Meán, Data Protection Commission, the Attorney General

Prior to the commencement of Part 5 of the Electoral Reform Act 2022, a joint statutory review should be undertaken to ensure full alignment with Ireland's obligations under the DSA.

This review should:

- Clearly delineate the respective roles of Coimisiún na Meán and An Coimisiún Toghcháin in relation to online electoral information;
- Identify and eliminate risks of regulatory duplication, inconsistency, or fragmentation;
- Provide for formal cooperation and data-sharing arrangements between the relevant bodies;
- Assess whether the definitions of 'misinformation' and 'disinformation' contained within Part 5 remain appropriate and necessary in light of developments in EU law and the contemporary digital regulatory framework; and
- Ensure that any future regulatory framework contains appropriate safeguards for freedom of expression and complies with relevant constitutional, ECHR, and EU fundamental rights standards.

Where necessary, legislative amendments should be introduced prior to commencement to ensure coherence, legal certainty, and respect for fundamental rights within Ireland's regulatory framework.

Explanation and Rationale

While both Coimisiún na Meán and An Coimisiún Toghcháin have responsibilities for preserving the integrity of elections, the implementation of the DSA requires that both bodies have clearly delineated functions to prevent regulatory fragmentation and duplication of work. Amendment or replacement of Part 5 of the Electoral Reform Act 2022 should be considered to align with the DSA, while fulfilling the objectives to be achieved by Part 5 concerning the regulation of online electoral information and misinformation and disinformation.

The non-commencement of Part 5 creates uncertainty regarding the precise role that An Coimisiún Toghcháin will ultimately play in the regulation of online electoral information and the governance of misinformation and disinformation. However, although aspects of the electoral integrity framework envisaged by the Electoral Reform Act 2022 remain unimplemented, the broader regulatory landscape has developed significantly since the Act's enactment. The DSA, the AI Act, and Regulation (EU) 2024/900 on the Transparency and Targeting of Political Advertising have collectively created a substantially different regulatory framework from that which existed when Part 5 was originally drafted.

Particular consideration should be given to whether the statutory definitions of misinformation and disinformation proposed by Part 5 remain appropriate in light of these developments. Clear legal definitions may improve certainty and transparency; however, overly broad definitions risk creating tensions with the right to freedom of expression protected under Article 10 of the European Convention on Human Rights and Article 11 of the Charter of Fundamental Rights of the European Union.⁴⁴⁷ Political speech receives especially strong protection under both instruments, and care must be taken to ensure that legitimate political disagreement, satire, journalistic error, or good-faith participation in public debate are not inadvertently captured by regulatory measures.

Any future commencement of Part 5 should therefore be preceded by a comprehensive review of its compatibility with contemporary EU legislation and relevant human rights standards. If statutory definitions are retained, they should be narrowly drafted, clearly distinguish between intentional and unintentional conduct, and contain robust safeguards to ensure proportionality and respect for fundamental rights.



Online voting box. (Image: Shutterstock)

⁴⁴⁷ Konrad Bleyer-Simon and Urbano Reviglio, *Defining Disinformation across EU and VLOP Policies* (European Digital Media Observatory, October 2024) <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Report-%E2%80%93-Defining-Disinformation-across-EU-and-VLOP-Policies.pdf>> accessed 24 July 2026.

Recommendation 4: Establishment of a National Election Information Partnership Framework

Lead Authority: Department of the Taoiseach

Key Stakeholders: Coimisiún na Meán and An Coimisiún Toghcháin

The Department of the Taoiseach, in collaboration with Coimisiún na Meán and An Coimisiún Toghcháin, should establish a formal Election Information Partnership Framework to coordinate the dissemination of trusted and verifiable information.

This framework should:

- Identify and accredit trusted partner organisations, including independent fact-checking bodies, academic institutions, public service media, and civil society organisations;
- Provide targeted funding mechanisms to support fact-checking and public information initiatives during electoral periods;
- Develop a coordinated amplification strategy for verified content; and
- Facilitate joint public awareness campaigns across governmental and non-governmental actors.

This approach will strengthen public access to reliable information while ensuring independence and pluralism in the information environment.

Explanation and Rationale

A persistent finding throughout this Paper is that effective election integrity responses require not only the mitigation of false information, but also the availability and visibility of reliable information sources. Survey data indicate that a substantial proportion of the Irish public (74%) regard the Government as a trustworthy source of information,⁴⁴⁸ suggesting that official channels can play a meaningful role in countering misleading narratives. Public bodies such as the Central Statistics Office provide factual, evidence-based material that can be amplified to support public understanding and reduce the impact of false claims.

At the same time, independent non-governmental organisations also play a crucial role in maintaining public confidence. Supporting reputable fact-checking bodies, academic research centres, and civil-society organisations will help to ensure that accurate information is available from sources that are insulated from the perception of political bias. A coordinated approach that draws on both governmental and independent institutions would therefore strengthen the overall information environment and contribute to safeguarding election integrity.

⁴⁴⁸ Central Statistics Office, 'Trust Survey 2023: News Sources and Views on National Statistics' (CSO 16 May 2025) <<https://www.cso.ie/en/releasesandpublications/ep/p-trsns/trustsurvey2023newssourcesandviewsonnationalstatistics/results/>> accessed 19 January 2026.

Recommendation 5: Establishment of a National Election Integrity Coordination Mechanism

Lead Authority: Department of the Taoiseach

Key Stakeholders: An Coimisiún Toghcháin, Coimisiún na Meán, the National Cyber Security Centre, An Garda Síochána, the Standards in Public Office Commission, Oifig IS na hÉireann, relevant Government Departments

A permanent Election Integrity Coordination Mechanism should be established to support information sharing, threat monitoring, and coordinated responses during electoral periods.

This mechanism should include:

- The establishment of a multi-agency Election Integrity Task Force comprising representatives from An Coimisiún Toghcháin, Coimisiún na Meán, the National Cyber Security Centre, An Garda Síochána, the Standards in Public Office Commission (SIPO), Oifig IS na hÉireann, relevant Government Departments, and other appropriate stakeholders;
- The creation of an election period coordination centre to facilitate situational awareness, incident monitoring, and information sharing between relevant agencies;
- The development of a national rapid-response protocol for electoral misinformation, disinformation, FIMI, cybersecurity incidents, AI-generated deceptive content, and malicious deepfakes, including procedures for verification, attribution assessment, escalation, public communication, and specialist technical input from Oifig IS na hÉireann regarding emerging AI-related risks during election periods;
- Formal engagement procedures with online platforms, trusted flaggers, fact-checking organisations, academic institutions, and civil society organisations during election periods;
- The conduct of election integrity exercises and scenario-based testing before major electoral events; and
- The publication of post-election assessments identifying lessons learned and opportunities for continuous improvement.

The purpose of this mechanism should be to strengthen electoral resilience through coordination and information sharing rather than to regulate political speech or interfere with legitimate democratic debate.

Explanation and Rationale

As discussed in the preceding Chapter, election-related risks increasingly cut across multiple institutional mandates. The purpose of this recommendation, therefore, is to translate existing cooperation into a formal and enduring framework for coordination.

Ireland has developed significant institutional capacity in recent years through the establishment of An Coimisiún Toghcháin, Coimisiún na Meán, and Oifig IS na hÉireann, the implementation of the DSA framework, and the publication of the National Counter Disinformation Strategy. However, responsibilities relating to election integrity remain distributed across multiple organisations. The establishment of a structured coordination mechanism would enable more efficient information sharing and reduce the risk of fragmented responses during electoral periods.

As previously discussed in this Paper, AI-generated content presents challenges relating to detection, verification, attribution, and response. Ensuring that relevant expertise (including that of Oifig IS na hÉireann) can be mobilised rapidly during electoral periods therefore requires effective coordination between regulators, online platforms, and independent experts.

International practice increasingly recognises the importance of structured coordination mechanisms in protecting electoral integrity.⁴⁴⁹ At EU level, the European Cooperation Network on Elections and the Rapid Alert System provide established frameworks through which authorities can share information, identify emerging risks, disseminate alerts, and coordinate responses to threats affecting democratic processes.⁴⁵⁰ While Ireland participates in these European arrangements, they cannot replace the need for a dedicated domestic framework capable of coordinating national regulators, Government Departments, online platforms, and other relevant stakeholders. The proposed mechanism would therefore complement existing European structures by providing an operational forum for cooperation within the Irish context.

Particular attention should be given to the role of Oifig IS na hÉireann within the proposed coordination mechanism. As the national authority responsible for overseeing aspects of the EU Artificial Intelligence Act framework, the Office possesses expertise relevant to AI-generated content, synthetic media, deepfake technologies, and systemic AI-related risks. Its participation would help ensure that election integrity responses remain aligned with evolving AI governance requirements and emerging technological threats.

The proposed mechanism would not create new censorship powers or confer authority to determine the truth of political opinions. Rather, its purpose would be to facilitate operational coordination, improve situational awareness, support the dissemination of verified information, and strengthen Ireland's capacity to respond proportionately to threats capable of undermining public confidence in elections.

As digital threats continue to evolve, a coordinated and whole-of-government response framework would complement Ireland's existing regulatory and institutional safeguards while reinforcing public trust in democratic processes.

⁴⁴⁹ European Commission, 'European cooperation network on elections' (European Commission) <https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/democracy-eu-citizenship-anti-corruption/democracy-and-electoral-rights/european-cooperation-network-elections_en> accessed 23 July 2026.

⁴⁵⁰ European Commission, 'Securing free and fair European elections' (European Commission) <https://commission.europa.eu/publications/securing-free-and-fair-european-elections_en> accessed 23 July 2026.

Recommendation 6: Strengthen Election Integrity Research and Monitoring Capacity

Lead Authority: Coimisiún na Meán

Key Stakeholders: Department of the Taoiseach, An Coimisiún Toghcháin, Oifig IS na hÉireann

A national framework should be established to support independent research, election monitoring, and evidence-based analysis of risks to election integrity in digital environments.

This framework should include:

- Support for academic research partnerships;
- Support for research concerning the use of artificial intelligence, synthetic media, and automated influence techniques in electoral contexts;
- Cooperation with Oifig IS na hÉireann regarding the identification, analysis, and monitoring of AI-related electoral risks, including synthetic media and AI-enabled influence operations;
- Utilisation of DSA researcher-access mechanisms;
- Establishment of election monitoring capabilities during electoral periods;
- Cooperation with European Digital Media Observatory (EDMO) Ireland and other research bodies;
- Publication of periodic election integrity risk assessments; and
- Development of secure arrangements for data-sharing consistent with privacy and data-protection obligations.

Explanation and Rationale

The effectiveness of measures designed to protect election integrity depends upon a robust understanding of how misinformation, disinformation, FIMI, political advertising, and AI-generated content operate within online environments.

Articles 40 and 41 of the DSA provide important opportunities for independent researchers to access platform data and assess systemic risks to democratic processes. Strengthening Ireland's research and monitoring capacity would support evidence-based policymaking, improve situational awareness during electoral periods, and contribute to the long-term resilience of democratic institutions.

Collaboration with Oifig IS na hÉireann would provide access to expertise regarding emerging AI systems, assist in identifying AI-related electoral risks, and support evidence-based responses to developments in synthetic media and AI-enabled disinformation.

Recommendation 7: Strengthened Coordination between SIPO and Digital Regulatory Bodies

Lead Authority: Standards in Public Office Commission (SIPO)

Key Stakeholders: Coimisiún na Meán, An Coimisiún Toghcháin, Oifig IS na hÉireann

A formal coordination mechanism should be established to address the increasing convergence between political finance regulation and digital campaigning.

This should include:

- The creation of a joint inter-agency working group;
- Mechanisms for consultation with Oifig IS na hÉireann on the use of AI systems and synthetic media in political campaigning;
- The development of shared monitoring and reporting protocols for online political advertising and campaign expenditure;
- The establishment of data-sharing arrangements, subject to applicable legal safeguards; and
- Consideration of legislative amendments to ensure that reporting requirements adequately capture digital campaign activity.

Explanation and Rationale

This measure recognises the continuing importance of financial transparency and seeks to ensure that SIPO's oversight functions remain effective within an evolving digital electoral landscape.

SIPO's role in ensuring financial transparency in elections therefore remains important, even as the mechanisms of influence evolve. A modernised approach to safeguarding election integrity requires closer coordination between SIPO and bodies such as

Coimisiún na Meán and An Coimisiún Toghcháin, which are increasingly focused on online harms and misinformation. Such coordination would better address the growing intersection between political finance and digital campaigning. Similar engagement with the recently established Oifig IS na hÉireann, where appropriate, would help ensure that emerging AI-related developments in political campaigning are considered within existing regulatory and oversight frameworks.

The purpose of this Recommendation is distinct from the broader election integrity coordination framework proposed in Recommendation 5. Recommendation 7's focus is on ensuring that political finance oversight keeps pace with digital campaigning practices and that expenditure, sponsorship, and online political advertising can be monitored consistently across regulatory regimes.

Recommendation 8: Coordination and Expansion of Existing Media Literacy Initiatives

Lead Authority: Department of Education and Youth

Key Stakeholder: Department of the Taoiseach

A coordinated national approach should be adopted to enhance media literacy and strengthen the public's capacity to critically assess online information, building on existing initiatives undertaken by public bodies, educational institutions, civil society organisations, and other relevant stakeholders.

This programme should:

- Integrate digital and media literacy components into primary, secondary, further education, higher education, and adult education frameworks;
- Expand, coordinate, and sustain national public awareness campaigns, including existing initiatives;
- Deliver targeted interventions for groups identified as particularly vulnerable to misinformation and other forms of information manipulation;
- Develop and deliver prebunking campaigns in advance of electoral events, highlighting common misinformation, disinformation, foreign influence, and AI-enabled manipulation techniques; and
- Establish evaluation and monitoring mechanisms to assess effectiveness and support evidence-based policy development.

This measure is intended to complement regulatory interventions and existing educational and public awareness initiatives by strengthening long-term societal resilience to misinformation and other forms of deceptive online content.

Explanation and Rationale

Research has suggested that improved media literacy is effective in combating online false information.⁴⁵¹ Ireland has already made significant progress in this area. Coimisiún na Meán has established media literacy as a core regulatory priority and has supported a range of initiatives designed to strengthen public understanding of online information. Recently, it published a revised Media Pluralism Policy which emphasises the importance of informed choice, access to diverse and reliable sources of information, and a safe and trusted media environment.⁴⁵² The policy also recognises challenges arising from online intermediaries, AI, and the misuse of technologies to influence public discourse. Similarly,

451 Sander van der Linden and others, 'Inoculating the Public Against Misinformation About Climate Change' (2017) 2(1) Global Challenges 1, 5.

452 Coimisiún na Meán, Media Pluralism Policy (Coimisiún na Meán, July 2026) <https://www.cnam.ie/app/uploads/2026/07/23227-CnaM-Media-Pluralism-Policy_ENG_FINAL_web.pdf> accessed 14 August 2026.

An Coimisiún Toghcháin has undertaken public information and voter awareness activities aimed at promoting informed democratic participation. This Recommendation, therefore, does not propose the creation of a new media literacy framework, but rather the expansion, coordination, and long-term integration of existing initiatives within a broader national strategy.

Recent research also highlights the value of prebunking approaches, which seek to build resilience before exposure to misleading content occurs.⁴⁵³ Unlike traditional debunking, which attempts to correct false information after it has spread, prebunking focuses on familiarising members of the public with common manipulation techniques in advance. Such approaches may be particularly valuable during election periods, where false narratives can spread rapidly and corrective interventions often struggle to reach audiences once misinformation has become established.

Alongside existing initiatives undertaken by Coimisiún na Meán, An Coimisiún Toghcháin, educational institutions, civil society organisations, and EDMO Ireland, increasing media literacy across Irish society would further strengthen the capacity of individuals to assess the reliability of information sources and engage critically with online content. Work undertaken through EDMO and related initiatives suggests that media literacy interventions are most effective where they are sustained, evidence-based, targeted towards identified vulnerabilities, and subject to ongoing evaluation.⁴⁵⁴



Ballot in a Voting Booth on the Day of National Elections in the European Union. (Image: Shutterstock)

⁴⁵³ Jon Roozenbeek, Sander van der Linden and others, 'Psychological Inoculation Improves Resilience Against Misinformation on Social Media' (2022) 8(34) *Science Advances* eabo6254. Jon Roozenbeek, Thomas Nygren, and Sander van der Linden, 'Prebunking Interventions Based on the Psychological Theory of Inoculation Can Reduce Susceptibility to Misinformation Across Cultures' (2020) 1(2) *Harvard Kennedy School Misinformation Review*.

⁴⁵⁴ European Digital Media Observatory (EDMO), EDMO Guidelines for Effective Media Literacy Initiatives (October 2024) 12-17 <<https://edmo.eu/wp-content/uploads/2024/10/EDMO-Guidelines-for-Effective-Media-Literacy-Initiatives.pdf>> accessed 20 August 2026; Chloé Pété, 'What 2 Years of Media Literacy Across Europe Have Taught Us: Successes and Challenges from the EDMO Hub Network (2023-2025)' (EDMO, 29 June 2026) <<https://ec.europa.eu/newsroom/edmo/redirection/item/949714/default/2487>> accessed 20 August 2026.

Conclusion

Open and free elections are the cornerstone of democracy. However, history offers many examples of attempts to undermine elections in pursuit of political goals, or to undermine the legitimacy of the government in power. The advancement of digital technologies has created new ways in which the integrity of elections – and democratic processes more broadly – can be threatened. The pace of technological innovation has outpaced that of regulatory adaptation, and governments continue to grapple with how to develop effective responses.

Across the European Union, elections held in 2024 and 2025 were frequently targeted by disinformation campaigns. These efforts came from a wide spectrum of actors – from local actors seeking to influence public discourse, to coordinated operations by political opponents and foreign governments – illustrating a broader pattern of democratic processes being undermined through the dissemination of false information.

The widespread use of online platforms has made the regulation of digital content an increasingly important component of protecting the integrity of elections. At the same time, any regulatory response must remain compatible with freedom of expression and democratic participation. The challenge for policymakers is therefore not simply to remove false information, but to strengthen the broader resilience of democratic institutions, support trusted sources of information, encourage informed public debate, and ensure effective cooperation between regulators, platforms, researchers, civil society, and other relevant stakeholders.

The evidence reviewed in this Paper does not establish that misinformation, disinformation, or AI-generated content are decisive determinants of electoral outcomes. Nevertheless, their cumulative impact on public trust, institutional legitimacy, candidate participation, and confidence in democratic processes represents a significant challenge for democratic governance. Protecting election integrity therefore requires more than the regulation of online content. It requires democratic resilience: effective institutions, informed citizens, independent journalism, trusted public information, robust research capacity, and coordinated responses to emerging threats.



US President Joe Biden delivers a speech at the Dail Eireann, the lower house of the Irish Parliament, at Leinster House in Dublin, on April 13, 2023, during his four day trip to Northern Ireland and Ireland. (Photo by JIM WATSON/AFP via Getty Images)





Law Society
of Ireland

Blackhall Place
Dublin 7, D07 VY24

t +353 1 672 4800
w www.lawsociety.ie

