

USE OF ARTIFICIAL INTELLIGENCE IN EUROPEAN UNION ELECTIONS: LESSONS FOR NEW ZEALAND

Nicky Gillibrand and Marcus Ganley***

The 2024 European Parliament elections offered an early and significant test of how generative artificial intelligence is reshaping democratic processes. This article evaluates the European Union's (EU) regulatory regime, including the General Data Protection Regulation (GDPR), Digital Services Act (DSA), Artificial Intelligence Act (AI Act) and the 2024 Code of Conduct (Code), and assesses their effectiveness in managing risks associated with AI-enabled campaigning. Drawing on documented uses of synthetic content and algorithmic targeting, it highlights key enforcement and transparency challenges. The article then considers the implications for New Zealand's electoral framework, identifying substantial legal and institutional gaps. While New Zealand's regulatory tradition emphasises flexibility and restraint, the analysis argues for targeted reforms to address the emerging risks of digital campaigning. The article concludes with a set of reform options grounded in constitutional principle, transparency and institutional coherence.

I INTRODUCTION

Artificial Intelligence (AI) is increasingly reshaping democratic processes. Although its transformative potential in law, business and the markets generate the most coverage, it also has the potential for significant impact on elections.

AI refers broadly to computational systems capable of performing tasks that previously required human cognition, such as pattern recognition, prediction or language processing.¹ This article focuses primarily on a subset of AI: generative AI by which we mean models capable of producing new text,

* PhD, LLM, LLB(Hons). Lecturer in Law at the University of Salford, Manchester, United Kingdom

** LLB(Hons), MA(Hons), BA. Director, Franks Ogilvie, Wellington, New Zealand

¹ Stuart Russell and Peter Norvig *Artificial Intelligence: A Modern Approach* (4th ed, Pearson, New York, 2020).

images, audio or video through probabilistic modelling of large training datasets.² These systems, typically based on large-scale neural networks such as large language models (LLMs) or diffusion models, differ from earlier forms of algorithmic or rules-based AI that have long shaped online political advertising and data-driven profiling. The ability of generative AI to automate persuasive communication at scale, personalise messaging and blur the boundary between synthetic and authentic media creates a distinct set of risks for democratic processes. It is this class of technologies, and these specific risks, that form the primary focus of this article.

While AI has held the potential to influence election outcomes through assisting in targeting, voter segmentation and message development for years, the public release of ChatGPT in November 2022 marked a turning point in mass adoption. By the time of the 2024 European Parliament elections, generative AI tools had been available for 18 months and were in widespread use. Though 2024 saw elections in over 60 countries, the EU vote stands out as an early and especially revealing test case: it occurred in a region with relatively advanced AI regulation,³ it was a multilingual electorate, and it had a high baseline of concern about online disinformation. It offers a useful lens on how generative AI can both challenge and reinforce democratic resilience.

Generative AI's electoral impact extended beyond messaging to the broader security and legitimacy of electoral infrastructure, including voter roll systems, online electoral information, such as guidance on how and where to vote, and the broader information environment in which voters form political judgments. The European Union Agency for Cyber Security (ENISA) set forth the risks of AI-enabled manipulation of information and their potential harm to public trust in democracy.⁴ These instruments, combined with the voluntary Code of Conduct for the 2024 European Parliament Elections,⁵ were intended to help manage AI-related threats to democratic processes. As such, the instruments and code sit within the broader goals of the EU AI Act which establishes a legal framework to mitigate the risks of AI across sectors.⁶

In addition, while it predated the widespread use of generative AI from 2022 onwards, the GDPR is relevant to AI-enabled campaigning because its data protection rules shape the permissibility of

2 "AI language models: Technological, socio-economic and policy considerations" (2023) 352 OECD Digital Economy Papers; and Adam Zewe "Explained: Generative AI" (9 November 2023) <<https://news.mit.edu>>. For a more critical definition see also UK Cabinet Office "Online Disinformation and AI: Threat Guidance for Electoral Candidates and Officials" (May 2021) GOV.UK <www.gov.uk>.

3 Nicky Gillibrand and Chris Draper "Informational Sovereignty: A New Framework for AI Regulation" (2023) 10(1) International Journal on Online Dispute Resolution 60.

4 European Union Agency for Cybersecurity *ENISA Threat Landscape 2023* (19 October 2023) at 83.

5 European Commission *Code of Conduct for the 2024 European Parliament Elections* (April 2024).

6 "AI Act" European Commission <<https://commission.europa.eu>>.

profiling, micro-targeting and other data-driven practices that underpin algorithmic delivery of political content.⁷

This article begins by outlining why generative AI poses distinctive challenges to electoral integrity. It then reviews the EU's regulatory framework for addressing these challenges and evaluates how those frameworks performed during the 2024 European Parliament elections. Finally, it considers the implications of this experience for New Zealand.

II WHY WORRY ABOUT GENERATIVE AI IN ELECTIONS?

The use of AI tools in elections long predates the emergence of generative AI. For more than a decade, algorithmic content ranking, social-media-based micro-targeting and data-driven voter segmentation practices have been documented in the political communication literature.⁸ These systems relied primarily on statistical inference and pattern recognition to deliver tailored advertising. Generative AI represents a technological paradigm shift. As Paris, Donovan and others have shown, generative AI tools introduce not merely improved targeting efficiency, but the ability to create novel, persuasive and contextually adaptive political content without direct human authorship.⁹ The technological progression from algorithmic delivery to synthetic content creation gives rise to new regulatory concerns and raises questions of the interaction of democratic theory and electoral law.

While digital campaigning and targeted messaging are not new, generative AI systems amplify existing challenges and introduce new ones, especially around speed, scale and opacity. These risks do not arise from technology alone but from how it is deployed in a political context marked by information asymmetry, low transparency and limited regulatory capacity.

A central concern is the opacity of generative AI-enabled political campaigning. Already voters often do not know how or why they are being targeted. Political campaigns may outsource advertisement delivery to platform algorithms, making it difficult to assign accountability. In many cases, these systems are what are referred to as "black boxes".¹⁰ While algorithmic opacity in ad-

7 Ran He, Jie Cao and Tieniu Tan "Generative artificial intelligence: a historical perspective" (2025) 12 National Science Review at 2.

8 Zeynep Tufekci "Engineering the public: Big data, surveillance and computational politics" (2014) 19(7) First Monday.

9 Britt Paris and Joan Donovan *Deepfakes and cheap fakes: The manipulation of audio and visual evidence* (Data & Society Research Institute, 18 September 2019).

10 Jonathan Roberge, Kevin Morin and Marius Senneville "Deep Learning's Governmentality: The Other Black Box" in Andreas Sudmann (ed) *The Democratization of Artificial Intelligence: Net Politics in the Era of Learning Algorithms* (transcript Verlag, Bielefeld, 2020) 123 at 123; and Yavar Bathaee "The artificial intelligence black box and the failure of intent and causation" (2018) 31(2) Harvard Journal of Law & Technology 901.

delivery has been a feature of digital campaigning since the early 2010s, generative AI compounds this opacity by automating the creation of synthetic content and tailoring messages at scale.

A black-box AI model is often defined as a system whose internal workings are not transparent to users, operators or regulators. This opacity may stem from two distinct but interrelated sources. First, the proprietary nature of commercial AI systems means that many algorithms are protected as intellectual property. Platform providers and technology companies are under no obligation to disclose the inputs, weightings or decision-making criteria used in their models. Indeed, they will have commercial imperatives not to do so. This creates a form of legal secrecy that prevents democratic scrutiny of how political content is delivered, moderated or promoted. Regulatory access to proprietary systems is often limited to aggregate outputs or high-level documentation, rather than granular access to operational logic.¹¹

Secondly, even where AI systems are not legally protected from inspection, they may be functionally uninterpretable. Many models, especially those built using deep learning architectures, process vast numbers of variables and non-linear relationships that make it extraordinarily difficult to identify why a particular output was generated. This phenomenon is sometimes described as algorithmic opacity.¹² In high-dimensional models, even the engineers who trained the system may be unable to explain specific decisions. This is especially concerning in electoral contexts where the ability to justify targeting decisions or trace responsibility for manipulative messaging is critical to public trust.

Together, these two forms of black-box opacity (legal-proprietary and technical-computational) present serious challenges for transparency and accountability. Electoral law traditionally assumes a chain of traceable authorship and responsibility: campaigns produce content which can be reviewed and attributed. But when that content is curated or delivered by systems whose internal logic is unknown or unknowable, that assumption breaks down. Regulators may be unable to audit compliance, opponents may be unable to respond and voters may be unaware of the influence architecture shaping their information environment.

By undermining electoral law's assumed chain of accountability, a serious accountability problem is introduced. Electoral law is predicated on a basic chain of responsibility: candidates and parties are responsible for the content they authorise and electoral authorities can audit and assess that content. When decision-making is delegated to systems whose functioning cannot be interrogated or understood, the understood chain of accountability breaks down. This is perpetuated by the potential

11 Frank Pasquale *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press, Cambridge (Mass), 2015).

12 Jenna Burrell "How the machine 'thinks': Understanding opacity in machine learning algorithms" (2016) 3(1) *Big Data & Society* 1 at 4–6.

of AI to be used as an accountability sink or even liability shield,¹³ obscuring who enabled the AI tool to act in a particular way.¹⁴ The opacity of these systems makes it difficult for regulators to verify whether campaign conduct complies with electoral law, and harder still for voters to understand how their own information environments are being shaped.

This opacity also fragments political discourse. Prior to the widespread adoption of platform-based campaigning in the early 2010s, political communication largely occurred in a shared public sphere through broadcast media, print journalism and in-person campaigning.¹⁵ While targeted advertising existed, its granularity was limited and its content publicly observable. By contrast, AI-enabled micro-targeting (which has been intensified by generative models capable of producing tailored variants of messages) fragments audiences into opaque informational micro-environments, undermining the visibility that historically supported rebuttal, accountability and deliberation.

That visibility enables rebuttal, fosters deliberation and supports electoral accountability. AI-enabled micro-targeting, by contrast, enables highly individualised message delivery. Political campaigns can send different messages to different segments of the electorate based on inferred preferences, emotional triggers or psychological vulnerabilities, none of which are visible to the public.

Voters are therefore no longer participants in a shared debate. Instead, they receive personalised appeals that may be invisible to other citizens, candidates or regulators. This undermines the contestability of claims. It becomes difficult to rebut arguments or fact-check messaging when those claims are delivered privately, vary by voter and may disappear once the campaign concludes. In such environments, false or misleading information can flourish, not necessarily because it is persuasive, but because it is insulated from scrutiny.

Micro-targeting exemplifies these challenges. Political campaigns now routinely profile individuals using personal data, including online behaviour, location, preferences and inferred traits, to segment the electorate. Generative AI enhances this process by generating tailored messages with unprecedented speed and precision.¹⁶ This is highly valuable for campaigns as it improves advertising

13 Dan Davies *The Unaccountability Machine: Why Big Systems Make Terrible Decisions—and How the World Lost Its Mind* (Profile Books, London, 2024).

14 Chris Draper and Nicky Gillibrand "The Potential for Jurisdictional Challenges to AI or LLM Training Datasets" (2023) 3435 CEUR Workshop Proceedings: Workshop on Artificial Intelligence for Access to Justice.

15 Andrew Chadwick *The Hybrid Media System: Politics and Power* (2nd ed, Oxford University Press, New York, 2017); and Pippa Norris *A Virtuous Circle: Political Communications in Postindustrial Societies* (Cambridge University Press, Cambridge, New York, 2000).

16 Normann Witzleb and Moira Paterson "Micro-targeting in Political Campaigns: Political Promise and Democratic Risk" in Uta Kohn and Jacob Eisler (eds) *Data-Driven Personalisation in Markets, Politics and Law* (Cambridge University Press, Cambridge, 2021) 223.

efficiency. For example, rather than advertising a policy for early childhood education to all voters, AI tools allow that communication to be narrowly cast to voters with young children who are likely to benefit. However, it also raises concerns around threats to voter autonomy, distortions of political equality and the erosion of accountability within communicative processes that underpin legitimacy.¹⁷ When targeting is opaque and personalised, voters cannot evaluate the broader argumentative field, opponents cannot meaningfully rebut claims and regulators cannot assess compliance with electoral norms.

The risks posed by generative AI are both technological and structural; they challenge the epistemic foundations of public reasoning by replacing shared visibility with personalised information environments and by introducing content whose provenance is systematically obscured.

Furthermore, micro-targeting is not just a tool for persuasion. It is a tool for selective engagement. Voters may be chosen not only based on their likelihood to respond to a message but also for their vulnerability to that message's emotional or psychological framing. In such contexts, the goal of campaigning may shift from fostering understanding to engineering behaviour. That possibility fundamentally challenges the norms of democratic participation.

Generative AI also enables the rapid generation of persuasive content, including synthetic media and deepfakes.¹⁸ These can be deployed at scale, cheaply and quickly. Deepfakes have the potential to erode public trust.¹⁹ In environments already saturated with disinformation, the existence of AI-generated forgeries, even when known to be fake, can create a generalised sense of doubt.²⁰ If voters cannot distinguish between authentic and synthetic content, or between factual reporting and AI-generated falsehoods, the democratic discourse risks becoming polluted and incoherent.²¹ None of these risks are unique to the EU context. They are sharpened in jurisdictions with high platform penetration, weak electoral enforcement capacity and a permissive digital environment. They also pose challenges that existing electoral laws, designed for a broadcast media era, are ill-equipped to manage. These include questions about who is responsible for AI-generated political content, what standards of transparency apply and how voter autonomy and equality can be safeguarded in a highly personalised information ecosystem.

17 Cass R Sunstein *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press, Princeton (NJ), 2017).

18 Bobby Chesney and Danielle Citron "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" (2019) 107(6) *California Law Review* 1753.

19 Mika Westerlund "The Emergence of Deepfake Technology: A Review" (2019) 9(11) *Technology Innovation Management Review* 39.

20 Don Fallis "The Epistemic Threat of Deepfakes" (2021) 34 *Philosophy & Technology* 623.

21 Christian Vaccari and Andrew Chadwick "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News" (2020) 6(1) *Social Media + Society* 1.

As explored in the following sections, the EU's decision to meet these challenges through law, rather than through market-led or self-regulatory approaches, offers important comparative lessons. Its framework is neither comprehensive nor conclusive, but it represents one of the first serious efforts to grapple with AI's electoral implications through formal regulation.

III THE EU'S REGULATORY FRAMEWORK

The European Union has pursued a regulatory approach to addressing the challenges posed by AI and digital campaigning: an approach that contrasts with more market-led or light-touch responses in jurisdictions such as the United States. While the relevant instruments were not designed specifically with elections in mind, they have come to play an increasingly important role in shaping the legal environment in which electoral communication now occurs. The GDPR, DSA, AI Act and the voluntary Code of Conduct for the 2024 European Parliament Elections together form a complex and evolving framework that reflects the EU's preference for pre-emptive legal constraint over ex post accountability or platform self-regulation.²²

The following section examines these responses in detail, with a view to understanding how they apply in electoral contexts. It outlines the key features of each instrument and considers their potential relevance and limitations in addressing the challenges identified in Section 2.

A The General Data Protection Regulation

The GDPR, in force since 2018, governs the collection, processing and storage of personal data within the EU. It includes provisions on consent, transparency, purpose limitation and data subject rights, all of which are highly relevant to political micro-targeting and AI-assisted profiling. Political data is classed as sensitive under art 9, requiring explicit consent for processing. In principle, this should prevent political parties or campaigns from using inferred political preferences without clear, informed agreement.

In practice, the GDPR enforcement has been uneven, particularly in the context of political communication. While art 9 of the GDPR prohibits the processing of sensitive personal data, including political opinions, without explicit consent, this safeguard is frequently circumvented through the use of indirect profiling mechanisms. Political campaigns may obtain access to voter segments not through direct data collection, but via third-party data brokers who compile and sell behavioural, demographic and psychographic profiles.²³ Platforms may also infer political leanings based on users' engagement patterns, browsing history and interactions with content, even if the user has never formally declared a political preference.

22 As noted above, while predating generative AI, the rules brought in by the GDPR provide part of the underpinning framework for regulation of AI.

23 Information Commissioner's Office "Tribunal rules on Experian Appeal Against ICO Action" (20 February 2023) Information Commissioner's Office <<https://ico.org.uk>>.

This reliance on inferred or proxy data raises significant concerns about the validity of consent. Under art 4(11) of the GDPR, consent must be freely given, specific, informed and unambiguous.²⁴ Yet, in many cases, users are unaware that their online activity contributes to political profiling at all, let alone that it may be used to shape the political messages they see. The bundling of consent within general terms of service agreements, or the use of default opt-in systems, undermines the meaningfulness of user control. Regulatory investigations, such as those undertaken by the Irish Data Protection Commission and other national supervisory authorities, have repeatedly highlighted these deficiencies but have struggled to impose consistent remedies across the Union.²⁵

These enforcement challenges are compounded by structural limitations. Data protection authorities differ widely in resources, enforcement priorities and interpretations of the regulation. Moreover, cross-border data flows make it difficult to localise accountability; a platform based in one member state may deliver political content targeting voters in another, with unclear jurisdictional consequences. As a result, even where political profiling violates the spirit of the GDPR, effective oversight remains patchy and reactive.

B The Digital Services Act

Adopted in 2022 and fully applicable from February 2024, the DSA²⁶ creates a horizontal framework for regulating digital services across the EU, with a particular focus on mitigating systemic risks posed by large online intermediaries. A central feature of the DSA is its graduated obligations for different categories of service providers. The most stringent requirements apply to Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), defined under art 33 as services reaching more than 45 million active users per month within the EU. These entities are deemed to have a disproportionate impact on the public sphere and are therefore subject to enhanced oversight.

Under arts 34–36, VLOPs must assess, mitigate and report on systemic risks arising from the functioning of their services. These risks include negative effects on civic discourse, electoral processes and the dissemination of disinformation. Platforms must also conduct independent audits²⁷ and ensure public access to meaningful data for scrutiny. The European Commission acts as the central enforcer for VLOPs, a significant step toward harmonised cross-border governance.

24 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1, art 4(11).

25 Data Protection Commission "Irish Data Protection Commission Fines Meta Ireland €91 million" (press release, 15 March 2024).

26 Regulation 2022/2065 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

27 Articles 37 and 40.

In the electoral context, the DSA's rules on advertising transparency are particularly relevant. Article 26 requires platforms to clearly label political advertisements and maintain searchable repositories containing key information about each advertisement's content, funding source, targeting criteria and delivery metrics. These provisions aim to improve visibility and accountability around paid political messaging, addressing long-standing concerns about "dark patterns" and undisclosed targeting.²⁸

However, the regulation's effectiveness remains limited by definitional scope and enforcement complexity. The DSA's concept of political advertising is narrower than the broader ecosystem of online political communication. Content shared by influencers, grassroots actors or coordinated networks may fall outside the definition if it is not paid for or formally sponsored. Similarly, recommender systems that shape what users see without direct advertising are subject only to limited transparency obligations under arts 27 and 38. These require platforms to explain the main parameters of their recommender algorithms and allow users to opt out of profiling-based feeds but they stop short of imposing detailed constraints on algorithmic amplification of polarising or misleading content.

Moreover, while the DSA represents a major advancement in platform regulation, enforcement capacity remains uneven.²⁹ National Digital Services Coordinators tasked with supervising smaller platforms vary significantly in resources and expertise. The centralised role of the European Commission for VLOPs provides greater consistency but questions remain about responsiveness, political independence and the ability to respond swiftly during fast-moving electoral events.

In sum, the DSA represents an important regulatory evolution that addresses key transparency and accountability gaps in the digital political sphere. Yet its protections are not comprehensive and significant challenges remain in applying its provisions to the diffuse and fast-changing realities of AI-enabled campaigning.

C The Artificial Intelligence Act

The AI Act³⁰ introduces a risk-based regulatory framework for AI systems within the EU internal market. The AI Act categorises AI applications into four tiers of regulatory scrutiny: unacceptable

28 Polona Car and Filippo Cassetti *Regulating Dark Patterns in the EU: Towards Digital Fairness* (European Parliamentary Research Service, PE 767.191, January 2025).

29 Such challenges are exacerbated more broadly by the uneven implementation of the DSA by member states, including the failure to set forth the applicable penalties for infringement. See GV De Clercq "EU Sues Several Countries for Not Properly Implementing the Digital Services Act" (7 May 2025) Reuters <www.reuters.com>.

30 Regulation 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689.

risk (prohibited),³¹ high risk,³² limited risk³³ and minimal risk (subject to voluntary codes of conduct).³⁴ Each level carries different obligations, with the most stringent requirements applying to systems considered high risk.

AI systems used in electoral contexts fall under Annex III, which defines high-risk use cases. Specifically, Annex III(8)(b) designate high risk to those systems "intended to be used for influencing the outcome of an election or referendum or the voting behaviour of natural persons".³⁵ This triggers obligations under arts 8–15, including requirements for risk management, data governance, technical documentation, transparency, human oversight and post-market monitoring.

However, this classification raises several interpretive challenges. The legal threshold of "intended use" is imprecise and open to circumvention or mischaracterisation. For example, it is unclear whether general-purpose systems, such as large language models or recommender systems used in campaigning, are covered when they indirectly shape political preferences. The law does not explicitly define how to distinguish between routine campaign tools and more complex instruments of behavioural manipulation, such as psychographic segmentation or adaptive AI chatbots tuned to exploit emotional triggers.

The ambiguity surrounding scope is further complicated by the treatment of general-purpose AI (GPAI) systems. While Title VIII (arts 51–55) provides for transparency obligations regarding GPAI models, it is left to downstream deployers to assess whether a particular application constitutes a high-risk use under art 6(2). This delegation of responsibility may result in under-classification or inconsistent application of safeguards, particularly where the electoral use of AI is not the developer's primary intention.

Implementation of the AI Act will rely heavily on national market surveillance authorities (designated under art 63), alongside a central coordinating role for the European Artificial Intelligence Office (art 56). However, disparities in capacity and enforcement practices across Member States risk generating fragmentation, echoing challenges already seen in the enforcement of the GDPR.

31 Regulation 2024/1689 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L 2024/1689, art 5.

32 Chapter 3, arts 6 and 29.

33 Article 52.

34 Article 69.

35 Article 50.

During the legislative process, civil society organisations, academics and Members of the European Parliament proposed stronger electoral safeguards.³⁶ These included an explicit designation of political micro-targeting and emotive manipulation as high-risk practices. Although some additional language on democratic processes was added late in the trilogue negotiations, these proposals were not fully adopted, reflecting political compromise and industry lobbying. As a result, while the AI Act represents a foundational step in regulating AI's role in democracy, many of the most urgent questions about electoral manipulation, disinformation and voter autonomy are left unresolved.

D The 2024 Code of Conduct

In addition to binding regulation, the European Union supported a voluntary Code of Conduct (Code) on the Use of Artificial Intelligence in the 2024 European Parliament Elections released in February 2024. The Code was developed in partnership with the European Cooperation Network on Elections, the European Commission and the International Institute for Democracy and Electoral Assistance (International IDEA) and was framed as a set of ethical commitments aimed at safeguarding democratic integrity during an election season shaped by rapid advances in generative AI.³⁷

The Code invited European political parties, candidates, campaign managers, online platforms, and AI developers to commit voluntarily to a set of best practices grouped under six key principles:

- (1) *Transparency*: Participants agreed to disclose the use of AI in campaign content, particularly generative or synthetic material (e.g. deepfakes, AI-written posts or speeches).
- (2) *Authenticity and Attribution*: Signatories committed to labelling AI-generated content clearly and avoiding deceptive practices that mislead voters about authorship or intent.
- (3) *Respect for Democratic Processes*: Parties pledged not to use AI tools to suppress voter participation, distort public debate or target individuals in ways that undermine informed choice.
- (4) *Data Responsibility*: The Code urged restraint in the use of personal data, recommending that parties avoid deploying AI systems based on intrusive profiling or opaque behavioural prediction.
- (5) *Non-Discrimination*: Signatories were advised to avoid deploying AI in ways that could reinforce bias, stigma or discriminatory messaging based on race, gender, religion or other protected characteristics.

36 Nicoletta Rangone and Luca Megale "Risks Without Rights? The EU AI Act's Approach to AI in Law and Rule-Making" (2025) 16(3) *European Journal of Risk Regulation* 1082.

37 European Commission, above n 5.

- (6) *Accountability*: Political actors agreed to maintain records of AI tool usage and ensure internal governance structures were in place to monitor compliance.³⁸

Although the Code was widely circulated and endorsed by several European political party families, including the European People's Party (EPP) and Renew Europe, compliance was not universal. The Code of Conduct was signed by many of the mainstream, centrist and pro-EU political parties, including: Germany's Christian Democratic Union (CDU) led by Ursula von der Leyen at the European level and part of the governing centre-right bloc; France's Renaissance, the party of French President Emmanuel Macron; Spain's Socialist Workers' Party (PSOE) led by Prime Minister Pedro Sánchez; and Poland's Civic Coalition (KO) the party of Prime Minister Donald Tusk.

These parties generally support EU integration and regulation of digital technologies. Their support for the Code reflected a desire to demonstrate democratic leadership and ethical campaigning.

By contrast, several prominent nationalist, far-right or Eurosceptic parties did not sign the Code. These included: Italy's Lega led by Matteo Salvini; France's National Rally led by Marine Le Pen (which made major gains in the 2024 election); Germany's Alternative für Deutschland (AfD); and Hungary's Fidesz, led by then-Prime Minister Viktor Orbán.

These parties either refused to endorse the Code outright or did not respond to invitations to participate. In some cases, this was a deliberate political statement; many of these parties oppose what they characterise as EU overreach and view ethical codes as tools of censorship or elite control. Others simply ignored the process, preferring not to submit to voluntary constraints in an election year.

Its voluntary nature and lack of independent monitoring or sanctioning mechanisms meant that even among signatories, adherence was uneven and difficult to verify. This was exacerbated by the Code's lack of specificity around enforcement timelines, definitions of "AI-generated content" and what constituted adequate labelling left significant room for interpretive flexibility. While platforms such as Meta and Google committed to limited compliance, for instance by flagging or downranking certain kinds of synthetic content, the effectiveness of these interventions during the campaign period has not been systematically assessed.

Nonetheless, the Code represents an important step in the EU's evolving approach to electoral integrity in the digital age. It reflects a growing recognition that formal law alone is insufficient in responding to fast-moving technological challenges and that soft law instruments, ethical frameworks and public commitments can play a complementary role in shaping norms and expectations. While uneven in its application, the 2024 Code of Conduct marked an early attempt to articulate shared standards for responsible AI use in democratic campaigning and may serve as a foundation for more formalised obligations in future electoral cycles.

38 At 1.

E Summary Assessment

The EU's regulatory framework represents one of the most comprehensive efforts globally to address the democratic risks posed by AI, and in particular, the use of generative AI. However, it remains incomplete, unevenly enforced and internally fragmented.

The GDPR foregrounds individual consent and sensitive data protection but its model of control is frequently circumvented through inferred data and proxy profiling, leaving political actors able to target voters in ways that are legally ambiguous and practically opaque.

The DSA strengthens transparency, especially for paid political advertising on large platforms, and introduces systemic risk mitigation duties for VLOPs. Yet its scope is narrow; it does not extend meaningfully to non-sponsored content, algorithmic amplification or indirect influence.

The AI Act provides a novel risk-tiering structure, formally categorising electoral manipulation as a high-risk application. But the Act's vague language around intent, its reliance on national enforcement and the political compromises made during its drafting process have limited its reach. Crucially, it avoids directly confronting some of the most contentious issues, such as emotional manipulation or political micro-targeting.

The Code, while normatively important, illustrates the limits of voluntary ethics regimes. Its uptake is selective, its commitments are vague and its impact on actual campaign behaviour remains uncertain.

Taken together, these instruments expose both the promise and the difficulty of regulating AI in electoral contexts. They reflect a sincere attempt to anticipate harms and constrain abuse, but they also reveal the structural and institutional challenges of doing so at scale. The EU experience underscores the importance of multi-level, cross-sectoral governance but also the need for better coordination, clearer definitions and stronger mechanisms for accountability, especially in a domain where democratic legitimacy is at stake.

IV CASE STUDY – THE 2024 EUROPEAN PARLIAMENT ELECTIONS

A Introduction and Context

The 2024 European Parliament elections were among the first large-scale democratic exercises to take place in the context of widespread access to generative AI tools.³⁹ While far from the first instance of digital campaigning or algorithmic targeting, the 2024 elections stood out for the visibility

39 Joram Feitsma and Mark Whitehead "Generative populism and fake content in election campaigns" (11 September 2024) Transforming Society <www.transformingsociety.co.uk>.

of AI-generated content and the growing concern about its potential to distort political communication.

At the same time, the elections served as a major test for the European Union's new regulatory framework. Instruments such as the DSA, the GDPR and the AI Act had recently been adopted or were coming into force. Although not designed specifically for electoral settings, they collectively shaped the environment in which digital campaigning and AI use were expected to occur.

This section evaluates how AI tools were actually used during the 2024 election period, what forms of disinformation or algorithmic manipulation emerged and what these developments reveal about the strengths and limitations of the EU's current approach to regulating electoral AI.

B Use of Generative AI in Political Campaigning

Contemporary monitoring of the use of generative AI during the 2024 European elections was undertaken primarily by media and civil-society organisations such as the European Digital Media Observatory (EDMO) network. Although the DSA was only months into full applicability, it nevertheless constituted the central legal framework against which platform conduct and political communication practices were increasingly assessed.

These investigations documented several notable instances of generative AI being used in political campaigning during the 2024 European Parliament elections. The most extensively covered case involved the Italian political party Lega led by Matteo Salvini. According to Tondo for the Guardian, opposition parties lodged a formal complaint with Italy's communications regulator, Agcom, after Lega's official social media accounts shared a series of disturbing AI-generated images.⁴⁰ These included fabricated scenes of Black men attacking women and police officers, clearly intended to provoke racial animus and support anti-immigration narratives. AI Forensics, a digital verification organisation, confirmed that these images bore distinct signs of AI generation. Agcom was reportedly considering whether such uses violated the DSA's provisions on harmful and misleading political content. Further detail was provided in a flash report by Alliance4Europe, which noted that Salvini and Lega had circulated nineteen separate AI-generated images on Instagram, Facebook and X (formerly Twitter) during the campaign period.⁴¹ These images were deployed without any watermarking or disclosure of their synthetic nature despite the party having signed the EU Code of Conduct for the 2024 EP Elections. The content formed part of the "More Italy, Less Europe" campaign and reached millions of users, prompting warnings from disinformation watchdogs that the materials risked violating both domestic laws and EU-level transparency commitments.

40 Lorenzo Tondo "Italian opposition file complaint over far-right party's use of 'racist' AI images" *The Guardian* (online ed, 18 April 2025).

41 Saman Nazari and Claudia De Sessa "Salvini and Lega's electoral campaign uses non-watermarked AI images" (6 Jun 2024) Alliance4Europe <<https://alliance4europe.eu>>.

In Germany, the Alternative für Deutschland (AfD) also used AI-generated media to bolster nationalist themes during the election campaign. A report by the Atlantic Council's DFRLab found that the AfD and other members of the Identity and Democracy (ID) coalition made systematic use of unlabelled synthetic content to promote anti-immigration messages and to amplify emotionally charged rhetoric.⁴² These posts frequently relied on evocative imagery aligned with right-wing populist aesthetics designed to appear authentic and to exploit existing algorithmic recommendation patterns on social media platforms.

In France, an incident involving anonymous creators was also documented. According to the same DFRLab report, fake social media accounts were established purporting to belong to family members of Marine Le Pen. These accounts used face-swapping generative AI to create composite images that placed Le Pen's relatives in politically inflammatory contexts, especially around migration and border security.⁴³ While the individuals responsible for these accounts were not publicly identified and their motives remain speculative, the case illustrates how generative AI can be used to fabricate identities and inject disinformation into electoral discourse.

Beyond these country-specific incidents, international monitors also recorded the circulation of AI-generated audio and fabricated candidate speeches in the months preceding the formal campaign period. Both DFRLab and the Kofi Annan Foundation note that such early-phase synthetic impersonation was already emerging across Europe in early 2024 before electoral protections formally applied.⁴⁴

What made these practices particularly significant was their interaction with the DSA's newly imposed obligations on large platforms. The Act requires "appropriate and proportionate" measures to address systemic risks relating to electoral manipulation and imposes heightened transparency duties on political advertising.⁴⁵ These provisions should have influenced platform responses to synthetic political content, including through labelling, risk mitigation and the removal of deceptive political materials. Yet across the 2024 electoral cycle, independent monitoring reports documented recurrent failures by major platforms to detect, label or moderate manipulated content in a timely manner.

The EDMO network is made up of national and regional fact-checking hubs established under Commission funding. Through its Disinfo Bulletin, EDMO provided the most detailed evidence of

42 Valentin Châtelet "Far-right parties employed generative AI ahead of European Parliament elections" DFRLab (11 June 2024) <<https://dfrlab.org>>.

43 Théophane Hartmann "Viral deepfake videos of Le Pen family reminder that content moderation is still not up to par ahead of EU elections" *Euractiv* (online ed, 16 April 2024).

44 Châtelet, above n 42; and Kofi Annan Foundation *The GenAI Factor at the Ballot Box: A review of Generative AI Use in the 2024 European Parliament Elections* (2024) 10.

45 Regulation 2022/2065 Digital Services Act OJ L277/1, arts 26–27.

how platforms applied (or failed to apply) their own commitments. Through the campaign fact-checking, organisations repeatedly identified manipulated or fabricated political content circulating without platform intervention.

The Kofi Annan Foundation similarly concludes that generative AI outpaces current best practices of manual verification supported by technical tools leaving fact-checking networks unable to match the volume and velocity of synthetic content produced during the election period.⁴⁶

EDMO recorded that platforms frequently took no visible action on verified cases of political disinformation, even where the content involved manipulated images, fabricated videos or synthetic audio. A large cross-national study of 1,321 verified disinformation posts found that 45 per cent received no visible moderation action across the major online platforms, including cases involving deceptive visual media.⁴⁷

This suggests that systems designed to label or demote manipulated content were functioning inconsistently and often reactively. As such, they failed to meet the DSA's emphasis on systemic risk mitigation.

EDMO repeatedly highlighted instances in which platforms removed or demoted harmful content only after escalation by national fact-checking organisations. This included examples in Germany, Spain, Ireland, Poland and the Baltic states, where manipulated visuals circulated widely before any intervention was recorded. The pattern was consistent across the bulletins: early detection came from civil society networks rather than platform-led enforcement. In several cases, misleading or false imagery remained online long after warnings had been issued by fact-checkers.

Platform transparency repositories also provide evidence on the operation of the DSA in practice. Maldita.es found that X's DSA-mandated ads repository frequently lacked required metadata for political promotions, including those involving misleading or synthetic visuals.⁴⁸ The application of the DSA during its first electoral test appears uneven and largely reactive. There is no evidence of platforms receiving DSA-related fines or formal proceedings in the context of election-related synthetic content and no indication that political actors faced regulatory consequences for deploying unlabelled AI-generated media.

There is no publicly available evidence of platforms engaging in broad pushback against DSA obligations; rather, they show limited implementation, inconsistent transparency practices and a high degree of reliance on civil-society escalation. The effect was a regulatory environment in which

46 Kofi Annan Foundation, above n 44, at 4.

47 Maldita.es *Platform Response to Disinformation during the EU Election 2024* (June 2024) at 2.

48 Maldita.es "76 million attempts to scam you on X, using celebrities" (16 May 2024) <<https://fundacionmaldita.es>>; and European Digital Media Observatory "Disinfo Bulletin – Issue n. 28" (17 May 2024) European Commission <<https://commission.europa.eu>>.

political actors faced few practical disincentives to experiment with generative AI, while platforms often failed to meet their own stated commitments to label or mitigate synthetic political content. The Maldita.es dataset reinforces this point, showing a consistent reliance on civil-society verification rather than proactive enforcement by platforms.

Overall, the evidence from the 2024 European elections suggests that generative AI was deployed in ways that exposed gaps in the early implementation of the DSA. The DSA's transparency and systemic-risk provisions provided a framework for accountability but not yet the operational conditions for consistent enforcement. As long as platform compliance remains uneven and political actors face minimal cost for using unlabelled synthetic media, generative-AI-enhanced campaigning will remain an attractive option for parties and influence networks across the political spectrum.

C Public Vulnerability to AI-Generated Content

Evidence suggests that voters across several EU states found it difficult to identify synthetic media. A 2023 German survey found that only 8 per cent of respondents correctly identified a photograph of a real person when it was presented alongside three AI-generated faces.⁴⁹ Similar findings were reported in UK-based surveys conducted around the same period.⁵⁰ These data points, compiled in part by researchers at The Alan Turing Institute's Centre for Emerging Technology and Security (CETaS), highlight a general lack of public literacy around the nature and appearance of AI-generated content.⁵¹

In such an environment, even relatively unsophisticated synthetic material may pass as authentic, enabling the spread of misleading or emotionally manipulative messages. The fact that generative AI content can mimic the visual and rhetorical styles of political actors with such realism means that it may enjoy greater initial trust than traditional forms of political satire or photo manipulation. This dynamic creates an informational asymmetry that favours political actors and platforms over voters, challenging the normative basis for informed democratic choice.

D Evaluating the Impact

Another CETaS assessment of AI-enabled disinformation campaigns across both the UK and European Parliament elections in 2024 identified 16 confirmed cases in the UK and 11 in EU states

49 SYZYGY Group *Imagine: A First Survey of Public Perceptions of Generative Artificial Intelligence in Germany* (Digital Insight Survey 2023, March 2023) at 31.

50 "A deep dive into deepfakes that demean, defraud and disinform" (23 July 2024) Ofcom <www.ofcom.org.uk>.

51 Tvesha Sippy and others *"Behind the Deepfake: 8% Create; 90% Concerned: Surveying public exposure to and perceptions of deepfakes in the UK"* (The Alan Turing Institute, June 2024).

where generative AI was used to spread political misinformation.⁵² The report concluded that there was limited evidence that these campaigns had a measurable effect on overall election outcomes. However, consistent with conclusions from other such as the Kofi Annan Foundation and EDMO, the report emphasised the more significant long-term risks to democratic legitimacy.

Rather than persuading undecided voters, much of the content appeared to reinforce existing political alignments, consistent with prior findings about algorithmic curation and filter bubbles. Nonetheless, researchers warned that the long-term effects on public trust, civic engagement and institutional legitimacy could be profound. The opacity of AI tools, the velocity with which synthetic content spreads and the growing scepticism toward all political information online together erode the conditions necessary for democratic deliberation.

This distinction is critical; while AI-based manipulation may not have swung vote margins in a measurable way, its corrosive effect on public confidence in elections and on the perceived authenticity of political discourse should not be underestimated. A democracy can be destabilised not only by altered outcomes but by declining belief in the fairness and reliability of its processes.

E Interim Lessons

The 2024 European Parliament elections illustrate both the potential and the limits of regulatory intervention. On one hand, the DSA and other instruments provided a framework for transparency obligations and risk mitigation strategies, including commitments from platforms to label political content and cooperate with regulators. On the other, enforcement remained uneven across member states, and voluntary codes were insufficient to prevent or address the most troubling uses of generative AI.

Perhaps most significantly, the events of 2024 demonstrate that a legal regime, however comprehensive, cannot fully be a substitute for public literacy, independent monitoring capacity and the political will to enforce emerging norms. As other jurisdictions, including New Zealand, consider how to regulate AI in elections, the European experience serves as both a resource and a cautionary tale.

V IMPLICATIONS FOR NEW ZEALAND

A Overview

The European Union's experience in regulating AI and digital campaigning during the 2024 European Parliament elections offers valuable lessons for New Zealand. While the EU's regulatory framework is not directly transplantable to the New Zealand context, its attempts to address

⁵² Sam Stockwell *AI-Enabled Influence Operations: Threat Analysis of the 2024 UK and European Elections* (Centre for Emerging Technology and Security, 2024).

disinformation, algorithmic opacity and AI-generated content highlight both the urgency and complexity of electoral regulation in the digital age.

New Zealand has a strong democratic tradition and relatively high public trust in its electoral processes.⁵³ However, it also has a regulatory framework that has not kept pace with technological change. As generative AI tools become increasingly accessible and sophisticated, and as global platforms play a central role in the dissemination of political messaging, New Zealand's existing laws and institutions appear increasingly ill-equipped to manage the risks posed by AI, particularly generative AI, in the electoral context.

This regulatory lag also reflects deeper features of New Zealand's legal and political culture. While the European Union favours structured, rule-intensive regimes as exemplified by instruments like the DSA and the AI Act, New Zealand tends to regulate incrementally and pragmatically, often relying on institutional discretion, soft law and general principles rather than tightly prescriptive rules.⁵⁴ This reluctance to intervene proactively creates both flexibility and risk: it may preserve democratic freedoms but may also leave gaps in electoral safeguards as new technologies outpace legacy frameworks.

This section provides a detailed examination of the current regulatory landscape in New Zealand, identifies key gaps in law and oversight and considers how the lessons from the EU might inform principled but practical reform.

To see where reform might be needed, it is first necessary to outline how New Zealand's electoral law is currently structured and administered.

B New Zealand's Electoral Law and Administration

The Electoral Act 1993 is the central statutory source for the rules and procedures governing New Zealand elections, providing the legal infrastructure for enrolling voters, conducting general elections and referenda, regulating political parties and managing the formal aspects of campaign activity.

The Electoral Act also contains provisions that regulate campaign activity, particularly in relation to election advertising and campaign finance. It defines what constitutes an "election advertisement"

53 Matthew SR Palmer "New Zealand Constitutional Culture" (2007) 22(4) NZULR 565; see also on pragmatism as an aspect of New Zealand's culture relevant to the exercise of power: Matthew SR Palmer and Dean R Knight *The Constitution of New Zealand: A Contextual Analysis* (Hart Publishing, Oxford, 2022) at 20–21.

54 Palmer "New Zealand Constitutional Culture", above n 53; Alan McRobie "The Electoral System" in Philip A Joseph (ed) *Essays on the constitution* (Brookers, Wellington, 1995) 312; and Janet McLean "Attorney-General v Taylor: An Example of the Cautious, Incremental and 'Common Law' Approach to Constitutional Change in New Zealand" (5 December 2019) International Association of Constitutional Law Blog <<https://blog-iacl-aidc.org>>.

and requires that such material include a promoter statement.⁵⁵ It imposes spending limits on parties and candidates and requires declarations of donations and campaign expenses.⁵⁶ These rules apply not only to political parties but also to third parties who engage in election advertising.

While the Electoral Act is the primary source of electoral law in New Zealand, it operates alongside a wider set of laws and institutions that shape electoral practice.

The Broadcasting Act 1989, while primarily focused on the operation and content standards of television and radio broadcasting, plays a central role in structuring how political parties access the airwaves during general elections.

It sets out a statutory regime for allocating both broadcasting time and public funding to registered political parties for the purposes of party election programmes. The allocation process, and the restrictions it entails, also generate legal obligations that are enforced during election periods. Parties receiving funding must comply with content restrictions and declaration requirements, and broadcasters are bound by time slots and fairness rules that emerge not from the Electoral Act, but from the Broadcasting Act.

The Broadcasting Act also prohibits broadcast party-political advertising other than through the allocation regime.⁵⁷ This operates as a total prohibition on paid party election programme broadcasts (other than those funded through the allocation process) on TV or radio both during and outside electoral periods.⁵⁸ In this way, while not an obvious source of electoral law, the Broadcasting Act plays an important role in regulating aspects of New Zealand political campaigns.

The Constitution Act 1986, although primarily structural, contains an express electoral law requirement: a general election of members of Parliament must be held every three years.⁵⁹ The New Zealand Bill of Rights Act 1990 plays a foundational role in shaping the permissible limits of electoral and communications law. Section 14 affirms the right to freedom of expression, including the freedom to seek, receive and impart information and opinions of any kind and in any form. Any statutory or regulatory intervention in political speech, such as rules governing campaign content, platform

⁵⁵ Electoral Act 1993, ss 3A and 204F.

⁵⁶ Parts 6A and 6B and ss 206K–206N.

⁵⁷ Section 70(1).

⁵⁸ While parties cannot advertise other than through the allocation process, there is a carve-out for individual candidates (s 70(3) and related definitions in s 69). Individual candidates are not part of the party allocation system and can purchase their own broadcast time but only during the regulated period (from writ day to the day before polling day) and subject to spending limits, promoter statement requirements and broadcasting standards.

⁵⁹ Section 17.

obligations or AI disclosures, must be demonstrably justified under s 5, which requires that limits on rights be reasonable and prescribed by law.

In parallel, the Human Rights Act 1993 (HRA) prohibits discrimination on various grounds, including political opinion. While the HRA is less directly engaged in electoral campaigning regulation, it provides a broader human rights context that constrains how technologies such as AI can be deployed in ways that disproportionately affect or target protected groups.

Alongside these statutory protections, the common law has played a role in defining fair process in election-related decision.⁶⁰

Against this background, it is possible to identify specific gaps in the current framework that are relevant to AI-enabled campaigning. The next section looks at these gaps.

C Key Gaps in the New Zealand Framework

New Zealand's electoral laws were designed for a pre-digital era and contain no rules that address AI in campaigning. This creates a regulatory asymmetry. Television and radio advertising is heavily circumscribed while Facebook, YouTube, Instagram and TikTok operate in a largely unregulated space during election periods. A party cannot broadcast a radio advertisement, other than using its broadcast allocation, but it can advertise on a podcast or YouTube TV. The allocation system has been described as "hopelessly outdated"⁶¹ and "outdated and inappropriate".⁶²

The Electoral Act 1993 and Broadcasting Act 1989 are also silent on algorithmic content generation, synthetic media, automated voter engagement or AI-assisted targeting. Section 3A of the Electoral Act defines an election advertisement as any form of words or graphics that can reasonably be regarded as encouraging or persuading voters to vote (or not vote) for a party or candidate. A video or message created entirely by AI is treated no differently from one produced by a human and there is no obligation to disclose that generative AI was used.

60 See *Dunne v Canwest TVWorks Ltd* [2005] NZAR 577 in which the High Court held that a private broadcaster could be subject to public law obligations when organising an election debate. The case remains significant for affirming that public law duties of fairness may apply to private actors where their decisions have significant consequences for democratic participation. For analysis see Dean R Knight "Dunne v Canwest TVWorks Ltd: Enhancing or Undermining the Democratic and Constitutional Balance?" NZULR 21(4) 711.

61 Andrew Geddis "Funding New Zealand's Election Campaigns: recent stress points and potential responses" (2021) 17(2) Policy Quarterly 9 at 13.

62 Margaret Courtney-Tennent "Political Finance and Government Legitimacy in New Zealand: A Review of New Zealand's Electoral Finance Regulations From a Constitutional Perspective" (2022) 30 Wai L Rev 94 at 125.

One area where the gap between the broadcast era rules and the current campaign environment has come into focus is the ban on polling day advertising.⁶³ The prohibition is broadly drafted, making it an offence on polling day to exhibit, publish, distribute or broadcast any statement advising or intended or likely to influence an elector as to the candidate or party for whom they should or should not vote. Geddis reports that in 2011 the Electoral Commission reported five people to the police for Election Day posts on social media intended or likely to influence voters.⁶⁴ Radio New Zealand reported in 2014 26 people were referred to the police for the same offence including a current and a former member of the All Blacks.⁶⁵

A lack of rules on content creation is mirrored by equally limited controls on how voter data is gathered and used. Under the Privacy Regulations 2020, political parties are exempt from key privacy principles when collecting data for political purposes.⁶⁶ They need not inform voters that data is being collected, grant access to that data or correct inaccuracies. There are no limits on profiling or inferring sensitive traits from third-party data brokers or platform analytics, and no duty to reveal targeting criteria, data sources or algorithmic logic.

This permissive approach to data use sits alongside weak obligations to disclose how that data is applied in campaigns. The Electoral Act requires promoter statements on advertisements and the Act's financial disclosure requirements cover donations and expenses, but there is no requirement to disclose targeting methods, the use of AI or data provenance.⁶⁷ There is no real-time ad register, no central repository of campaign material and no archiving requirement for online content. By contrast, the EU's DSA requires platforms to maintain searchable ad libraries and conduct democratic-integrity risk assessments.⁶⁸

There is also no requirement to preserve or archive online campaign content for post-election scrutiny. In the absence of a proactive transparency regime, public and academic monitoring of digital campaigning remains extremely difficult.

63 Electoral Act 1993, s 197(1)(g)(i). See also s 197(2A), on material published on websites.

64 Andrew Geddis *Electoral Law in New Zealand: Practice and Policy* (2nd ed, LexisNexis, Wellington, 2014) at 223.

65 "Sports stars' tweets referred to police" *Radio New Zealand* (online ed, 4 November 2014); "Editorial: Changing times remove need for ban on tweets" *The New Zealand Herald* (online ed, 25 July 2015); "Absurdity of law must be changed" *Taranaki Daily News* (online ed, 6 November 2014); and Katarina Williams "Warning issued after sportsmen sin binned for Election Day tweets" *Stuff* (online ed, 21 September 2017).

66 Schedule 4 cl 9.

67 Sections 204F and 206K–206N.

68 Regulation 2022/2065 Digital Services Act [2022] OJ L277/1, art 39 (requiring online platforms to maintain a publicly accessible and searchable repository of advertisements for at least one year after display).

The value of transparency rules also depends on the strength of the bodies tasked with enforcing them. The Electoral Commission lacks any specific enforcement powers with respect to AI and digital platforms. It cannot compel platforms to disclose algorithmic processes or remove content. Other regulatory bodies, such as the Privacy Commissioner, the Broadcasting Standards Authority and the Commerce Commission, operate under different statutes with distinct mandates. None of these bodies address the use of AI. No cross-agency body exists to monitor the role of AI in elections, leaving a regulatory vacuum. This institutional fragmentation is a significant vulnerability. It contrasts with jurisdictions, such as Australia, where multi-agency electoral integrity taskforces coordinate threat assessments and enforcement strategies.⁶⁹

D Comparative Reflections: What the EU Experience Reveal

While the EU and New Zealand have different legal cultures, approaches to regulation and regulatory capacity reflection on the EU's experience reveals strategies and pitfalls that New Zealand may wish to consider when responding to AI-enabled campaigning.

While New Zealand cannot impose EU-style obligations on global platforms, such as those set out in the DSA, the logic of transparency and accountability can still inform domestic law, for instance, through disclosure rules, digital ad registers or co-regulatory arrangements supported by legislative backstops.

A second strand of the EU framework, found in the AI Act, offers a different kind of regulatory tool. The AI Act reflects a risk-based regulatory model, classifying AI systems by their potential impact on human rights and democratic integrity. Systems used to influence voting behaviour are considered high-risk, triggering documentation and transparency obligations. This tiered approach could inform future legislative frameworks in New Zealand, particularly if election-related AI tools are recognised as warranting heightened scrutiny.

However, the EU's experience also highlights the limits of regulation alone. This reinforces a point that has been long recognised in New Zealand: legal instruments must be supported by institutional capacity, political will and cultural legitimacy.

The value of the EU model lies in its layered approach, combining general legal duties (such as privacy and fairness) with election-specific tools (such as transparency registers and audit regimes). For New Zealand, the challenge is not how to import EU-style rules, but how to adapt core principles, like transparency, equity of access and protection from manipulation, into a legal culture that prioritises pragmatism, flexibility, institutional discretion and strong rights protections.

69 Australian Electoral Commission "Electoral Integrity Assurance Taskforce" <www.aec.gov.au>.

E Reform Options for New Zealand

Any proposed reform in this area must be approached in light of both constitutional protections (under the New Zealand Bill of Rights Act 1990 and the Human Rights Act 1993) and the practical realities of enforcement in a small jurisdiction. Any implications under the Treaty of Waitangi need to be carefully considered. The regulatory capacity of the New Zealand state is also relevant.

It is also important to remember that whatever their motivations, reforms of electoral laws have real world implications for politics. There will be winners and losers, and this will, and should be, contested. As Geddis reminds us "a change in those legal rules may have immediate consequences for the fortunes of one or another electoral participant".⁷⁰

With these constraints in mind, there are reforms that could be taken that improve transparency without restricting freedom of expression. Steps that could be taken without requiring legislative change include the Electoral Commission, Privacy Commissioner and other relevant agencies updating their existing guidance to reflect the challenges posed by emerging AI tools, including synthetic content generation, microtargeting techniques and algorithmically curated information environments.

Political parties could be encouraged to include disclosure statements identifying the use of AI-generated or algorithmically targeted content in their campaign materials. The creation of a norm whereby failure to make such a disclosure would call advertisements into question is plausible, particularly if major parties agreed. Such disclosures could be modelled on existing promoter statement requirements, adapted for the digital environment.⁷¹

While the EU experience casts doubt on the effectiveness of voluntary regimes, the experience of the 2023 New Zealand election gives grounds for optimism. Following an admission from the National Party that it had used generative AI in some advertising, other parties were prepared to go on the record with their policy towards AI in political advertising.⁷² By ruling out its use, the Labour, Green and ACT parties set a standard to be assessed against.⁷³

⁷⁰ Geddis *Electoral Law in New Zealand: Practice and Policy*, above n 64, at xvi.

⁷¹ For discussion of the merits of disclosure see for example Bronwyn Isaacs "Playing politics with AI: why NZ needs rules on the use of 'fake' images in election campaigns" (9 August 2023) The University of Waikato <www.waikato.ac.nz>; and Phil Pennington "Election 2023: Artificial intelligence attack ads – to disclose, or not disclose for political campaigns?" *New Zealand Herald* (online ed, 30 May 2023).

⁷² Tess McClure "New Zealand's National party admits using AI-generated people in attack ads" *The Guardian* (online ed, Auckland, 24 May 2023); "National Party uses AI in attack ads: Christopher Luxon 'not aware'" *New Zealand Herald* (online ed, 23 May 2023); and Justin Hu "Revealed: National's rejected AI attack ads" *1News* (25 May 2023) <www.1news.co.nz>.

⁷³ Andrea Vance "National using AI for attack ads: The AI political campaign has arrived" *Stuff* (23 May 2023) <www.stuff.co.nz>.

Establishing a voluntary digital advertising register, similar in design to the ad libraries already maintained by large online platforms in other jurisdictions, could also promote transparency. The National Archives could be funded as host, serving a dual purpose of a register for the current election and maintaining the historical record.⁷⁴

Public education campaigns could improve digital literacy and raise awareness of how AI tools are used (and potentially misused) in election campaigns. Although these measures would not prevent problematic uses of AI, they could increase transparency, bolster informal accountability and help build public resilience to manipulation and misinformation.

In addition to voluntary regimes and information campaigns, there is a strong case for considering targeted statutory reforms to strengthen disclosure and promote transparency without unduly infringing on rights of political expression.

A comprehensive review of the Electoral Act 1993, the Broadcasting Act 1989 and associated regulations is long overdue. These frameworks remain structurally anchored in an era where campaign communication was dominated by broadcast television and print media. Despite incremental reforms, the frameworks continue to presume the primacy of traditional media and are poorly adapted to a platform-driven, algorithmically personalised campaign environment. The fact that party political radio ads are effectively banned but an identical advertisement can be run on a digital platform goes beyond making a mockery of the law.

A full review must not only catch up with the reality of the modern communications environment but also confront the reality that AI and digital technologies are reshaping political communication, from the creation of synthetic content to automated persuasion and microtargeted engagement.

Such a review would need to consider whether the existing architecture remains fit for purpose and could include the introduction of new statutory definitions (such as "synthetic content" or "automated persuasion"), updated enforcement powers and enable provisions for responsive rulemaking as new technologies emerge. These changes would not only modernise the legislative framework, but would provide the legal infrastructure necessary to ensure electoral integrity in a digital and data-saturated political environment.

One concrete change that could be made could be introducing basic AI-related disclosure requirements as called for by Isaacs among others.⁷⁵ Political parties and third-party promoters could be required to declare use of AI tools to generate, curate or personalise content. Currently, the promoter statement regime requires that electoral advertisements must state the name and contact

74 For recent imitative example see National Library of Australia "National Library takes poll position to collect 2025 federal election" (media release, 14 April 2025).

75 Isaacs, above n 71.

details of the promoter.⁷⁶ This requirement could be broadened to require disclosure of the use of AI. While the growing integration of AI into daily work means the boundaries of what constitutes disclosable use of AI will be fraught, the EU's Code of Conduct provides a useful model that focuses on the use of synthetic content and algorithmic targeting.

Narrowing the privacy exemption for political parties in relation to inferred or sensitive information used in microtargeting or profiling could bring New Zealand into closer alignment with international privacy norms.

Beyond such targeted amendments, there is also scope for broader, more structural measures. For instance, an AI accountability clause could be inserted into the Electoral Act, modelled on the EU AI Act's risk-based framework, identifying election-related AI systems as requiring documentation, explanation or audit.

Even with enhanced statutory tools, institutional capacity and coordination remain critical. New Zealand's electoral regulation operates across a relatively decentralised landscape, with responsibilities shared between multiple agencies. To ensure coherent oversight, a cross-agency Electoral Technology Taskforce could be established. This taskforce could monitor the role of AI in campaigns, coordinate responses, issue joint guidance and serve as a clearinghouse for risk identification.

Within the Commission itself, both mandate and capacity could be expanded. This could include specific powers to request information from platforms, investigate novel campaigning practices and issue compliance notices.

Finally, a co-regulatory approach might be considered, whereby the Commission works in partnership with digital platforms to develop voluntary codes of practice with clearly defined baselines. In cases of non-compliance or harm, these arrangements could be supported by legislative backstops, providing both flexibility and enforceability where appropriate.

Together, these proposals could lead to a more coordinated and responsive oversight system that is relevant to modern political campaigning. A forward-looking regulatory posture in New Zealand is likely to be one that blends pragmatism with principle, adapting institutional structures while upholding the constitutional values that underpin its electoral system.

VI CONCLUSION

Reviewing the New Zealand situation in light of the lessons from the EU experience shows the need for action. The legal and institutional responses to AI in electoral campaigns, whether in Europe, New Zealand or elsewhere, are necessarily partial. This is an emerging field. Regulation is moving at a far slower pace than technological advancement.

⁷⁶ Electoral Act 1993, s 204F(2).

The emerging implications of AI in NZ elections are yet to be explored in academic writing on campaigns. For example, the leading work on the 2023 election has only one reference to AI, whereby a candidate is referring to a public meeting on the topic. There is no examination of the role AI played in the campaign.⁷⁷

As our analysis has shown, transparency obligations, disclosure regimes and oversight mechanisms can address many of the structural risks posed by synthetic content, algorithmic targeting and unregulated data use. But beneath these regulatory challenges lies a more fundamental concern: whether the communicative conditions necessary for democratic legitimacy can survive in an environment shaped by AI.

Democratic theory has long held that legitimate political authority depends not just on procedural fairness, but on the capacity of citizens to form judgments in a shared public sphere. As articulated most fully in the deliberative model developed by Jürgen Habermas, democracy presupposes certain discursive conditions: communication that is reasoned, sincere, contestable and grounded in shared factual reference points.⁷⁸

These deliberative norms are also reflected in the Venice Commission's *Code of Good Practice in Electoral Matters* which frames democratic legitimacy as dependent on transparency, equal opportunity and voters' access to information that enables genuine choice. Although formulated before the emergence of generative AI, the Code's concern with the quality and integrity of the information environment provides a useful reference point for assessing how synthetic content and algorithmic targeting erode the shared communicative space on which electoral fairness depends.⁷⁹

AI disrupts these conditions by introducing falsehoods or disinformation. It also reshapes the communicative environment itself: fragmenting audiences, obscuring sources and inserting persuasive techniques that operate beneath the level of conscious deliberation.

Seen in this light, the reforms outlined above are means of preserving the communicative conditions that give elections their democratic legitimacy. When political communication becomes personalised, optimised and increasingly indistinguishable from organic discourse, the possibility of public contestation is diminished. Voters may still cast ballots, but they do so in increasingly isolated informational cocoons without knowing what others are seeing and without the opportunity to challenge or be challenged in common view. AI-generated content, and the platforms that distribute it, operates in ways that decouple political persuasion from democratic accountability. In such an

77 Stephen Levine (ed), *Back on Track? The New Zealand General Election of 2023* (Te Herenga Waka University Press, Wellington, 2024).

78 David Rasmussen "Ideal Speech Situation" in Amy Allen and Eduardo Mendieta (eds) *The Cambridge Habermas Lexicon* (Cambridge University Press, Cambridge, 2019) 182.

79 European Commission for Democracy through Law *Code of Good Practice in Electoral Matters: Guidelines, explanatory report and interpretative declarations* (Council of Europe, Strasbourg, 2002) at I.2–I.3.

environment, the ideal of public reasoning begins to erode, not by censorship or repression, but by the quiet replacement of communication with simulation.

However, regulation of campaigning is necessarily contentious. It brings into conflict the right of freedom of expression and the democratic ideals of political equality⁸⁰ and fairness.⁸¹ Regulation can promote democratic engagement by protecting political equality and share of voice. However, to the extent that it does so by limiting political expression, it risks citizens disengaging from democratic involvement.⁸²

Reforms that prioritise transparency, disclosure and institutional coordination can go some distance in protecting the integrity of electoral processes without unduly restricting freedom of expression. However, the ultimate risk posed by AI in elections is not simply the loss of legal control, it is the dissolution of the communicative infrastructure on which democracy depends.

That infrastructure cannot be legislated into existence. It rests on shared norms, institutional trust and a public sphere in which voters can reason together. As AI becomes more central to political campaigning, New Zealand must look not only to regulation, but ask what kind of democratic culture it wants to preserve. Legal reform can help protect the integrity of elections, but it cannot substitute for the public discourse that gives them meaning.

80 Joshua Cohen "Money, Politics, Political Equality" in *Philosophy, Politics, Democracy: Selected Essays* (Harvard University Press, Cambridge (Mass), 2009) 268 at 268.

81 Courtney-Tennent, above n 62, at 125.

82 Jonathan Boston and Alec Mladenovic "Political Equality and the Regulation of Election Spending by Parallel Campaigners" (2010) 45(4) *Australian Journal of Political Science* 623.