Algorithmic Electoral Manipulation and Constitutional Democracy: Comparing Regulatory Safeguards in India and the European Union

Prof. (Dr.) Mohd Imran

Maulana Azad National Urdu University, India

DOI: https://doi.org/10.68050/JAMS.2026.884

Received: 30 October 2026; Accepted: 04 November 2026; Published: 13 November 2026

ABSTRACT

Algorithmic electoral manipulation raises a constitutional problem that extends beyond the falsity of campaign messages: control over voter data and the distribution of political communication can weaken the conditions under which electoral choices are made and challenged. This article compares India and the European Union through a functional doctrinal analysis of election law, data protection, intermediary regulation and artificial intelligence governance, assessing the legal position on 13 October 2026. It distinguishes legitimate persuasion from deceptive impersonation, exploitation of vulnerabilities, covert sponsorship and opaque algorithmic distribution. The comparison identifies a difference in regulatory emphasis. India combines constitutional election supervision, campaign rules and increasingly specific synthetic-content duties, while the EU distributes obligations across data controllers, advertising intermediaries, major platforms and AI providers. Neither architecture establishes that formal compliance preserves electoral autonomy in practice. The article develops an electoral contestability framework that examines whether sponsorship can be traced, targeting can be scrutinised, exposure can be independently assessed and corrective decisions can be reviewed within an election-relevant period. It argues that synthetic-content labels and rapid removal cannot substitute for distribution transparency, and that structural platform duties require safeguards against political censorship. Rather than recommending wholesale transplantation of EU legislation, the article proposes targeted Indian reforms concerning political-data use, public campaign repositories, platform risk assessment, independent evidence access and urgent judicial review. The contribution is a constitutional account of how electoral regulation should govern influence infrastructures while preserving political expression and privacy.

Keywords: constitutional democracy, electoral integrity, artificial intelligence, political microtargeting, platform accountability, comparative constitutional law.

1. INTRODUCTION

An election can remain procedurally regular while its information environment becomes difficult for voters, competitors and regulators to scrutinise. A candidate's speech may be authentic but delivered through undisclosed profiling. A fabricated endorsement may be labelled on its original upload and circulated without that label elsewhere. A platform may prohibit political advertisements while its recommendation system promotes coordinated campaign material. These situations reveal a constitutional difficulty: rules directed at a message, a candidate or a formally purchased advertisement may overlook the infrastructure through which political influence operates.

This article examines that difficulty through India and the European Union. India supplies a constitutional setting in which electoral supervision is concentrated in the Election Commission of India (ECI), fundamental rights constrain state intervention and election legislation identifies particular campaign offences and corrupt practices. The EU provides a contrasting regulatory setting in which obligations concerning data, advertising, platforms and AI operate across a multilevel constitutional order. The comparison concerns the legal protection of democratic choice, rather than treating the EU as a state with an electoral system equivalent to

India's.[1]

The article's central proposition is that electoral integrity requires legally supported opportunities to scrutinise algorithmic influence. A voter cannot meaningfully assess personalised persuasion if its sponsor and informational basis are concealed. A challenger cannot rebut inconsistent campaign messages if their distribution is inaccessible. An adjudicator cannot determine whether an intervention was justified if platforms or public authorities fail to preserve evidence. These are problems of electoral contestability: the practical ability to identify, examine, dispute and obtain review of political influence and regulatory responses to it.

The approach also limits the regulatory claim. Democracy does not entitle the state to guarantee that voters encounter only correct, balanced or rational political speech. Political argument involves emotion, selective emphasis, uncertainty and disagreement. Regulation must identify legally relevant interference with electoral agency rather than condemn every successful act of persuasion. The constitutional protection of debate would be weakened if regulators could remove a message merely because an algorithm helped write it or because its argument was controversial.

Existing research establishes several relevant starting points. Zuiderveen Borgesius and colleagues identify the possible participatory benefits of microtargeting alongside privacy risks and fragmented campaign representations. Dobber, Ó Fathaigh and Zuiderveen Borgesius analyse the interaction of European data-protection and electoral rules. Susser, Roessler and Nissenbaum locate manipulation in covert influence that exploits decision-making vulnerabilities. These contributions suggest that an assessment should ask how influence is organised, rather than equating personalisation with illegality.[2]

This article contributes a comparison of the allocation of responsibility along the electoral influence process. It examines whether the relevant duties attach to the actor who controls the source of a risk, whether the evidence needed to assess compliance is available and whether remedies can operate before the electoral opportunity disappears. Its argument is therefore more specific than a general claim that AI threatens democracy. Content authenticity, lawful data use, campaign financing and platform distribution are distinct regulatory objects. Their interaction determines the practical protection that each legal regime can provide.

Three questions organise the inquiry. First, which forms of algorithmic influence implicate constitutional rights and electoral integrity, and which remain legitimate political communication? Second, how do India and the EU allocate preventive duties, disclosure obligations and remedies across the actors involved? Third, what reforms can improve scrutiny without authorising a politically controlled system of truth determination? The article answers these questions through a structured comparison and a set of hypothetical applications rather than an unsupported ranking of national regulatory effectiveness.

The temporal dimension matters. India adopted synthetic-content amendments to its intermediary rules in February 2026, while the ECI had already issued campaign labelling advice in January 2025. The EU's political-advertising regulation became generally applicable in October 2025. The EU's current implementation timetable defers the main Annex III high-risk AI obligations to December 2027. Accordingly, the existence of an enacted rule and the availability of an enforceable safeguard must be assessed separately.[3]

The article proceeds by explaining its method, defining the threat and rights framework, examining each jurisdiction and developing a comparative reform model. It argues that the most useful lesson from the

[1] Constitution of India, arts 14, 19, 21, 324 and 326. Consolidated Version of the Treaty on European Union [2012] OJ C326/13, arts 2 and 10.

[2] Frederik J Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82–96. Tom Dobber, Ronan Ó Fathaigh and Frederik J Zuiderveen Borgesius, 'The Regulation of Online Political Micro-Targeting in Europe' (2019) 8(4) Internet Policy Review. Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8(2) Internet Policy Review.

[3] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E), 10 February 2026, effective 20 February 2026. Election Commission of India, Advisory for labelling synthetic/AI generated content used by Political Parties for election campaigning, No 491/Social media-SOP/2025/Communication, 16 January 2025. European Commission, New EU rules on political advertising come into effect, 10 October 2025. European Commission, AI Omnibus enters into force, 27 July 2026, updated 31 July 2026; revised Annex III application date 2 December 2027.

comparison is the allocation of duties across an influence process. India can strengthen oversight of campaign infrastructures without reproducing the entire EU legislative architecture. The EU, in turn, must assess whether its layered framework makes electoral influence genuinely open to challenge or distributes responsibility in ways that leave voters without a timely remedy.

2. RESEARCH DESIGN AND EVIDENTIAL LIMITS

2.1 A functional doctrinal comparison

The method is comparative and doctrinal. The materials include constitutional texts, judgments, legislation, commencement notifications, election directions, regulatory guidance and selected original empirical research. The legal cut-off is 13 October 2026. A source's legal character is recorded before its content is used: statutory provisions are distinguished from delegated legislation, judicial holdings, administrative directions, interpretive guidance, voluntary commitments and company policy statements. This distinction prevents an advisory or platform announcement from being represented as an independently enforceable legislative prohibition.

The units of comparison are regulatory functions. Six functions are examined: the protection of voter agency; the governance of political data; the identification of campaign sponsorship; the visibility of distribution; institutional enforcement; and timely contestation of content or regulatory action. A functional approach is necessary because no single Indian enactment corresponds to the combination of the General Data Protection Regulation (GDPR), Digital Services Act (DSA), political-advertising regulation and AI Act. Comparison by legislative title would therefore obscure both overlapping obligations and unregulated activities.

The selection of India and the EU is analytically justified by their different institutional arrangements and shared rights tensions. Each must reconcile political expression, privacy and democratic participation with the regulation of private intermediaries. India combines national election administration with linguistic, social and federal complexity. EU measures interact with national election law and several categories of supervisory authority. The analysis does not assume that a common value produces identical competence, remedies or institutional capacity.

The EU Charter applies to EU institutions and to Member States when implementing Union law. Its electoral provisions concerning European Parliament elections should not be described as a universal constitutional code for every national election. However, platform and data regulations apply within their own material and territorial scopes and can affect national electoral communication. Similarly, India's constitutional guarantees do not automatically create a directly enforceable obligation against every private campaign contractor. Statutory and institutional mechanisms are needed to translate constitutional concerns into actor-specific duties.[4]

2.2 Source selection and analytical procedure

Sources were selected purposively for their relevance to the six functions, with priority given to official legislative texts, published judgments and regulator-issued materials. The literature search focused on political microtargeting, online manipulation, algorithmic curation, synthetic political media and AI persuasion. This is a focused doctrinal review, not a systematic bibliometric review; no claim is made to an exhaustive search, a preregistered review protocol or independently coded inter-rater reliability.

The analytical procedure has four steps. First, the relevant activity is identified: collection of data, generation of material, selection of recipients, recommendation, payment, moderation or redress. Second, the actor exercising control over that activity is located. Third, the legal instrument, operative duty and commencement status are determined. Fourth, the duty is assessed against the evidence and remedy needed for meaningful contestation. The assessment is qualitative and provision-specific; it assigns no numerical score to a jurisdiction's democratic quality or enforcement success.

[4] Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7–8, 11, 21, 39, 47 and 51–52.

This procedure differentiates legal coverage from effectiveness. A rule may require disclosure but remain difficult to enforce against an offshore contractor. An authority may possess an urgent removal power without providing a proportionate appeal mechanism. A data-protection duty may be enacted but not yet applicable. Each situation requires a different conclusion. The article uses 'coverage' to mean an identified legal duty and 'effectiveness' only where implementation evidence supports such a claim.

2.3 What the figures and examples establish

The figures serve different evidential purposes. Figure 1 is an analytical graph of possible relationships between actors, activities and rights. Figure 2 replots published experimental estimates from Salvi and colleagues, using the corrected article and its September 2026 author correction. Figure 3 plots verified regulatory milestones and distinguishes dates preceding the cut-off from later implementation. None estimates the prevalence of manipulation in India or the EU.[5]

The hypothetical scenarios in Table 4 are legal stress tests. They are not accounts of documented wrongdoing by named parties, platforms or candidates. Their purpose is to reveal how a change in sponsorship, data source, distribution method or representational context changes the applicable legal analysis. By holding the scenario approximately constant, the comparison can identify a difference in regulatory response without claiming a causal effect on voting.

Several limitations follow. Closed messaging, private targeting data and platform algorithms prevent a complete public account of electoral exposure. Enforcement announcements reflect the categories and priorities of reporting authorities. Removal counts cannot establish how much AI-generated content existed, whether removals were justified or whether voters changed their preferences. The absence of an accessible decision cannot establish that no action occurred. These limitations make a descriptive cross-jurisdictional prevalence graph inappropriate for this article.

The resulting claims are about legal architecture, rights and institutional design. The article does not assert that AI determined an election result, that EU safeguards are empirically superior or that a proposed reform would eliminate manipulation. It identifies conditions that would make those propositions more capable of independent testing.

3 ALGORITHMIC INFLUENCE AND CONSTITUTIONAL HARM

3.1 Persuasion and manipulation

For this analysis, algorithmic electoral manipulation means the use of computational systems to organise political influence through deception, covert exploitation of vulnerabilities, unlawful profiling or concealed coordination in ways that materially obstruct informed and contestable electoral choice. This is an analytical definition, not a claim that Indian or EU law contains a single offence with these elements. Particular liability must be established under the applicable provision, including its requirements concerning intent, harm, actor responsibility and jurisdiction.

The definition deliberately leaves space for legitimate political persuasion. A campaign may explain different policy implications to farmers and students without manipulating either group. Translation can allow a candidate to communicate with voters who otherwise face a language barrier. An openly identified chatbot can answer questions about a manifesto. An algorithm can help schedule campaign meetings without addressing voters at all. The relevant question is whether the practice interferes with the conditions of choice through a legally cognisable mechanism.

[5] Francesco Salvi, Manoel Horta Ribeiro, Riccardo Gallotti and Robert West, 'On the Conversational Persuasiveness of GPT-4' (2025) 9 Nature Human Behaviour 1645–1653, as corrected in September 2026. Francesco Salvi, Manoel Horta Ribeiro, Riccardo Gallotti and Robert West, 'Author Correction: On the Conversational Persuasiveness of GPT-4' (2026) Nature Human Behaviour, published 3 September 2026.

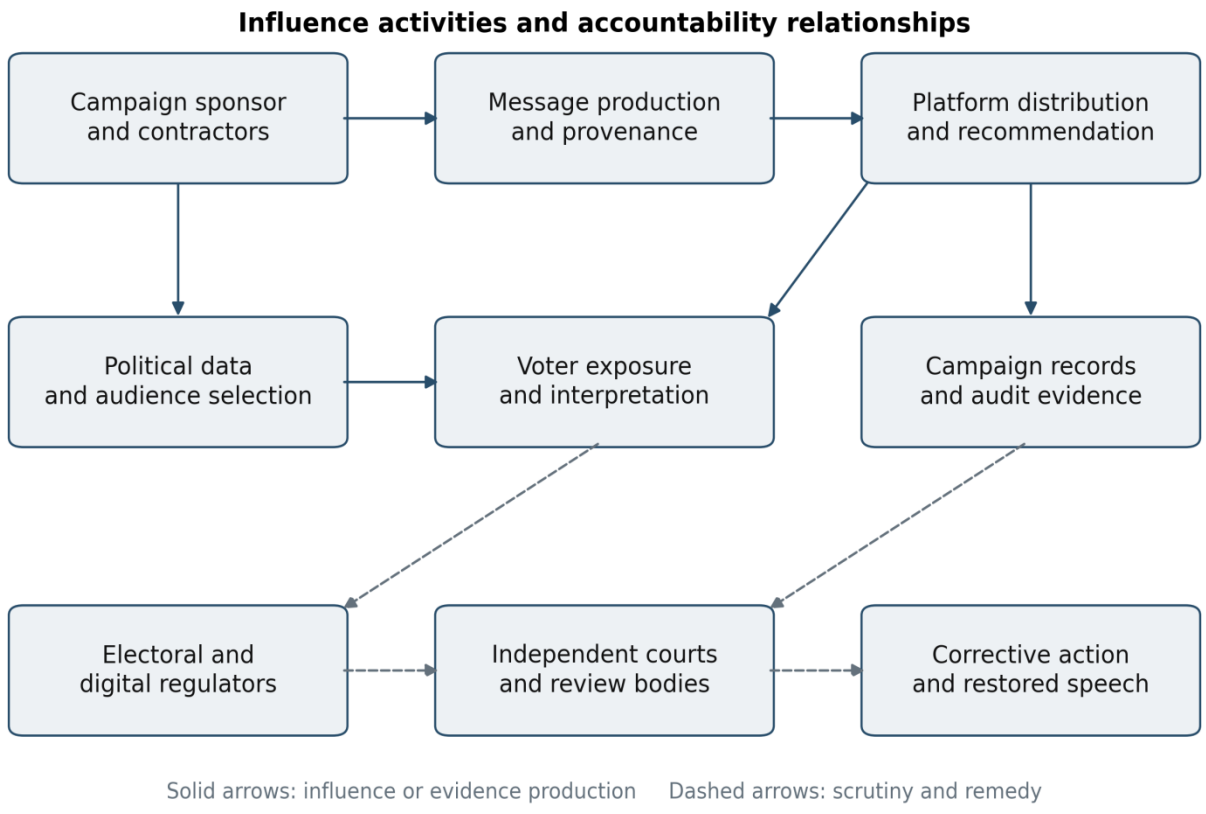
Several distinctions are essential. AI generation concerns how material is produced; deception concerns what it falsely represents. Targeting concerns the selection of recipients; discriminatory or exploitative targeting concerns its basis and purpose. Recommendation concerns platform distribution; coordinated inauthentic amplification concerns an attempt to manufacture apparent support or evade distribution rules. Sponsorship transparency concerns who finances or directs communication; a synthetic-content label alone does not answer that question.

Yeung's account of continuously adjusted choice architectures provides a useful explanation of why influence can arise through the environment in which decisions occur. The constitutional implication developed here is that a content-centred safeguard may miss repeated selection, sequencing and exclusion of messages. This implication does not establish that every personalised feed changes political attitudes. It identifies why legal scrutiny needs evidence about distribution as well as content.[6]

3.2 The influence process and its rights implications

Figure 1 represents the relationships that the comparison examines. Campaign actors and contractors may commission messages, acquire information and select audiences. Platforms can further determine actual exposure through delivery and recommendation. Public authorities and courts intervene through supervision, correction and adjudication. The graph shows possible accountability relationships, not an empirical claim that every campaign uses each mechanism.

Figure 1 A conceptual graph of electoral influence and accountability



Author's analytical model. Arrows identify possible relations, not estimated causal effects or a documented campaign network.

The first possible harm is impairment of personal agency. A voter may be confronted with a fabricated official instruction or an impersonated candidate. The second is loss of public accountability: different audiences may

[6] Karen Yeung, 'Hypernudge: Big Data as a Mode of Regulation by Design' (2017) 20(1) Information, Communication & Society 118–136.

receive incompatible promises that competitors cannot observe. A third concerns political equality, where data-intensive infrastructures allow some actors to buy or engineer visibility that remains difficult to attribute. A fourth concerns privacy, including inference of political preferences from information supplied for a different purpose. These harms need not coincide, and the remedy appropriate to one may not address another.

Synthetic media also creates an evidential risk. Once credible fabrication becomes possible, genuine recordings can be dismissed as artificial. Chesney and Citron describe this possibility as the liar's dividend. The implication for electoral administration is that authenticity disputes require evidence preservation and careful communication, rather than an assumption that a detector can settle every contested recording. Vaccari and Chadwick's experimental work further directs attention to uncertainty and trust, alongside direct deception.[7]

Table 1 Practices and the legal questions they raise

Practice	Principal constitutional concern	Appropriate object of scrutiny
Deceptive synthetic impersonation	Authenticity, agency and reputation	False representation, authorisation, actor intent and likely harm
False official voting instructions	Practical exercise of the franchise	Verifiable procedure, source impersonation and urgency
Sensitive-data microtargeting	Privacy, equality and autonomy	Data source, inference, purpose, consent and prohibited profiling
Covert paid or coordinated amplification	Transparency and political accountability	Beneficial sponsor, payment, contractor control and inauthentic conduct
Opaque algorithmic delivery	Visibility of political influence	Optimisation objective, actual aggregate exposure and audit evidence
Overbroad automated restriction	Expression and procedural fairness	Legal ground, contextual accuracy, reasons and timely review

Analytical taxonomy developed in this article. Categories may overlap; inclusion does not establish liability.

3.3 What experimental evidence does and does not show

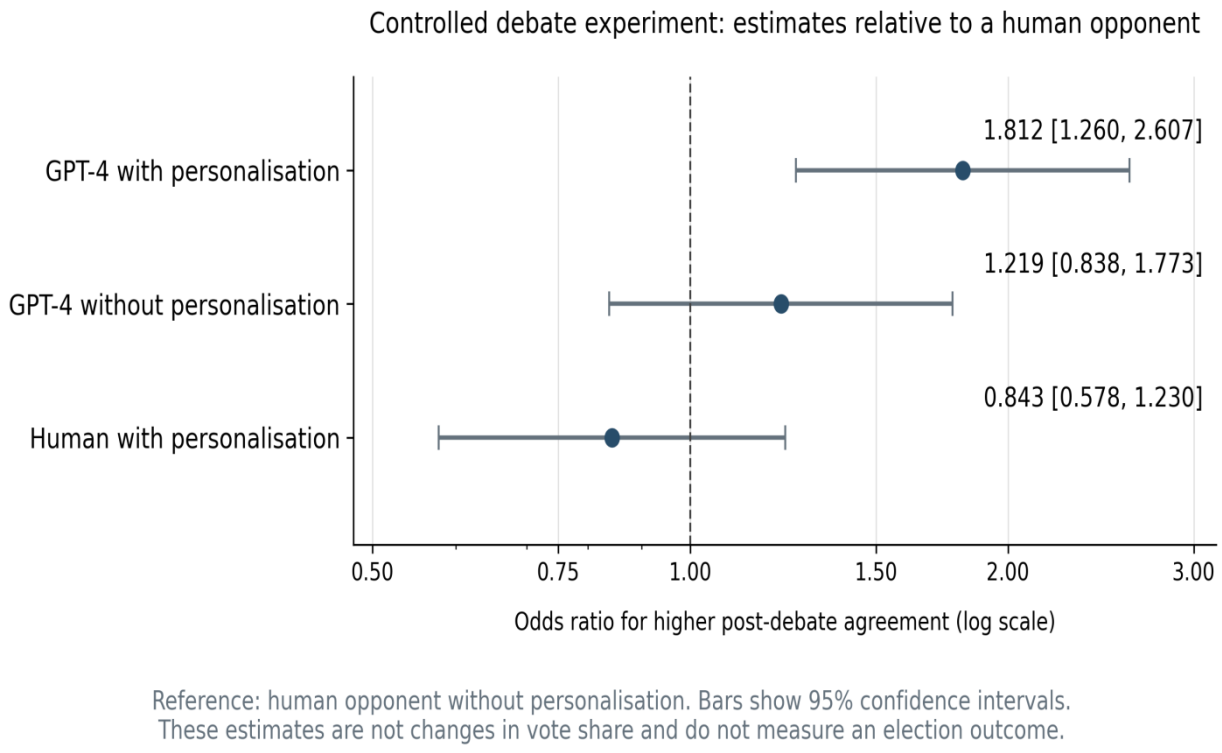
Empirical findings counsel against both complacency and technological determinism. Guess and colleagues' field experiment during the 2020 US election changed Facebook and Instagram feed ordering. It found substantial changes in users' platform experience without detectable changes in several measured political attitudes over the study period. The result does not show that algorithms are politically irrelevant; it demonstrates that a particular intervention, population and period cannot support a universal causal claim about electoral manipulation.[8]

Salvi and colleagues studied controlled debates with 900 participants. Figure 2 shows their corrected aggregate estimates relative to a human debate opponent without personalisation. Personalised GPT-4 had an estimated odds ratio of 1.812 for higher post-debate agreement, with a 95% confidence interval of 1.260–2.607. The

[7] Bobby Chesney and Danielle Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753–1820. Cristian 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.
[8] Andrew M Guess and others, 'How Do Social Media Feed Algorithms Affect Attitudes and Behavior in an Election Campaign?' (2023) 381 Science 398–404.

plotted estimates for non-personalised GPT-4 and personalised human opponents had intervals crossing 1. The study's modelled aggregate figure uses 750 observations; this differs from its participant total.[9]

Figure 2 Published odds ratios from a controlled persuasion experiment



Author's replot of corrected estimates in Salvi and others (2025): 95% confidence intervals; reference is a human opponent without personalisation. Study N = 900; modelled aggregate observations n = 750. Not a voting-effect estimate.[10]

The September 2026 correction is substantively relevant. The direct comparison between personalised and non-personalised GPT-4 did not reach the conventional significance threshold, with p = 0.07. The paper should therefore not be used to claim a conclusively isolated causal advantage of personalisation. The experiment supports the existence of persuasive capabilities under controlled conditions, not a measured change in Indian or European vote shares.[11]

Table 2 Selected original studies and limits on inference

Study and design	Relevant finding	Limit for this comparison
Guess and others (2023): US election field experiment	Feed-order intervention changed platform experience without detectable changes in several measured attitudes.	One intervention and study period; does not establish absence of all algorithmic political effects.
Salvi and others (2025), corrected 2026: controlled debates	Personalised GPT-4 exceeded the human baseline; direct comparison with non-personalised GPT-4 was not significant at 0.05.	Proof of capability in a controlled setting; no Indian or EU vote-share estimate.

[9] Salvi and others (2025), corrected 2026.
[10] Salvi and others (2025), corrected 2026. Salvi and others, Author Correction (2026).
[11] Salvi and others, Author Correction (2026).

Vaccari and Chadwick (2020): synthetic political video experiment	Examines deception, uncertainty and trust as distinguishable effects.	Does not establish that a synthetic video caused an election result.

Sources: studies identified above and cited in notes 7–11. Outcomes are not pooled.

These results support an evidence-sensitive regulatory approach. Demonstrated capability can justify attention to foreseeable misuse, while sanctions and severe speech restrictions require provision-specific proof. Transparency, retention of campaign records and proportionate access for independent researchers can reduce uncertainty about real-world deployment. Conversely, suppressing a campaign message on the unsupported assumption that an AI system must be irresistibly persuasive would undermine the democratic agency that regulation is intended to protect.

4. THE INDIAN REGULATORY ARCHITECTURE

4.1 Constitutional foundations and their limits

India's constitutional starting points include equality under Article 14, expression under Article 19(1)(a), privacy and dignity under Article 21 and electoral supervision under Article 324. Article 326 establishes adult suffrage for the relevant elections. These provisions supply distinct foundations: political speech protects campaigning and criticism, privacy concerns constrain voter surveillance, and electoral administration protects the conditions in which the franchise is exercised. A unified analysis should preserve these differences rather than treating 'democracy' as a free-standing authorisation for censorship.[12]

In Association for Democratic Reforms, the Supreme Court invalidated the electoral-bonds framework and protected voters' access to political-finance information. The holding concerns electoral funding, not an existing constitutional right to an explanation of every advertising algorithm. Its relevance here is analogical: information about the organisation of political influence may be important to an informed electoral choice. Extending that reasoning to beneficial campaign sponsors and targeted advertisements requires a separately justified legislative design.[13]

Puttaswamy recognises the constitutional significance of informational privacy and decisional autonomy. It also places state interference within a framework of legality, legitimate purpose and proportionality. Applied to electoral infrastructures, privacy reasoning supports scrutiny of the collection, combination and use of political data. It does not automatically resolve every private-data dispute or establish that campaign profiling is unlawful in all circumstances. Statutory duties, factual context and the relationship between state and private conduct remain necessary.[14]

Shreya Singhal supplies a constraint on overbroad regulation of online expression. Its treatment of vagueness, chilling effects and the distinction between discussion, advocacy and incitement matters when 'manipulation' is used as a legal label. The judgment struck down section 66A and read down the actual-knowledge requirement under section 79(3)(b). An electoral-integrity objective cannot itself replace the constitutional requirements for restricting speech.[15]

This leads to a central distinction in the proposed framework. A requirement that a paid campaign disclose its sponsor and preserve distribution records concerns accountability for organised activity. A power to delete any statement that an authority considers politically misleading directly controls expression. Both require legal justification, but the second presents a sharper risk of partisan intervention and demands stronger safeguards concerning grounds, evidence, reasons and review.

[12] Constitution of India.
[13] Association for Democratic Reforms v Union of India, 2024 INSC 113, Supreme Court of India, 15 February 2024.
[14] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, Supreme Court of India, 24 August 2017.
[15] Shreya Singhal v Union of India (2015) 5 SCC 1, Supreme Court of India, 24 March 2015.

4.2 Election law and supervision

The Representation of the People Act 1951 provides relevant, but bounded, mechanisms. Sections 77–78 concern election expenditure accounts. Section 123 identifies corrupt practices, including undue influence, specified religious appeals, promotion of enmity and particular false statements concerning a candidate's personal character or conduct. Section 126 regulates specified election communication during the period preceding the conclusion of polling. Its wording should not be treated as an AI-specific prohibition on every online statement. An algorithmic practice must be connected to the elements and scope of the relevant provision.[16]

For example, a fabricated statement about a candidate may raise a question under section 123(4), but not every false policy claim constitutes a corrupt practice. Its conditions concerning the responsible actor and the nature of the statement matter. A targeted promise does not become statutory undue influence merely because it is personalised. A campaign's outsourced expenditure may require accounting and attribution, but a contractor's involvement does not remove the need to prove the relevant relationship and authorisation.

Article 324 enables the ECI to address electoral administration, including situations not exhaustively dealt with by legislation. Mohinder Singh Gill recognises the breadth of this supervisory role while also locating it within the legal order. The institutional strength is a specialist constitutional authority able to respond during a campaign. The limit is that supervisory power cannot be assumed to create every substantive offence or to displace applicable law and fundamental rights.[17]

ECI instructions concerning social-media campaigning require information about relevant accounts, address pre-certification of political advertisements and connect online campaigning with expenditure monitoring. Pre-certification makes some organised advertisements visible before publication. It should be distinguished from universal prior approval of ordinary citizens' political posts. Its practical scope also differs from a public archive documenting the audiences actually reached and the targeting techniques used.[18]

The constitutional problem is therefore one of translation. Electoral law recognises several underlying wrongs, but platform delivery can divide the relevant evidence among a party, candidate, consultant, advertising exchange and host platform. Investigation requires rules determining who must keep which records and how the ECI obtains them. Without those rules, even a clearly identified offence may be difficult to establish within an election-relevant period.

4.3 Campaign directions concerning synthetic content

The ECI's 6 May 2024 directions warned political parties against misleading or unlawful synthetic material and required the removal of relevant deepfake posts within three hours of coming to their notice. The addressees and trigger are important: the instruction should not be rewritten as a general statutory three-hour obligation for every intermediary or every disputed political statement. The January 2025 advisory called for prominent labels and disclaimers on AI-generated or significantly altered campaign material.[19]

The ECI's April 2026 release reiterated campaign labelling and disclosure of the originating entity, and described action concerning unlawful social-media material. These developments demonstrate that India's position has moved beyond an exclusively voluntary request to avoid deepfakes. However, an administrative account of action does not establish the prevalence of manipulation or the accuracy of each intervention.[20]

[16] Representation of the People Act 1951, ss 77–78, 100, 123 and 126.
[17] Mohinder Singh Gill v Chief Election Commissioner (1978) 1 SCC 405, Supreme Court of India, 2 December 1977.
[18] Election Commission of India, Instructions with respect to use of Social Media in Election Campaigning, 25 October 2013, reproduced in Social Media and Fake News training materials, updated 31 August 2024.
[19] Election Commission of India, Responsible and ethical use of Social Media platforms by political parties and their representatives, 6 May 2024. ECI, AI Labelling Advisory, 16 January 2025.
[20] Election Commission of India, General Elections and bye-elections 2026: ECI action on unlawful social media content, 19 April 2026, Press Information Bureau release 2253528.

The directions have a useful informational function. They can tell voters that a representation is synthetic and identify the actor originating it. They do not necessarily reveal who selected the recipients, what data were used, whether competing versions were distributed or how much additional exposure recommendation produced. This is the difference between the provenance of a message and accountability for its delivery.

Campaign labels should also be interpreted with attention to context. An accessible translation of an authentic speech, a disclosed fictional illustration and a fabricated recording of an opponent do not present the same risk. Clear explanation can permit legitimate use while reducing deception. Indiscriminate labels that merely announce the use of AI may convey little about what changed or whether a real person authorised the representation.

4.4 Intermediary duties after the 2026 amendments

The Information Technology Act establishes relevant liability and intermediary mechanisms, including section 69A blocking and conditional protection under section 79. Identity theft or computer-mediated impersonation provisions may apply where their elements are satisfied; they should not be described as offences automatically covering every synthetic political image. The Act's intermediary framework is concerned with legal responsibility and lawful orders, rather than a complete election-specific audit of recommendation systems.[21]

The February 2026 amendments introduced duties concerning 'synthetically generated information'. The definition focuses on audio, visual and audiovisual representations appearing real or authentic, with exclusions for specified good-faith editing and other non-misrepresentative uses. Rule 3(3) addresses prevention of prohibited synthetic material and labelling and provenance for permissible material. Rule 4(1A) adds declaration and verification obligations for significant social-media intermediaries. These provisions must be applied within their actual scope; pure text generation and every form of audience profiling cannot simply be assumed to fall within this synthetic-media definition.[22]

The amended rules also distinguish procedural triggers. The three-hour timeline under rule 3(1)(d) follows actual knowledge arising through a competent court order or specified reasoned written intimation. Rule 3(2)(b) contains a separate two-hour process for specified victim complaints involving intimate material or electronic impersonation. Treating these provisions and the ECI's party-directed instruction as one undifferentiated takedown rule would obscure legal responsibility and procedural safeguards.[23]

The Ministry's August 2026 statement confirms the government's emphasis on labels, traceable metadata and technical measures. The constitutional issue developed here concerns how these mechanisms operate in contested political cases. Automated systems may assist triage, but the fact that a detector gives a high-confidence result is not, by itself, a complete legal assessment of satire, authorisation, news reporting, culpability or statutory harm.[24]

An original label can be lost through recompression, cropping or reposting. These possibilities indicate why provenance mechanisms need interoperability and why absence of metadata is not affirmative proof that a recording is fabricated. Regulators should preserve the original item and document uncertainty. A correction that explains what is known and what remains disputed may protect voters more effectively than a definitive announcement unsupported by reliable evidence.

Rapid intervention is sometimes necessary, particularly for fabricated polling instructions. Nevertheless, speed changes the distribution of error. A platform facing liability pressure may remove lawful material before contextual review. An appeal decided after polling cannot restore the lost opportunity to speak. This is a reason

[21] Information Technology Act 2000, ss 66C, 66D, 69A and 79.
[22] IT Amendment Rules 2026, GSR 120(E).
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, consolidated text updated 10 February 2026, rr 2(1)(wa), 3, 3A and 4.
[24] Ministry of Electronics and Information Technology, Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes, 6 August 2026, Press Information Bureau release 2295500.

to couple urgent powers with contemporaneous reasons, tightly defined scope, preservation of evidence and a rapid independent review route.

4.5 Political data and phased data protection

The Digital Personal Data Protection Act 2023 creates a general framework governing relevant digital personal data. It contains consent and notice requirements, duties of data fiduciaries and additional requirements for significant data fiduciaries. It does not reproduce the GDPR's general category of sensitive personal data, nor does it provide a separate statutory prohibition on sensitive political-advertising profiles comparable to the EU political-advertising regulation. Its exclusion for data made publicly available by the individual or by a person legally required to publish it is relevant to campaign data strategies, but should not be extended to everything that happens to be accessible online.[25]

Commencement is decisive. GSR 843(E) stages the Act's operation. The principal provisions governing processing and individual rights belong to the eighteen-month commencement group following publication in November 2025. On the article's October 2026 cut-off, they should not be presented as a fully operative consent-and-remedy system. The 2025 Rules likewise stage the operation of notice, security and rights provisions. The comparison accordingly evaluates this component both as an enacted architecture and as a future implementation question.[26]

A consent-centred framework leaves additional electoral questions. A person may agree to receive campaign messages without understanding that a platform will infer susceptibility from unrelated behaviour. A set of individually authorised messages may remain collectively unobservable, allowing incompatible commitments to different groups. Consent therefore addresses an important relationship between a person and a data user, but it does not necessarily provide public accountability for organised campaigning.

Public electoral data create another difficulty. Legal publication of a roll serves administrative and verification purposes. Combining published information with inferred religion, financial distress or behavioural records serves a different function. Whether a particular data flow falls within statutory scope must be determined carefully; the normative case for additional campaign rules does not depend on treating a lawful electoral roll as confidential in its entirety. A tailored rule can instead restrict specified combinations or uses for political targeting.

4.6 Institutional capacity and remedies

India's architecture involves the ECI, state electoral machinery, intermediary grievance systems, law-enforcement agencies, courts and the developing data-protection institutions. The platforms' Voluntary Code of Ethics provides cooperation mechanisms, but participation in a code is not equivalent to an independently audited statutory duty addressing electoral distribution. It is particularly important to distinguish collaborative incident handling from the creation of a substantive prohibition.[27]

Linguistic and procedural access should be treated as part of enforcement design. A notice or complaint route that is technically available but incomprehensible to an affected voter provides limited practical protection. Review of synthetic audio requires competence in language, idiom and context. Election administration should therefore assess complaint accessibility and contextual review capacity rather than relying only on response-time targets.

Judicial independence has a direct place in this framework. Authorities may face pressure to classify criticism as unlawful manipulation; platforms may seek to avoid regulatory conflict through excessive removal. Courts

[25] Digital Personal Data Protection Act 2023, ss 3, 4–6, 9–10, 11–17 and 18–26.
[26] Ministry of Electronics and Information Technology, commencement notification under s 1(2) of the Digital Personal Data Protection Act 2023, GSR 843(E), 13 November 2025. Digital Personal Data Protection Rules 2025, GSR 846(E), 13 November 2025, rr 1, 3, 12 and 17.
[27] Internet and Mobile Association of India and participating platforms, Voluntary Code of Ethics for the General Elections 2019, 20 March 2019, reproduced by the Election Commission of India in its social media instructions.

must be able to assess the legal basis and proportionality of both action and inaction. The argument is for appropriately timed judicial scrutiny, not routine judicial management of every campaign dispute or an unrestricted bypass of the constitutional rules governing election challenges.

The principal Indian gap is consequently more specific than an absence of AI law. India has several applicable legal mechanisms and has added synthetic-media duties. What remains underdeveloped is a connected framework for political-data restrictions, attribution of campaign contractors, observable delivery, independent evidence access and effective correction of erroneous restrictions during the campaign itself.

5 THE EUROPEAN UNION REGULATORY ARCHITECTURE

5.1 A multilevel constitutional setting

The EU's framework combines democratic values under Article 2 TEU and representative democracy under Article 10 with Charter protections concerning privacy, personal data, expression, equality and effective remedies. The relevant rights do not operate as a single permission to restrict political communication. Data minimisation can limit targeting while expression protects campaign debate. Effective remedies require scrutiny of restrictions as well as of harmful influence. The EU's institutional competence and the Charter's field of application remain part of every analysis.[28]

The distinctive feature is the allocation of responsibilities across different regulatory objects. Data protection addresses the conditions for processing information about people. The DSA addresses intermediary procedures and, for designated major services, systemic risks. Regulation 2024/900 addresses political-advertising transparency and targeting. The AI Act imposes system-related requirements and particular transparency duties. Compliance with one layer does not establish compliance with the others.

This layered architecture has a constitutional advantage: it can identify the platform, advertiser or AI operator whose decisions generate a risk. It also has an institutional cost. A voter may struggle to determine which authority can obtain relevant evidence and provide timely relief. The comparison therefore asks whether the layers connect around a real electoral dispute rather than merely accumulating formal obligations.

5.2 Personal data and political targeting

The GDPR supplies lawful-processing, fairness, transparency, purpose-limitation and data-minimisation duties. Article 9 gives political opinions and other specified categories additional protection, subject to defined exceptions. It is inaccurate to describe this as an unconditional ban on every processing activity involving political affiliation. Likewise, Article 22 concerns qualifying solely automated decisions with legal or similarly significant effects; it is not a general right to challenge every political advertisement as an automated decision.[29]

The EDPB's targeting guidance examines provided, observed and inferred data and the responsibilities of targeters and social-media providers. Inference matters because a campaign need not possess a declared political preference to construct a politically relevant audience. Determining responsibility can require examination of the respective actors' decisions about purposes and means rather than acceptance of a contractual description of one party as a passive processor.[30]

The Court of Justice's Meta Platforms judgment also demonstrates that legal analysis of data use cannot be separated entirely from market power and the conditions of consent. Schrems emphasises limits on aggregation and use for personalised advertising, including the fact that public disclosure of some information does not

[28] Treaty on European Union, arts 2 and 10. EU Charter of Fundamental Rights.
[29] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 5–9, 13–15, 21–22, 35 and 77–82.
[30] European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, version 2.0 adopted 13 April 2021; references amended 7 July 2021.

authorise unrestricted processing of related sensitive data. Neither judgment is an election-specific ruling, but each is relevant to the informational infrastructure on which campaigns may depend.[31]

The constitutional significance developed here is preventive. A fabricated political message can be addressed after circulation; an unlawful profiling practice should be constrained at the stage when an audience is constructed. Nevertheless, private-data protection does not provide full campaign accountability. A lawful list of willing supporters can still be used to distribute contradictory political commitments. Lawful processing and public contestability are therefore separate requirements.

Data-protection controls also create boundaries around enforcement. A regulator should not collect unlimited identifiable political-preference records merely to determine whether a campaign complied. Targeting parameters, aggregated delivery records and carefully governed access may provide evidence with less intrusion. The design question is how to disclose the existence and mechanics of organised influence without exposing the political beliefs of individual recipients.

5.3 Political advertising and sponsorship transparency

Regulation 2024/900 became generally applicable on 10 October 2025. It is directed at recognising political advertisements, identifying their sponsors and making targeting more accountable. Its definition extends beyond an advertisement expressly requesting a vote and includes relevant influence on legislative or regulatory processes. At the same time, exclusions and the distinction between advertising services and personal political expression remain important. The regulation does not establish a general prohibition on political discussion.[32]

For relevant personal-data targeting and ad delivery, Article 18 requires collection from the data subject and separate explicit consent for political advertising, and prohibits profiling using GDPR special-category data. It also restricts targeting involving persons known with reasonable certainty to be at least one year below the applicable voting age. Article 5 includes restrictions concerning eligible sponsors in the three months preceding relevant elections or referendums. These are conditional rules whose scope must be determined rather than universal bans on all foreign political expression.[33]

Articles 11–12 provide the basis for labels and transparency notices, with formats and technical specifications addressed by Implementing Regulation 2025/1410. The informational task is different from an AI label: a voter needs to know that a communication is political advertising, who sponsors it and how to obtain the associated transparency information. A message can be entirely human-produced and still require that information.[34]

Public repositories can make dispersed campaigns more observable. The regulatory provisions for repositories and associated transparency information support scrutiny beyond the individual recipient's screen. Their constitutional value lies in permitting competitors, journalists and voters to compare messages and investigate funding. However, a database's legal existence should not be equated with comprehensive coverage, easy search or complete attribution of campaign networks.[35]

The regulation also creates a foreseeable problem of displacement. An actor can avoid purchasing a formally identified advertisement and instead pay an influencer, fund an apparently independent page or coordinate organic-looking distribution. Whether such activity is captured depends on its actual organisation and the legal definition, not merely on the platform's label. Rules must distinguish genuinely independent political

[31] Case C-252/21 Meta Platforms and Others v Bundeskartellamt, EU:C:2023:537, Court of Justice of the European Union, 4 July 2023. Case C-446/21 Schrems v Meta Platforms Ireland, EU:C:2024:834, Court of Justice of the European Union, 4 October 2024.
[32] Commission, Political Advertising Rules, 10 October 2025.
[33] Regulation (EU) 2024/900 on the transparency and targeting of political advertising, OJ L, 2024/900, 20 March 2024, arts 3, 5, 11–13, 18–19 and 30.
[34] Commission Implementing Regulation (EU) 2025/1410 of 9 July 2025 on the format, template and technical specifications of labels and transparency notices of political advertisements under Regulation (EU) 2024/900.
[35] Political Advertising Regulation (EU) 2024/900.

commentary from concealed paid promotion without treating ordinary supporters as presumed campaign agents.

Platform responses reinforce the distinction between legislative and practical effects. Meta announced that political, electoral and social-issue advertisements would no longer be delivered in the EU from October 2025, while ordinary political posting would remain possible. This is a company policy response, not an EU prohibition requiring every platform to stop political advertising. Meta's account of compliance burdens is the company's stated explanation, not an independently established finding that the regulation is unworkable.[36]

The analytical implication is that regulated advertising can contract while political influence continues through other channels. A reduction in formally purchased political ads does not establish a reduction in manipulation. It may change which actors can communicate effectively and which messages remain publicly archived. Evaluation must examine those changes rather than treat platform withdrawal as either definitive regulatory success or definitive failure.

5.4 Platform systems and electoral risk

The DSA contains general intermediary and platform procedures and additional duties for designated very large online platforms and search engines. Its structure distinguishes actionable illegal content from systemic risks that may arise through lawful content and service design. Risk assessment and mitigation under Articles 34–35 therefore provide a way to examine the operation of recommendation, advertising and related systems in electoral contexts. These duties do not convert all political misinformation into illegal content.[37]

The Commission's electoral guidelines identify practical measures concerning election-specific risk assessment, cooperation, local expertise, incident response and generative-AI risks. They guide implementation of statutory obligations; the guidelines themselves should not be described as an independent criminal ban or as a duty imposed identically on every small platform. The Commission's 2025 toolkit further addresses application by Digital Services Coordinators.[38]

The distinction matters for constitutional analysis. A rule directed at distribution incentives can require a platform to investigate whether a coordinated campaign exploits its design without requiring the regulator to pronounce on the truth of every political proposition. An effective measure might concern deceptive accounts, advertising attribution or the recommendation of already assessed material. Each measure should identify a causal pathway and explain why its scope is proportionate.

Systemic governance still presents a speech risk. A provider may adopt broad automated restrictions to demonstrate that it has acted. If 'electoral risk' becomes a label for suppressing disputed political views, a preventive framework can function as opaque censorship. Review should ask whether mitigation concerns identifiable conduct or design features, whether alternatives were examined and whether affected users received an explanation and a route to contestation.

The DSA's procedural framework includes statements of reasons for relevant restrictions, internal complaints and specified independent dispute-settlement possibilities. It also preserves a prohibition on general monitoring obligations. Transparency and user choice concerning recommendation, including the relevant non-profiling option for designated major platforms, can support agency. These mechanisms should be evaluated

[36] Meta, Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation, 25 July 2025, updated 6 October 2025.
[37] Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1, arts 8, 14, 16–17, 20–21, 26–28, 34–35, 37–40, 51, 56 and 74.
[38] 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, C/2024/3014, OJ C, 26 April 2024; announced 26 March 2024. European Commission, Commission presents new best-practice election toolkit on the Digital Services Act, 20 February 2025.

for their accessibility and speed in election disputes, rather than assumed to restore a lost opportunity simply because an appeal exists.[39]

Evidence access is another important component. The Commission's researcher-access initiative explains a process through which qualified, vetted researchers can seek internal platform data concerning systemic risks. Its significance is that assessment need not rely exclusively on the provider's public account. Access nevertheless requires safeguards for personal data, confidentiality and information security; it does not make all internal data available to the public.[40]

The EDPB's September 2026 guidance on the interplay between the DSA and GDPR reinforces the need to reconcile platform compliance with data protection. From the article's perspective, an audit should not remedy one democratic risk by creating another through indiscriminate collection of political information. Secure access environments, purpose-specific requests and aggregate reporting can help separate investigation of distribution from identification of voters.[41]

The Commission's December 2024 proceedings against TikTok concerning the Romanian presidential election illustrate attention to recommender systems and coordinated inauthentic activity. The announcement records suspected breaches and the opening of proceedings. It is not proof of a final infringement finding or that a platform's algorithm caused an election outcome. The example is used here to identify the object of regulatory investigation, rather than to make a current claim about the ultimate outcome of the proceedings.[42]

5.5 AI systems and the limits of high-risk classification

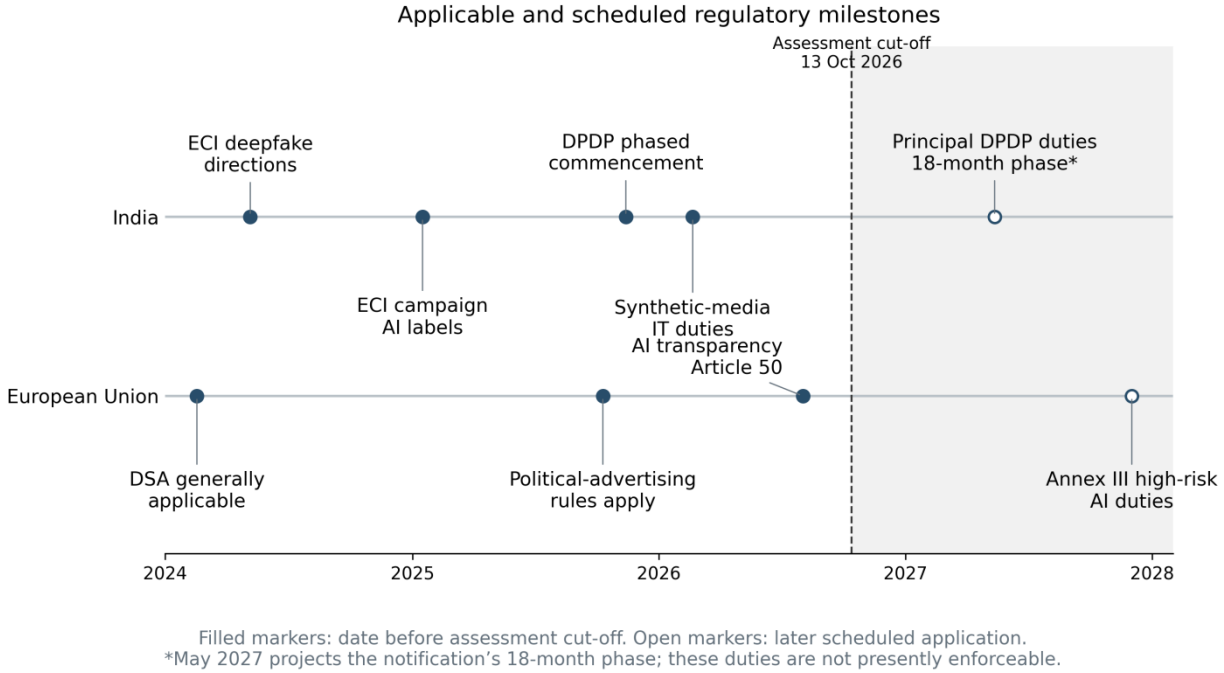
The AI Act adds a different set of controls. Article 5 prohibits specified manipulative or deceptive techniques and exploitation of particular vulnerabilities where the statutory conditions, including significant harm, are met. It does not ban all political persuasion, emotional campaigning or personalised communication. Democratic concerns may arise without satisfying those prohibited-practice thresholds, which is one reason the advertising and platform regimes remain necessary.[43]

Annex III point 8(b) identifies AI systems intended to influence election or referendum outcomes or voting behaviour as high-risk, while excluding systems whose outputs are not directly exposed to people, such as specified administrative or logistical campaign tools. Classification requires attention to intended purpose, the applicable Article 6 framework and the actual system. High-risk status ordinarily entails compliance duties; it is not itself a categorical prohibition of the system.[44]

The current timetable is equally important. The Commission's July 2026 implementation update states that Annex III high-risk rules apply from 2 December 2027. On the October 2026 cut-off, those requirements cannot be credited as fully applicable protections. The delay creates a period in which existing platform, advertising, data and transparency obligations must do much of the work. Figure 3 makes this temporal distinction visible.[45]

[39] DSA, Regulation (EU) 2022/2065.
[40] European Commission, Commission facilitates data access for researchers under the Digital Services Act, 2 July 2025, updated 24 September 2025.
[41] European Data Protection Board, Guidelines 3/2025 on the interplay between the DSA and the GDPR, version 2.0, 17 September 2026, section 2.7.
[42] European Commission, Commission opens formal proceedings against TikTok on election risks under the Digital Services Act, IP/24/6487, 17 December 2024.
[43] European Commission AI Act Service Desk, Article 5: Prohibited AI practices, current consolidated article text, accessed 13 October 2026.
[44] Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 2024/1689, 12 July 2024, arts 5–6, 9–15, 26–27, 50 and 113, and Annex III point 8(b); current article texts accessed through the European Commission AI Act Service Desk.
[45] Commission, AI Omnibus implementation update, 27 July 2026.

Figure 3 A timeline of selected regulatory milestones



Author's compilation from ECI directions, Indian commencement notifications, the EU political-advertising application notice and Commission AI implementation materials. Later dates are scheduled, not current safeguards.[46]

An additional boundary concerns rights impact assessment. Article 27 attaches its mandatory assessment to specified categories of deployer and use. An ordinary private campaign should not be assumed to owe that obligation solely because it deploys an electoral high-risk system. This limitation leaves a policy question about whether election-specific public impact reporting should apply to significant campaign deployments even where the particular Article 27 duty does not.[47]

Article 50 addresses information about direct AI interaction and specified generated or manipulated material. It distinguishes machine-readable marking by providers from disclosure by deployers. Its treatment of deepfakes includes adapted disclosure for evident artistic, satirical or similar works, while public-interest AI-generated text is subject to an exception involving human review or editorial control and responsibility. These distinctions should not be collapsed into a requirement that every AI-assisted political sentence carry the same warning.[48]

The Commission's transparency FAQs identify 2 August 2026 as the Article 50 application date and describe a limited transitional arrangement concerning marking and detection for systems already on the market. This prevents the deferral of high-risk requirements from being misread as a deferral of every AI transparency duty. Nevertheless, transparency about generation does not disclose the complete targeting and delivery process.[49]

There is also a question of communicative design. A prominent, intelligible disclosure can assist a voter who would otherwise mistake an artificial spokesperson for a human. A technically present marker that disappears

[46] ECI, Social Media Guidelines, 6 May 2024. ECI, AI Labelling Advisory, 16 January 2025. DPDP commencement notification, GSR 843(E). IT Amendment Rules 2026, GSR 120(E). Commission, Political Advertising Rules, 10 October 2025. European Commission, Transparency obligations under Article 50 of the AI Act, current FAQs, accessed 13 October 2026. Commission, AI Omnibus implementation update, 27 July 2026.
[47] European Commission AI Act Service Desk, Article 27: Fundamental rights impact assessment for high-risk AI systems, current article text, accessed 13 October 2026.
[48] European Commission AI Act Service Desk, Article 50: Transparency obligations for providers and deployers of certain AI systems, current article text, accessed 13 October 2026.
[49] Commission, Article 50 Transparency FAQs.

in a forwarded recording cannot offer the same protection. The constitutional assessment concerns notice at the point of exposure, accompanied where necessary by an accessible explanation, rather than compliance measured only at the point of original production.

5.6 Enforcement fragmentation and the scope of protection

EU governance distributes enforcement across data-protection authorities, Digital Services Coordinators, Commission powers concerning designated services, AI oversight and national electoral institutions. Specialisation allows different kinds of expertise, but an influence operation can cross several mandates. The decisive practical question is whether evidence collected by one authority can lawfully and promptly inform action by another, with the affected parties able to challenge the resulting decision.

The framework's reach is also uneven. General platform duties are distinct from the enhanced obligations of designated major services. Private messaging, small services, offshore actors and covertly funded accounts may expose boundaries in the relevant scope or enforcement capacity. Territorial reach in legislation does not guarantee cooperation, identification or collection of evidence from every actor abroad.

The EU therefore supplies a stronger formal account of distributed responsibility than a content-only regime, but it does not resolve the constitutional problem by legislative accumulation. The adequacy of the architecture depends on institutional coordination, relevant evidence and remedies that operate within the political opportunity at stake. The following comparison identifies where those requirements are addressed and where the gap remains.

6. COMPARATIVE FINDINGS

6.1 Responsibility follows different regulatory objects

The first finding concerns the object of regulation. India's election framework primarily identifies participants, campaign conduct, expenditures and unlawful material. Its 2026 intermediary amendments add specific duties concerning synthetic representations and their handling. The EU allocates responsibility more explicitly across political data, advertising services, platform systems and AI products or deployments. This is a difference in emphasis, not a claim that India has only reactive rules or that the EU has only preventive ones.

Table 3 Functional comparison at 13 October 2026

Function	India	European Union
Constitutional protection	Expression, equality, privacy and constitutional electoral supervision.	Democratic principles and Charter rights within their fields of application.
Political personal data	General DPDP architecture enacted; principal processing and rights provisions remain in the 18-month phase.	GDPR protections plus political-advertising targeting restrictions.
Campaign sponsorship	Expenditure and campaign-disclosure mechanisms; no complete statutory cross-platform repository identified in the instruments examined.	Political-advertising labels, transparency notices and repository provisions.
Synthetic representations	ECI campaign directions and 2026 IT synthetic-media duties, with distinct scopes and triggers.	AI Act Article 50 duties applicable subject to relevant scope and transitions.
Platform distribution	Intermediary compliance and campaign cooperation; no equivalent general election-specific statutory audit duty identified.	DSA systemic-risk duties for designated major services; duties differ for other services.

Electoral high-risk AI	Fragmented statutory and administrative controls; no equivalent horizontal high-risk classification identified in the instruments examined.	Annex III electoral classification enacted; main requirements scheduled for 2 December 2027.
Independent evidence access	No comparable general vetted-researcher entitlement identified in the electoral instruments examined.	DSA data-access framework with vetting, confidentiality and privacy safeguards.
Review and enforcement	ECI, intermediary complaints, public-law review and election-law remedies with different scopes.	Specialised national and EU authorities and platform/judicial remedies; coordination remains necessary.

Author's qualitative synthesis of the instruments discussed in sections 4–5. "Not identified" is bounded by the stated source corpus; coverage is not an effectiveness score.

Both systems combine prevention and response. Indian advertising pre-certification acts before publication, while European notice-and-action mechanisms respond to identified content. The relevant distinction is whether preventive oversight reaches the distribution process. A pre-certified message can still be delivered to an undisclosed audience on a problematic basis. A labelled deepfake can still be used as part of a coordinated campaign. Compliance at one point therefore cannot substitute for responsibility at the other points.

The allocation of duty should follow practical control. A candidate may authorise a message while a platform determines its actual delivery. A contractor may build the audience without publishing the advertisement. The provider of a generative system may supply a model without directing any electoral campaign. A connected regulatory account must identify those differences, rather than making the most visible candidate or host solely responsible for every stage.

6.2 Transparency must include actual exposure

The second finding concerns the information required for scrutiny. A sponsor label explains who commissioned a communication. A synthetic-content label explains something about its production. A notice concerning targeting explains the basis on which recipients were selected. An exposure record shows what the delivery system actually did. These disclosures answer different questions. The constitutional value of transparency is limited if only one is available.

The distinction between selected and actual audiences is especially important. A campaign can select a broad audience and let an optimiser allocate impressions. A public record of the campaign's requested targeting then describes a choice that does not fully explain actual exposure. Conversely, individual-level recipient records would create a serious privacy risk. The proposed solution is aggregate information sufficiently detailed to reveal distribution patterns, subject to controls against re-identification.

This produces a specific comparative recommendation. India should add campaign repositories and appropriate delivery information to its developing provenance requirements. The EU should evaluate whether its existing repositories and evidence-access arrangements make algorithmically allocated exposure inspectable. Neither conclusion assumes that publishing source code is necessary. An audit may need selected inputs, optimisation objectives, aggregated outputs and relevant tests rather than unrestricted disclosure of proprietary systems.

6.3 Election time changes the meaning of an effective remedy

The third finding concerns time. Electoral influence can be concentrated in a period when a correction delivered several days later has limited practical value. Rapid removal may also silence a lawful speaker at precisely that point. An effective remedy must therefore be evaluated from both perspectives: the person harmed by manipulation and the person harmed by erroneous restriction.

An electoral remedy has at least two purposes. It can stop an ongoing interference, and it can make relevant evidence available for later adjudication. These purposes may call for different actions. A temporary restriction on a fabricated official polling instruction can be accompanied by a public correction and secure retention. A disputed satirical recording may require a clarification or label while contextual review proceeds. Permanent deletion without preservation can undermine both later enforcement and review of the restriction itself.

Existing election litigation and digital grievance procedures must be respected in their own scopes. The proposal is not to use content complaints to invalidate a completed election without satisfying election-law conditions. A judicial order reviewing an online restriction and an election petition challenging a result have different functions. The framework instead asks whether the immediate dispute can receive lawful, appropriately narrow scrutiny before the opportunity to communicate or vote is irretrievably lost.

6.4 Labels and consent leave collective harms unresolved

The fourth finding concerns the relationship between individual rights and collective accountability. Consent can protect a data subject's choice to receive communication, but cannot alone expose inconsistent promises to separate groups. A label can disclose an artificial image, but cannot alone show a concealed sponsor's funding or the manipulation of recommendation signals. Democratic accountability requires some information to become available beyond the directly affected individual.

This does not justify making every recipient's political preferences public. Instead, the framework identifies a carefully delimited public interest in the organisation of paid or coordinated influence. The relevant information concerns actors, funding, messages and aggregate distribution. A person's reading history, party membership or political opinion should not become a public compliance record merely because an advertisement reached them.

The comparative implication is that data protection and election transparency should be designed together. A disclosure rule that publishes identifiable political audiences can undermine privacy. A privacy rule interpreted to prevent any scrutiny of organised targeting can undermine accountability. Purpose-specific records, aggregation and secure independent access offer a more proportionate way to address the conflict.

7 AN ELECTORAL CONTESTABILITY FRAMEWORK

7.1 Four requirements for organised algorithmic influence

The proposed framework applies to organised electoral influence, with graduated duties determined by payment, coordination, targeting intensity, reach and the role of the actor. It asks four questions. Can responsibility for the communication be traced? Can the legal basis and method of targeting be examined? Can relevant aspects of actual distribution be independently assessed? Can harmful influence and erroneous regulatory intervention receive a timely, reasoned review? These are proposed normative requirements, not a claim that either jurisdiction already recognises a complete four-part legal test.

Traceability should identify the sponsor, beneficial controller and relevant campaign contractor. It should not compel every citizen who expresses political views to register with an election authority. Scrutiny of targeting should concern the categories and sources of data and the method of selecting or excluding recipients. Assessment of distribution should provide evidence about reach, recommendation and amplification at an appropriate level of aggregation. Review should be accessible to persons affected by manipulation and to speakers affected by restrictions.

The framework should not require proof of a changed election outcome before every preventive duty applies. Record-keeping, sponsorship disclosure and a lawful targeting basis can be justified by the risks of organised influence and the feasibility of compliance. Severe sanctions, criminal liability or invalidation of an election remain subject to their own legal standards. Distinguishing these thresholds prevents preventive governance from lowering the evidential burden for punitive conclusions.

7.2 Targeted legislative reform in India

India's most practical route is to connect its existing election and digital frameworks through targeted legislation. A law should define organised digital campaign services and paid or coordinated electoral communication in functional terms. It should specify responsible actors, record requirements, competent authorities, sanctions and review procedures. ECI directions can implement a clear legislative framework; they should not carry the entire burden of creating new offences or comprehensive restrictions on political-data processing.

A public campaign repository should contain the communicated material, its sponsor and beneficial controller, the dates and platforms of dissemination, expenditure ranges, relevant targeting criteria and aggregate delivery information. Links between versions should allow scrutiny of materially inconsistent claims. The repository should be searchable in relevant languages and preserve a transparent record of corrections or restrictions. Small campaigns should receive simplified reporting tools, while material targeting and expenditure obligations remain enforceable.

Repository design requires limits. Recipient identities should not be public. Small-cell delivery data should be suppressed or combined to reduce re-identification. Material adjudged unlawful should not remain openly accessible merely because it formed part of a campaign; restricted evidential retention can serve later review. Archives should distinguish the original message, the reason for restriction and any verified correction, without unnecessarily republishing intimate or defamatory material.

Political-data rules should address information revealing or used to infer religion, caste, political preferences and other demonstrably sensitive attributes in the electoral context. The recommendation is a campaign-specific approach to prohibited profiling, data sources and prohibited combinations, rather than an assumption that every data category must be treated identically. Separate, intelligible consent should be required where permissible political targeting uses personal data. Contextual communication based on the subject matter or general location can provide a less intrusive alternative.

Consent should not legalise every practice. Targeting designed to exploit acute vulnerability, suppress lawful voting or conceal materially misleading official instructions should remain restricted where precise statutory elements are satisfied. The law should also distinguish an individual's voluntary relationship with a party from a data broker's construction of a predictive audience from unrelated records. Contractors and platforms should keep evidence sufficient to establish the data flow and relevant authorisation.

7.3 Platform duties calibrated to control and scale

Platforms with substantial electoral reach should conduct election-specific risk assessments concerning their recommendation, advertising and synthetic-media systems. The assessment should identify foreseeable misuse, contextual language requirements, incident response and less restrictive mitigation options. A public summary should explain the evaluated risks and adopted measures, while a confidential annex can protect security-sensitive details and information capable of identifying individuals.

Scale should be measured by relevant reach and control, not simply a general user-count threshold. A small service used intensively in a particular constituency may have a significant local role; a large neutral infrastructure provider may exercise less direct control over political exposure. Graduated duties should recognise those differences. It would be disproportionate to impose a full platform audit on every local community group administering a messaging channel.

Platforms should retain records of material campaign advertisements and significant moderation interventions for a defined period compatible with privacy and applicable election litigation. The relevant record should show the original content, responsible account, available sponsorship information, targeting settings, aggregate exposure and the reason for intervention. Retention should be governed by access controls and a defined deletion schedule rather than indefinite accumulation of political data.

Independent assessment should occur through authorised researchers and appropriately constituted technical auditors with conflict-of-interest safeguards. The goal is verifiable scrutiny of specific electoral risks, not a requirement that a platform submit all political communication to continuous state observation. Secure environments and restricted queries can allow analysis without distributing raw personal data. Platforms should have a procedure to object to a request on specified grounds, with review by an independent decision-maker.

7.4 Procedural safeguards against political censorship

Content restrictions should distinguish factual impersonation and demonstrably false voting instructions from contested political claims, opinions and satire. The first categories can present an immediate obstacle to the franchise. The latter demand particular caution because an authority's view of political truth may be partisan or incomplete. A restriction should identify the applicable legal provision and the evidence supporting each necessary element.

Notice should ordinarily identify the material, the reason, the deciding authority or platform procedure, the scope and duration of the measure and the available review route. An urgent exception to prior notice should require a documented reason and prompt subsequent notice where lawful. Measures should be time-limited when the factual assessment is provisional. Restoration should be available when an initial restriction proves unjustified.

Human contextual review is particularly important where classification turns on satire, consent, source authenticity or a language-specific meaning. Detection tools can identify items requiring attention and support comparison with authenticated records. They should not be treated as an infallible judge of truth or authorisation. Public explanations should make uncertainty visible, especially where a contested recording has not been conclusively authenticated.

Correction and disclosure should be considered alongside removal. A verified polling clarification can be disseminated by an election authority without resolving every accusation about campaign motives. A sponsorship omission can sometimes be repaired through conspicuous disclosure and a repository update. A lawful satire may benefit from contextual presentation rather than deletion. The choice depends on urgency, harm, evidence and the adequacy of the less restrictive measure.

Independent review should be organised for election time. A specialised urgent procedure can review the legality and scope of a significant restriction without becoming a general appellate forum for political disagreement. Judicial scrutiny should remain available, with reasons and access to the underlying evidence consistent with confidentiality and security. Institutional independence matters because both public and private decision-makers may otherwise be pressured to favour an incumbent or a commercially powerful actor.

7.5 Applying the framework to difficult scenarios

Table 4 applies the framework to hypothetical practices. It illustrates why the analysis cannot be reduced to whether AI was used. A disclosed translation and an impersonated polling announcement may both involve synthetic audio while calling for very different legal responses. Similarly, profiling and an apparently organic influence operation create questions that a synthetic-content label may not answer.

Table 4 Hypothetical applications of electoral contestability

Hypothetical practice	Indian legal question	EU legal question	Proportionate response to examine
Candidate uses an authorised AI translation of an authentic speech.	Campaign disclosure and relevant good-faith/accessibility exclusions.	Applicable generation or interaction disclosure; scope and exceptions.	Preserve legitimate communication; disclose material synthetic alteration where required.

Cloned election official announces a false polling date.	Impersonation, applicable election law and urgent lawful intervention.	Illegal-content rules and relevant AI transparency/prohibited-practice conditions.	Verified public correction, narrow urgent restriction and retained evidence.
Broker-built audience uses inferred religion for paid election ads.	Actual DPDP commencement and scope; absence of a dedicated equivalent political-profile rule.	GDPR sensitivity and Article 18 targeting conditions.	Investigate the data flow; restrict unlawful targeting while protecting lawful speech.
Paid contractors distribute labelled synthetic material as spontaneous support.	Attribution, expenditure and deceptive coordination.	Political-advertising definition and platform systemic-risk obligations.	Disclose beneficial sponsor and coordination; audit distribution.
Detector flags a clearly contextualised satire on the eve of polling.	Relevant scope, expression, legal ground and urgent review.	Artistic/satirical disclosure treatment and procedural safeguards.	Contextual human review, explanation and prompt restoration if restriction is unjustified.

Hypothetical legal stress tests, not documented incidents. Each conclusion depends on the statutory elements, evidence, actor and applicable dates.

The scenarios also expose the limits of legal transplantation. A European first-party-data requirement cannot be imported into Indian electoral administration merely through an advisory; legislation and institutional capacity must support it. Conversely, an Indian rapid-response model should not be copied without examining the applicable notice, reasons and appeal requirements. Functional comparison identifies the problem a measure addresses and the legal conditions for introducing it.

Two scenarios deserve particular attention. A sponsor may purchase broad reach while a platform independently optimises the audience toward a vulnerable group. Allocating responsibility solely to the advertiser's selected criteria misses the platform's control. Alternatively, a campaign may distribute a disclosed AI-generated message through concealed contractors who manufacture the appearance of spontaneous support. In that case, generation disclosure can coexist with coordination deception. The framework requires distinct records and duties for each activity.

7.6 Evaluation without invented effectiveness scores

A credible evaluation programme should publish indicators tied to specific duties. Sponsorship completeness can be assessed by the proportion of sampled paid messages linked to a verifiable beneficial sponsor. Targeting accountability can be assessed through audits of relevant data sources and consent records. Distribution visibility can be assessed by the availability and reliability of aggregate delivery data. Procedural fairness can be assessed through reason-giving, contextual review, reversals and the time required for urgent appeals.

Each indicator requires a declared sampling frame and denominator. A count of removed items is insufficient: it can rise because harmful conduct increased, detection improved or enforcement became overbroad. Appeal reversals also require interpretation, because a low reversal rate may reflect correct initial decisions or an inaccessible appeal system. Metrics should therefore be reported with limitations and independent assessment rather than converted automatically into a single national score.

Future empirical research can examine the implementation of the two frameworks using a common protocol. It could sample a defined set of campaign communications, compare repository completeness, submit standardised information requests and examine documented complaint outcomes. Such a study would require ethical review where appropriate, lawful access to data and measures to protect political privacy. The present

article provides the doctrinal categories for that work; it does not report results from an investigation that has not been conducted.

Accessibility should also be evaluated. Researchers should examine whether voters can understand notices, lodge complaints in the relevant language and use review procedures without prohibitive cost. The issue is especially acute for audio-based communication and people with limited literacy or disabilities. A technically compliant disclosure that the intended recipient cannot perceive or understand offers weak constitutional protection.

Cross-border cooperation should focus on specific evidence and actors. Authorities need procedures for preserving campaign records, identifying responsible service providers and coordinating lawful requests. Blanket restrictions justified by an undifferentiated reference to foreign interference risk restricting legitimate diaspora participation, journalism and international debate. The legal design should identify prohibited financing, covert control or deceptive conduct while preserving lawful transnational communication.

Gendered and identity-based abuse requires similarly specific attention. Synthetic intimate material and impersonation can deter candidates from public participation, while caste or religious profiling can combine privacy invasion with discriminatory exclusion. Effective protection requires accessible victim procedures and restraint in republishing harmful material as evidence. These issues should be integrated into election-risk assessment instead of being treated as incidental effects unrelated to participation.

The model is institutionally demanding but can be introduced in stages. Sponsorship and evidence-preservation requirements can establish an initial foundation. Political-data restrictions and campaign repositories can then make organised activity more visible. Independent access and rapid review can address disputes about distribution and enforcement. Each stage should be assessed for cost, accessibility and rights effects before expansion, with technical obligations revised through an accountable process rather than open-ended executive discretion.

8 CONCLUSION

Algorithmic electoral manipulation poses a problem of constitutional accountability because influence can be distributed across data collection, message generation, audience selection and platform delivery. Neither authenticity labels nor a general prohibition on falsehood provides a complete response. Legitimate political persuasion must remain protected, and the legal elements of particular wrongs must be established rather than inferred from the use of AI.

The India–EU comparison identifies different allocations of responsibility. India combines constitutional election supervision, campaign rules and increasingly specific intermediary duties, but lacks a sufficiently connected account of political data and observable distribution. The EU supplies a more differentiated formal architecture, while facing fragmented enforcement, boundaries in material scope and postponed high-risk AI requirements. These findings concern legal design; they do not establish an empirical ranking of electoral protection.

The article's proposed contribution is an electoral contestability framework linking traceable responsibility, scrutinised targeting, independent assessment of distribution and timely review. It supports targeted reform in India and a practical evaluation of the EU's existing layers. Its constitutional premise is that voters and political competitors should be able to examine organised influence without exposing individual political beliefs or surrendering debate to a public authority's determination of truth.

The central regulatory task is to make the infrastructures of electoral influence accountable to law. That requires preventive obligations and evidence access, but also reasons, proportionality and independent judicial scrutiny. A democracy protects electoral agency when citizens can challenge both concealed manipulation and unjustified restrictions on political expression.

REFERENCES

Indian Legislation and Regulatory Materials

1. Constitution of India, arts 14, 19, 21, 324 and 326.
2. Digital Personal Data Protection Act 2023, ss 3, 4–6, 9–10, 11–17 and 18–26.
3. Digital Personal Data Protection Rules 2025, GSR 846(E), 13 November 2025, rr 1, 3, 12 and 17.
4. Election Commission of India, Advisory for labelling synthetic/AI generated content used by Political Parties for election campaigning, No 491/Social media-SOP/2025/Communication, 16 January 2025.
5. Election Commission of India, General Elections and bye-elections 2026: ECI action on unlawful social media content, 19 April 2026, Press Information Bureau release 2253528.
6. Election Commission of India, Instructions with respect to use of Social Media in Election Campaigning, 25 October 2013, reproduced in Social Media and Fake News training materials, updated 31 August 2024.
7. Election Commission of India, Responsible and ethical use of Social Media platforms by political parties and their representatives, 6 May 2024.
8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E), 10 February 2026, effective 20 February 2026.
9. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, consolidated text updated 10 February 2026, rr 2(1)(wa), 3, 3A and 4.
10. Information Technology Act 2000, ss 66C, 66D, 69A and 79.
11. Internet and Mobile Association of India and participating platforms, Voluntary Code of Ethics for the General Elections 2019, 20 March 2019, reproduced by the Election Commission of India in its social media instructions.
12. Ministry of Electronics and Information Technology, Government Strengthens Regulatory Framework to Address AI-Generated Deepfakes, 6 August 2026, Press Information Bureau release 2295500.
13. Ministry of Electronics and Information Technology, commencement notification under s 1(2) of the Digital Personal Data Protection Act 2023, GSR 843(E), 13 November 2025.
14. Representation of the People Act 1951, ss 77–78, 100, 123 and 126.

Judicial Decisions

1. Association for Democratic Reforms v Union of India, 2024 INSC 113, Supreme Court of India, 15 February 2024.
2. Case C-252/21 Meta Platforms and Others v Bundeskartellamt, EU:C:2023:537, Court of Justice of the European Union, 4 July 2023.
3. Case C-446/21 Schrems v Meta Platforms Ireland, EU:C:2024:834, Court of Justice of the European Union, 4 October 2024.
4. Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1, Supreme Court of India, 24 August 2017.
5. Mohinder Singh Gill v Chief Election Commissioner (1978) 1 SCC 405, Supreme Court of India, 2 December 1977.
6. Shreya Singhal v Union of India (2015) 5 SCC 1, Supreme Court of India, 24 March 2015.

European Union legislation and regulatory materials

1. Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7–8, 11, 21, 39, 47 and 51–52.
2. Commission Implementing Regulation (EU) 2025/1410 of 9 July 2025 on the format, template and technical specifications of labels and transparency notices of political advertisements under Regulation (EU) 2024/900.
3. Consolidated Version of the Treaty on European Union [2012] OJ C326/13, arts 2 and 10.

4. European Commission AI Act Service Desk, Article 27: Fundamental rights impact assessment for high-risk AI systems, current article text, accessed 13 October 2026.
5. European Commission AI Act Service Desk, Article 50: Transparency obligations for providers and deployers of certain AI systems, current article text, accessed 13 October 2026.
6. European Commission AI Act Service Desk, Article 5: Prohibited AI practices, current consolidated article text, accessed 13 October 2026.
7. European Commission, AI Omnibus enters into force, 27 July 2026, updated 31 July 2026; revised Annex III application date 2 December 2027.
8. European Commission, Commission facilitates data access for researchers under the Digital Services Act, 2 July 2025, updated 24 September 2025.
9. European Commission, Commission opens formal proceedings against TikTok on election risks under the Digital Services Act, IP/24/6487, 17 December 2024.
10. European Commission, Commission presents new best-practice election toolkit on the Digital Services Act, 20 February 2025.
11. 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, C/2024/3014, OJ C, 26 April 2024; announced 26 March 2024.
12. European Commission, New EU rules on political advertising come into effect, 10 October 2025.
13. European Commission, Transparency obligations under Article 50 of the AI Act, current FAQs, accessed 13 October 2026.
14. European Data Protection Board, Guidelines 3/2025 on the interplay between the DSA and the GDPR, version 2.0, 17 September 2026, section 2.7.
15. European Data Protection Board, Guidelines 8/2020 on the targeting of social media users, version 2.0 adopted 13 April 2021; references amended 7 July 2021.
16. Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1, arts 5–9, 13–15, 21–22, 35 and 77–82.
17. Regulation (EU) 2022/2065 (Digital Services Act) [2022] OJ L277/1, arts 8, 14, 16–17, 20–21, 26–28, 34–35, 37–40, 51, 56 and 74.
18. Regulation (EU) 2024/1689 (Artificial Intelligence Act), OJ L, 2024/1689, 12 July 2024, arts 5–6, 9–15, 26–27, 50 and 113, and Annex III point 8(b); current article texts accessed through the European Commission AI Act Service Desk.
19. Regulation (EU) 2024/900 on the transparency and targeting of political advertising, OJ L, 2024/900, 20 March 2024, arts 3, 5, 11–13, 18–19 and 30.

Research literature and other primary materials

1. Andrew M Guess and others, ‘How Do Social Media Feed Algorithms Affect Attitudes and Behavior in an Election Campaign?’ (2023) 381 Science 398–404. https://doi.org/10.1126/science.abp9364
2. Bobby Chesney and Danielle Citron, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (2019) 107 California Law Review 1753–1820.
3. Cristian 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. https://doi.org/10.1177/2056305120903408

4. Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8(2) Internet Policy Review.https://doi.org/10.14763/2019.2.1410
5. Francesco Salvi, Manoel Horta Ribeiro, Riccardo Gallotti and Robert West, 'Author Correction: On the Conversational Persuasiveness of GPT-4' (2026) Nature Human Behaviour, published 3 September 2026.https://doi.org/10.1038/s41562-026-02588-0
6. Francesco Salvi, Manoel Horta Ribeiro, Riccardo Gallotti and Robert West, 'On the Conversational Persuasiveness of GPT-4' (2025) 9 Nature Human Behaviour 1645–1653, as corrected in September 2026.https://doi.org/10.1038/s41562-025-02194-6
7. Frederik J Zuiderveen Borgesius and others, 'Online Political Microtargeting: Promises and Threats for Democracy' (2018) 14(1) Utrecht Law Review 82–96. https://doi.org/10.18352/ulr.420
8. Karen Yeung, 'Hypernudge: Big Data as a Mode of Regulation by Design' (2017) 20(1) Information, Communication & Society 118–136. https://doi.org/10.1080/1369118X.2016.1186713
9. Meta, Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation, 25 July 2025, updated 6 October 2025.
10. Tom Dobber, Ronan Ó Fathaigh and Frederik J Zuiderveen Borgesius, 'The Regulation of Online Political Micro-Targeting in Europe' (2019) 8(4) Internet Policy Review. https://doi.org/10.14763/2019.4.1440