Panjab University Law Magazine (MAGLAW)
ISSN: 2582-3507, Volume IV Issue II, pp 194-213

SOCIAL MEDIA, DIGITAL CAMPAIGNING, AND THE FUTURE OF ELECTION LAW IN INDIA- TOWARDS DECLINE OR RENEWAL

Anushka Sharma*

ABSTRACT

India's electoral ecosystem has been reshaped by social media, targeted advertising, and algorithmic amplification at a pace that outstrips the evolution of its regulatory framework. This paper examines the resulting mismatch between platformed political communication and India's statutory architecture, principally the Representation of the People Act, the Election Commission's Model Code of Conduct, and the intermediary-liability regime under the Information Technology Act, and demonstrates how these instruments, drafted for an analogue era, leave doctrinal and procedural lacunae when applied online. Building on Supreme Court jurisprudence from Shreya Singhal to Anuradha Bhasin, and a comparative review of US, UK, and EU regulatory responses, the paper interrogates four core risks: algorithmic amplification of content, opaque micro-targeting and hidden financing, cross-border interference, and weak enforcement of transparency and silence-period rules. The analysis finds promise in India's Digital Personal Data Protection Act (2023) but highlights its broad state exemptions, centralised enforcement, and lack of explicit electoral safeguards. The paper proposes a calibrated, rights-respecting reform package comprising narrow DPDP carveouts; decentralised, independent enforcement capacity; mandatory digital imprints and ad-disclosure; platform risk assessments and algorithmic audits; and coordinated ECI–data-regulator mechanisms. Such measures, it argues, can protect voter autonomy and electoral integrity without unduly constraining legitimate political speech, thereby preserving democratic legitimacy in an age of commercial platforms and algorithmic mediation.

Keywords: *Digital Campaigning; Intermediary Liability; Data Protection; Algorithmic Amplification; Electoral Transparency.*

1. INTRODUCTION

India's electoral democracy rests on the twin constitutional commitments of free expression and fair representation. In the twenty-first century, however, that balance is being renegotiated in real time as digital campaigning and social media

* LLB, Department of Laws, Panjab University, Chandigarh.

have tremendously reshaped the modalities of political communication. Where print media and broadcast once structured political messaging, platforms such as Facebook, Twitter, YouTube, WhatsApp and Google Ads now function as primary channels for political mobilisation, persuasion, and debate—often in ways that evade the assumptions of older legal instruments.

Digital tools have drastically altered the reach, speed, and targeting of audiences. Micro-targeted advertisements, platform-enabled virality (for example, forwarding messages on WhatsApp), and live-streamed events allow political actors to reach and engage with millions of voters directly, compressing message cycles and amplifying emotional rhetoric. Scholars and journalists have called the 2014 Lok Sabha campaign India's first major "social media election," noting the Bharatiya Janata Party's deliberate integration of multiple platforms and innovations such as the Chai Pe Charcha live events to stimulate real-time interaction and networked mobilisation.[1]

Electoral politics has now become fully integrated into a growing, global commercial digital media and marketing ecosystem that has already transformed how corporations market their products and influence consumers.[2]

While these technological affordances produce clear democratic benefits, including wider access to political information, new forms of participatory communication, and low-cost mobilisation for grassroots actors, they also create serious regulatory and constitutional problems. The problems include, but are not limited to

- The ability of false and misleading content to travel faster than verification,
- The provenance and funding of targeted online political advertising are often opaque.
- Platform algorithms rank and amplify content according to commercial rules that are neither transparent nor democratically accountable,
- And domestic electoral processes have become vulnerable to cross-border manipulation and sophisticated influence operations.

---

1 Ronojoy Sen, *From Chaiwala to Chowkidar: Modi's Election Campaigns Online and Offline* (ResearchGate, 2021).

2 P. Chahal, *Digital Political Marketing* (Sage 2013); LiveRamp, *Data-Driven Advertising Report* (2015); D. Rubinstein, "Social Media and Political Advertising," *Harvard Journal of Law & Technology* (2014); M. Schuster, *Political Microtargeting and Democracy* (Cambridge University, Press 2015).

These dynamics compel a recalibration of how electoral integrity and fundamental freedoms are to be protected in an algorithmic environment.[3]

India's statutory and institutional architecture principally comprises the Representation of the People Act, 1951, the Election Commission's Model Code of Conduct, and the intermediary-liability and content-removal regime under the Information Technology Act. This architecture was developed for a pre-platform era and contains doctrinal and procedural lacunae when applied to digital campaigning. The courts have been an important corrective, striking down manifestly overbroad restrictions on online speech while wrestling with state powers in times of crisis. In Shreya Singhal v. Union of India (2015)[4], the Supreme Court declared section 66A of the IT Act unconstitutional for being vague and overbroad, holding that it impermissibly constrains speech protected by Article 19(1)(a). Likewise, Anuradha Bhasin v. Union of India (2020)[5] engaged squarely with the legality and proportionality of internet shutdowns and emphasised that access to the internet is integral to the freedom of speech and press. Yet these judicial interventions, while landmark, have not produced a positive, pragmatic and comprehensive regulatory scheme tailored to the political economy of platformed information[6]; Section 3.1 will examine these cases in detail, highlighting their implications for digital campaigning and the regulation of social media in Indian elections.

This regulatory gap has practical consequences. The 2014 campaign demonstrated how quickly political actors can operationalise platform affordances to reshape public discourse long before regulators and courts developed calibrated responses; a pattern repeated in subsequent Indian elections.[7]

Such experiences across established democracies across the barriers of the nations underscore a common challenge, that is, the crafting of responses to digital

---

3 Morgan Meaker, "Ukraine War Prompts Europe's New Emergency Rules for the Internet," *WIRED*, April 25 2022.

4 *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.[1]Ronojoy Sen, *From Chaiwala to Chowkidar: Modi's Election Campaigns Online and Offline* (ResearchGate, 2021).

5 *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637.

6 Gautam Bhatia, *The Transformative Constitution: A Radical Biography in Nine Acts* 215 (HarperCollins, New Delhi, 2021).

7 Usha M. Rodrigues & Michael Niemann, "Social Media as a Platform for Incessant Political Communication: A Case Study of Modi's 'Clean India' Campaign," 11 *International Journal of Communication*, (2017).

political advertising, algorithmic amplification[8], and disinformation that do not suppress legitimate discourse.

Algorithmic amplification and targeted political messaging have been shown to influence voter behaviour globally, with multiple countries, including the US and UK, experiencing coordinated campaigns of computational propaganda.[9]

The United States has pursued disclosure and transparency mechanisms through the Federal Election Commission's rules on internet disclaimers;[10] the United Kingdom has introduced statutory guidance on "digital imprints" to identify responsibility for online political material[11]; and the European Union has enacted the Digital Services Act to increase platform accountability, require risk-assessments, and mandate transparency for targeted ads and recommender systems.[12] These divergent approaches illustrate the two central regulatory risks-under-regulation that permits manipulation and opacity, and over-regulation that curtails robust political debate.

Scholarly debate centres on three fault lines. First, the doctrinal fault line concerns how to interpret Articles 19(1)(a) and 19(2) in the platform era so that restrictions remain narrowly tailored, necessary, and proportionate. Second, the institutional fault line asks which public bodies, including the Election Commission, sectoral regulators, competition authorities, and independent digital regulators, should police online political influence and with what powers. Third, the technical fault line, which asks how to make platform practices such as algorithmic amplification and ad-targeting intelligible to regulators and citizens without importing excessive regulatory capture or stifling innovation. Each fault line raises difficult trade-offs between liberty, equality of access to the public sphere, and the integrity of the electoral process.

The fault lines identified above cannot be addressed without examining India's evolving privacy and data-governance regime. Transparency around data flows, user profiling, and targeted advertising lies at the heart of any effort to regulate

---

8 Ferenc Huszár, Sofia Ira Ktena, Conor O'Brien, Luca Belli, Andrew Schlaikjer and Moritz Hardt, "*Algorithmic amplification of politics on Twitter"* 118 Proceedings of the National Academy of Sciences of the United States of America e2025334119 (2021).

9 Woolley, Samuel C., and Howard, Philip N. *Computational Propaganda Worldwide: Executive Summary*. (Oxford Internet Institute, 2017).

10 Federal Election Commission, *Internet Disclaimers and Definition of "Public Communication"* (Final Rule, 11 C.F.R. §§ 110.11 & 100.26, 2022).

11 UK Electoral Commission, "*Digital Imprints: Statutory Guidance,"* (2023).

12 European Commission, "*Digital Services Act*," Europe Fit for the Digital Age, (2022).

political influence online. Consequently, the next section turns to the Digital Personal Data Protection Act, 2023 (DPDP Act) and related jurisprudence to assess how India's data-protection framework equips regulators to demand algorithmic disclosure while safeguarding fundamental rights under Articles 19(1)(a) and 21.

Against this background, this paper asks: How should Indian election law evolve to regulate online influence and digital campaigning without undermining constitutional freedoms? To answer this, the inquiry proceeds in three parts.

Part I situates digital campaigning within India's constitutional and statutory framework and identifies the doctrinal and institutional limitations that constrain effective regulation. Part II analyses the principal risks posed by unregulated online influence—disinformation and deepfakes, hidden political financing, algorithmic micro-targeting, and foreign interference—using recent Indian elections as illustrative case studies. Part III undertakes a comparative and pragmatic assessment of foreign regulatory models (U.S. disclosure regimes, U.K. imprints, the E.U.'s DSA and related instruments), evaluating which elements might be adapted for India's federal constitutional architecture and plural political economy.

Ultimately, this paper argues that regulating online influence is not merely a matter of electoral administration; it is a constitutional imperative. A calibrated regulatory response must protect free expression, ensure transparency and contestability of algorithmic systems, and strengthen institutional capacity for oversight—all while remaining sensitive to India's social diversity and political pluralism. The challenge is to design rules that can defend the conditions of democratic legitimacy in an information environment shaped by commercial platforms and algorithmic mediation.

1.1 Objectives of Study

This paper seeks to:

- **Analyse the Indian Legal Framework**

Examine how existing constitutional provisions and election laws address (or fail to address) digital campaigning and social-media influence in elections.

- **Assess Key Democratic Challenges**

Identify the major risks posed by online political activity—such as disinformation, hidden financing, and algorithmic targeting—drawing on recent Indian electoral experiences.

- **Recommend Practical Reform**

Suggest balanced regulatory measures, informed by comparative global practices, that can safeguard both free expression and electoral integrity in India.

2. RESEARCH METHODOLOGY

This paper uses a qualitative legal research design, combining doctrinal, comparative, and analytical methods to examine India's electoral law in the context of digital campaigning.

2.1 Doctrinal Method

This method involves interpreting primary legal sources[13], including constitutional provisions (Articles 19 and 21), statutes like the Representation of the People Act, the Information Technology Act, and the Digital Personal Data Protection Act, as well as Supreme Court judgments. The aim is to identify legal gaps and limitations in applying traditional electoral laws to digital platforms.

The analysis is guided by:

- Normative coherence[14]: alignment with constitutional rights[15]
- Temporal adequacy[16]: responsiveness to digital-era challenges, and Regulatory sufficiency[17]: clarity and enforceability of obligations.

2.2 Comparative Method

This paper examines legal frameworks from the United States, the United Kingdom, and the European Union, chosen for their diversity in regulating online political influence. These jurisdictions were selected based on:

---

13 India Ian Dobinson & Francis Johns, "Legal Research as Qualitative Research", in *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (European Academy of Legal Theory Series, Hart Publishing, 2007).

14 H. Koff, *et al.*, "How Green Are Our Laws? Presenting a Normative Coherence for Sustainable Development Methodology" *Environmental Policy and Governance* (2022).

15 M. Balkin, "Understanding Legal Understanding: The Legal Subject and the Problem of Legal Coherence", 103 *Yale L.J.* 105 (1993).

16 F. Serra, *et al.,* "Use of Context in Data Quality Management: A Systematic Literature Review" (2022) arXiv:2204.10655.

17 Jonas Lage, "Sufficiency and Transformation – A Semi-Systematic Literature Review of Notions of Social Change in Different Concepts of Sufficiency" 3 *Frontiers in Sustainability* 954660 (2022).

- Existing legal standards for political advertising;
- Platform accountability mandates;
- Independent regulatory institutions;
- Transparency requirements (e.g., ad disclaimers, digital imprints);
- Relevance to India's federal and constitutional context.

The method applies legal transposability[18], assessing which foreign elements can be adapted to Indian law.

2.3 Analytical Method

This approach critically evaluates the consistency and effectiveness of legal regimes in protecting electoral integrity. It goes beyond description to ask whether current laws are enforceable, whether they align with democratic values, and how they could be improved. This is applied throughout the paper, particularly in assessing state exemptions under the DPDP Act and the absence of ad-transparency obligations

2.4 Qualitative Framework

The research is non-empirical and entirely text-based, relying on statutes, case law, policy documents, academic literature, and regulatory texts from India and abroad. The study covers the period 2014–2024, during which digital tools became central to Indian elections. A key limitation is the lack of access to proprietary platform data[19] (e.g., algorithms targeting metrics[20]), though triangulation across doctrinal and policy sources ensures analytical reliability

3. CONTENT AND DATA ANALYSIS

India's digital ecosystem has expanded exponentially over the last decade. By 2024, approximately 886 million Indians were online, a figure that has been projected to exceed 900 million by this year.[21] This massive digital presence

---

18 Anthony Ogus, *Comparing Regulatory Systems: Institutions, Processes and Legal Forms in Industrialised Countries* (Centre on Regulation and Competition Working Paper No. 35, 2002).

19 European Commission, *Digital Services Act: Ensuring Transparency and Accountability in Online Platforms* (2022).

20 T Gillespie, *Custodians of the Internet: Platforms, Content Moderation and The Hidden Decisions That Shape Social Media* (Yale University Press, 2018)

21 Internet and Mobile Association of India (IAMAI) & Kantar, *Internet in India Report 2024* (2024)

underscores the critical need for a robust legal framework that will rigorously govern online political communication, data protection, and digital campaigning

3.1 Doctrinal Context: Constitutional and Legal Frameworks

Indian election law and constitutional provisions provide a solid foundation for regulating online influence. Articles 19(1)(a) and 19(2) of the Constitution guarantee freedom of speech and expression while permitting "reasonable restrictions" in the interests of sovereignty, integrity, public order, and electoral integrity. The Representation of the People Act, 1951 (RPA) and the Information Technology Act, 2000 (IT Act) also offer procedural and substantive norms for electoral conduct and imply obligations for intermediaries. Supreme Court judgments, including Shreya Singhal v. Union of India and Anuradha Bhasin v. Union of India, further clarify the scope of digital speech and the balance between liberty and regulation.

Despite these frameworks, doctrinal and institutional limitations continue to persist. These statutory provisions were drafted years before the rise of social media and algorithm-driven targeting, leaving gaps in addressing modern social media-specific problems, including disinformation, micro-targeting, hidden financing, and foreign interference; all of which arise with digital campaigning. The Election Commission of India (ECI), while empowered to regulate campaigns, currently lacks comprehensive tools to monitor algorithmic amplification or ensure transparency in digital political advertising.

3.2 Data Protection and Digital Campaigning: The DPDP Act

The Digital Personal Data Protection Act, 2023 (DPDP Act), introduced a statutory framework for processing personal data in India, aligning closely with international standards such as the EU's GDPR[22]. It applies to processing within India and even outside if services are offered to Indian users. Under this Act, personal data may be processed only for lawful purposes, with either the explicit consent of the data principal or under narrowly defined "legitimate uses".[23] The consent must be free, specific, informed, unconditional, and unambiguous, and subsequently, the data fiduciaries (platforms or service providers) must safeguard security, provide breach notifications, and allow individuals to access, correct, or erase their data. Large-

22 Hemalatha G. and Saikrupaa K., "Comparative Analysis of GDPR and Digital Personal Data Protection Act, 2023", Vol. 11 Issue 12, International Journal of Creative Research Thoughts (IJCRT), (2023)

23 Jindal Policy Research Lab, *Digital Personal Data Protection Act, 2023* (O.P. Jindal Global University, 2023)

scale processors designated as Significant Data Fiduciaries (SDFs) have additional obligations, such as conducting audits and appointing data protection officers.

In practice, the Act establishes a hybrid approach: it codifies the robust notice-and-consent principles while incorporating India-specific flexibility, which includes broad state exemptions for national security, public order, or investigations. Although aligned with GDPR-style protections, notice, breach reporting, and data minimisation, the Act omits certain features such as mandatory privacy-by-design, special categories of sensitive data, and explicit data portability.[24]

The Data Protection Board of India (DPB) is the authority set up under the DPDP Act to enforce data protection rules. Although it can hear complaints and impose fines, it holds limited powers to actively monitor or prevent misuse of personal data. This means that in the current fast-paced world of digital campaigning, where political actors can process and target large amounts of voter data, the Board may struggle to catch violations in real time.

3.3 Democratic Risks in the Digital Sphere

The expansion of social media has introduced significant electoral risks, reshaping how citizens perceive, process, and act on political information. Key challenges include:

- Disinformation and Deepfakes: Algorithmically amplified false content can distort public perception, spread rapidly across platforms, and create echo chambers that polarise voters.
- Hidden Political Financing: Digital micro-targeting enables hidden influence campaigns, allowing parties or interest groups to spend undisclosed funds on highly personalised messaging.
- Algorithmic Targeting: Platforms' opaque recommendation and ad-targeting systems concentrate messaging to selected demographics, which has the ability to influence voter behaviour without transparency or accountability.
- Foreign Interference: Cross-border actors can exploit digital channels to affect electoral outcomes, often bypassing the domestic regulatory framework

---

24 Prakhar Dwivedi and Rohit Kumar Chaturvedi, "*A Critical Analysis of the Issues and Practical Challenges in the Digital Personal Data Protection Act, 2023*" 7 Indian Journal of Law and Legal Research (IJLLR) (2023).

Real-World Illustration: During the 2023 Karnataka Assembly elections, allegations emerged that over 6,000 voter names were deleted in the Aland constituency. Social media amplified the controversy, with Twitter and WhatsApp channels enabling rapid dissemination of claims and counterclaims. This incident demonstrates a dual dynamic: digital platforms that can both reveal administrative vulnerabilities and be leveraged to shape public narratives, therefore, illustrating the intersection of offline electoral challenges with online influence.

Empirical studies indicate a "privacy paradox". While multiple Indian internet users express concern about data privacy, their ability to exercise meaningful control over consent mechanisms remains limited.

A study analysing 143 open-ended responses from users found that their privacy concerns are often rooted in scepticism towards the government, shaping their perceptions of the Digital Personal Data Protection Act (DPDPA) and fuelling demands for policy revisions.[25] The study highlights the need for clearer communication regarding the DPDPA, user-centric consent mechanisms, and policy refinements to enhance data privacy practices in India.

3.4 Comparative Analysis: Lessons from Global Models

Looking at how other countries handle digital campaigning indeed provides useful lessons for India. In the United States, the Federal Election Commission (FEC) requires online disclaimers to ensure transparency, though it largely depends on voluntary compliance by political actors, which means that while the rule formally applies to online ads, enforcement relies significantly on voluntary compliance by political actors rather than proactive federal monitoring. The United Kingdom's Digital Imprint rules go a step further, making it mandatory to clearly identify the sponsors behind political content, which strengthens accountability. Meanwhile, the European Union's Digital Services Act (DSA) places direct obligations on platforms themselves, which ultimately promotes transparency in content, monitoring of algorithmic amplification, and holding platforms accountable for how information spreads. These global models highlight a spectrum of regulatory approaches, from light-touch disclosure to strong platform responsibility, which can inform India's ongoing policy and legislative debate

To consolidate the key features of international approaches and clarify points of divergence, the following comparative table summarises the regulatory

---

25 Sana Athar, Devashish Gosain, *et al.*, "'Nobody Should Control the End User': Exploring Privacy Perspectives of Indian Internet Users in Light of DPDPA," *ResearchGate*, August 2025.

frameworks governing digital political communication across India, the United States, the United Kingdom, and the European Union.

Feature	India	United States	United Kingdom	European Union (DSA/GDPR)
Political Ad Disclosures	No digital imprint mandate; only pre-certification for social media ads (ECI MCC).[26]	FEC requires disclaimers on paid online political ads (2023).	The Elections Act 2022 mandates digital imprints.	DSA & Political Ads Proposal require sponsor labelling.
Algorithm Accountability	No algorithmic audit/transparency obligation.	Voluntary transparency; no federal audit requirement.	Limited platform duties; ongoing policy debate.	VLOPs must undergo risk assessments & independent audits.
Data Protection Law	DPDP Act (2023) with broad state exemptions; political data not specially protected.	No unified federal privacy law; sectoral framework.[27]	UK GDPR treats political opinions as sensitive data.	GDPR provides the strongest protections; political data = special category.
Enforcement Model	Centralised DPB; ECI lacks digital enforcement power.	Multiple regulators; fragmented oversight.[28]	ICO + Electoral Commission (independent regulators).	National DPAs coordinated by the EDPB.
Strengths	Strong constitutional speech protections; active judiciary.	Growing transparency norms & civil oversight.	Established campaign finance accountability.	Comprehensive privacy & platform-duty regime.
Key Gaps	No imprint rules; weak digital oversight & transparency.	Weak unified enforcement;	Slow digital enforcement pace.[29]	High compliance burden & complexity.[30]

Table 1: Comparative Overview of Digital Election Regulation

---

26 Election Commission of India, *Model Code of Conduct & Social Media Guidelines* (2013; revised 2019); Representation of the People Act 1951; Digital Personal Data Protection Act 2023).

27 (Samuel Levine, *The Federal Trade Commission: 2023 Privacy and Data Security Update* (2023) Federal Trade Commission, Bureau of Consumer Protection).

28 Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law* (7th ed., Aspen 2023).

29 Information Commissioner's Office (ICO), *Annual Performance Report 2022–23* (ICO, 2023).

30 *Supra* note 14.

3.5 Synthesis and Implications

Based on the comparative insights, India has made progress with its legal and data protection frameworks, yet doctrinal gaps, institutional limitations, and technological risks remain. A calibrated regulatory response should include:

- Strengthened institutional capacity for oversight (ECI and DPB)
- Clear, enforceable transparency and accountability obligations for platforms
- Public awareness campaigns to bridge the consent-action gap
- Pragmatic adoption of international best practices, adapted to India's political and constitutional context

Interpretation: Digital campaigning is not only a matter of electoral administration; it is a constitutional imperative. Legal and regulatory design must defend democratic legitimacy in an environment increasingly moulded by commercial platforms and algorithmic systems.

4. Arguments and Discussion

4.1 Consent and Data Governance under the DPDP Act

Under the DPDP Act, personal data may be processed only with explicit and informed consent, reflecting a rights-based approach similar to the EU's GDPR, while diverging from the U.S.'s more sectoral, implied-consent model. Individuals are empowered to access, correct, and erase their personal data, while data fiduciaries must implement safeguards such as data minimisation, security measures, breach notifications, appointment of a Data Protection Officer, and grievance redressal mechanisms, thereby reflecting a structured, rights-based approach akin to GDPR standards. The law also creates a category of Significant Data Fiduciaries (SDFs) (based on data volume, sensitivity and risk) subject to extra obligations like impact assessments. In theory, these provisions limit unchecked data use.

In practice, however, the DPDP Act contains broad exceptions that limit its bite in elections. A wide array of "legitimate uses" permits processing without fresh consent; for example, sharing data between government agencies if a citizen has used any prior state service. More generally, the Act exempts processing "in the interests of sovereignty, integrity, public order," law enforcement, and so on. Human rights observers warn these carveouts "enable unchecked data collection

and state surveillance".[31] Crucially, the DPDP Act does not treat political opinions or affiliations as special categories; it imposes no direct limits on microtargeting or profiling of voters. Civil society has noted that past campaigns (e.g. a 2019 app using 78 million voters' data) have skirted scrutiny, and the Act does nothing to prevent similar future abuses. The Supreme Court's recent recognition of a voter's privacy in their political leanings[32] has not yet been translated into statutory safeguards.

In short, while the DPDP Act establishes a modern consent-based framework, its many state-centric exceptions and lack of explicit electoral safeguards leave a large governance gap around political data.

4.2 Enforcement Mechanisms: DPB vs. GDPR and US/UK Models

India's DPDP Act vests all enforcement power in a single Data Protection Board (DPB) appointed by the federal government.[33] Unlike the independent authorities envisaged in earlier drafts, the DPB is a quasi-judicial body with no rulemaking or proactive audit powers. All complaints must be adjudicated at this New Delhi body, with appeals to the Telecom Disputes Settlement Appellate Tribunal. Experts warn that this highly centralised model strains India's scale: one board would oversee millions of data processors and hundreds of millions of users. Capacity is a concern as minor violations by smaller entities may simply fall "below the radar" while only high-profile cases (or those volunteered by the state) get attention.

By contrast, the EU enforces data protection through a network of national Data Protection Authorities (DPAs). Each Member State (and the UK, post-Brexit) has an independent regulator (e.g. the UK's ICO) with investigatory and sanctioning power, coordinated via a GDPR "one-stop shop" mechanism for cross-border cases.

In practice, EU regulators have issued hundreds of fines (over 800 by 2021 but with a strong focus on large tech firms- smaller businesses often escape scrutiny despite being in scope. Similarly, the UK's ICO has shown it can levy multi-million-pound penalties under the GDPR regime.

---

31 Human Rights Watch. *India's General Elections, Technology, and Human Rights Questions and Answers* (Human Rights Watch, April 8, 2024).

32 Sridhar, Sriya. "The Hidden Opportunity to Regulate Targeted Political Advertising in India." *TechPolicy.Press*, July 25, 2024.

33 Abhijith Balakrishnan, "Enforcement Gaps in India's DPDP Act and the Case for Decentralized Data Protection Boards", *Express Computer*, July 4, 2025.

The US, by contrast, has no single data protection authority. Agencies like the FTC and state attorneys general pursue privacy violations as unfair trade practices, for example, the FTC's record $5 billion Facebook settlement for privacy breaches[34] but there is no consumer-privacy regulator equivalent to a DPA.

These comparative models suggest vulnerabilities for India. With only one DPB and limited autonomy, enforcement may skew like the GDPR did – heavy on the biggest violators, light on the rest. Indeed, commentators argue India should consider a federal approach: for instance, creating state-level data protection boards alongside the DPB so that local grievances can be addressed promptly. In any event, India's current enforcement architecture seems under-resourced relative to its promise: the DPB lacks rulemaking power or guaranteed independence, which raises doubts about its ability to hold either large corporations or governments to account.

4.3 Platform Regulation and Algorithmic Amplification

India currently lacks targeted regulation of online political advertising or algorithmic dissemination. There are no election-specific provisions in the DPDP Act or IT Rules that curb microtargeting by parties or require transparency of political ads. In contrast, the UK's recent Elections Act (2022) introduced digital imprint requirements: any paid online campaign advert in the UK must carry an imprint identifying the sponsor[34]. The Electoral Commission's guidance makes it clear that all paid "political material" needs an explicit imprint, improving transparency on who is behind each ad.

In the US, the Federal Election Commission now similarly requires disclaimers on most paid internet political communications. As of March 2023, online ads are "placed for a fee" on websites, apps, or social media must include clear information about who paid for them.[35]

These measures aim to bring online political ads into line with long-standing disclosure laws; without them, voters may not know who is influencing them. The European Union's approach goes further to tackle algorithmic influence. Under the Digital Services Act (DSA), very large platforms must assess risks from their "algorithmic systems" and advertising tools on "civic discourse and electoral

---

34 Electoral Commission (UK), Statutory Guidance on *Digital Imprints under the Elections Act 2022* (2023).

35 Express Computer. "Enforcement Gaps in India's DPDP Act and the Case for Decentralised Data Protection Boards," *Express Computer*, July 4, 2025.

processes".[36] The DSA also obliges platforms to be transparent about their recommender and ad-selection algorithms, specifically to mitigate harms like disinformation.[37]

Effectively, the European Union requires online platforms to actively monitor, report, and mitigate the amplification of harmful content, a mandate that India's regulators currently do not impose. Indian elections have already witnessed largely unchecked algorithmic campaigns; recent investigations reveal that major political parties have deployed AI-generated advertisements to spread divisive content and, in some cases, have violated "silence period" restrictions on digital platforms. In the absence of regulatory mechanisms such as mandatory imprints, disclaimers, or platform-level risk obligations, India continues to rely heavily on self-regulation and the goodwill of intermediaries—a notable divergence from the more robust governance frameworks established in the United Kingdom, the United States, and the European Union.

4.4 Synthesis and Recommendations

A comparative review shows that India's new data law provides formal privacy rights and consent obligations, but also allows broad state exemptions and suffers from weak enforcement. By contrast, Europe's GDPR/DSA and UK laws combine privacy protections with active enforcement and advertising transparency, while the US adds mandatory political advert disclosure. For India's federal and expanding democracy, these international models suggest several reforms.Narrow exemptions and strengthen consent. The DPDP Act's "legitimate use" carve-outs for the state permit citizen data to be repurposed for political profiling without rigorous oversight. Mandating procedural safeguards- such as privacy impact assessments for state-agency data used in elections and treating political opinions or party affiliation as sensitive data could close electoral loopholes.

- **Enhance enforcement capacity and independence:**

The Data Protection Board must be independent, adequately resourced, and empowered to initiate investigations proactively, make rules, and protect whistleblowers. A "cooperative federalism" approach could establish state-level data protection bodies alongside the central DPB, mirroring India's pollution control model, to manage local cases and relieve systemic bottlenecks. Regulators

---

36 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), Art. 34, OJ L 277, 27 October 2022.

37 Iyer, Pooja. "What Does Europe's Digital Services Act Mean for Targeted Political Advertising in the U.S.?" *Tech Policy Press*, November 17, 2022.

must avoid conflicts of interest, as GDPR experience shows enforcement suffers when boards are beholden to the government as a data fiduciary.

- **Mandate political-ad transparency:**

India should require clear disclosures for digital campaign content. This could include digital imprint rules or mandatory disclaimers, similar to the UK and the US. Election law should explicitly cover social media and messaging platforms: paid political advertisements, even in closed WhatsApp groups or SMS, should be treated as "published material," with promoter identities disclosed. Platforms should maintain ad libraries akin to Facebook's Archive, allowing regulators and the public to audit political spending.

- **Regulate algorithms in the public interest:**

Large online platforms could adopt an EU-style risk-assessment framework, analysing how recommender and advertising algorithms affect elections. Where amplification of disinformation or hate is identified, platforms must mitigate systemic risks. Following the DSA, regulations might prohibit using sensitive personal attributes (e.g., religion, caste) in political targeting and require independent audits of algorithmic bias. Such measures would curb "black box" influence operations that distort voter choice.

- **Integrate electoral norms and data policy:**

The Election Commission of India should collaborate with privacy regulators. Election manuals could stipulate that pre-campaign voter data (e.g., census-linked rolls) be anonymised and that cross-platform microtargeting be prohibited. Political parties acting as significant fiduciaries could be required to certify compliance before each election. At a constitutional level, transparency rules must align with free speech; narrowly tailored imprint and disclosure requirements have been upheld internationally as valid regulations on political campaigning, not censorship.

In sum, bridging India's current gaps requires a calibrated mix of privacy safeguards, public transparency, and institutional reform. By narrowing DPDP exemptions, strengthening enforcement, and imposing disclosure duties on political advertisements and platforms, India can better protect elections from opaque, data-driven influence. New rules should be grounded in India's rights framework, using legitimate state interests such as electoral integrity to justify measured data-processing restrictions, thereby aligning with judicial review. In this way, India can draw on global best practices while tailoring them to its multi-party democracy and federal structure.

5. FINDINGS

5.1 Principles versus Practice

The DPDP Act promises strong data protections on paper: consent, notice, and rights for individuals. Yet in practice, broad exemptions for the state and the centralised nature of the Data Protection Board limit its impact. While many see the law as a step forward, enforcement remains patchy, and smaller breaches often go unnoticed.

5.2 Efficacy of Protections

Although the Act requires breach notifications and data minimisation, loopholes allow both government bodies and organisations to bypass safeguards. Crucially, sensitive political data, voter preferences or party affiliations are not specially protected, leaving room for micro-targeted campaigns to operate largely unchecked.

5.3 Public Perception

A "privacy paradox" persists in the online sphere: people care about consent and privacy but remain sceptical of government oversight. This lack of trust suggests that even a well-designed law cannot build confidence without transparency and active enforcement.

5.4 Comparative Gaps

Compared to the EU, UK, and US, India's framework misses key features like portability, privacy-by-design, and compensation mechanisms. Algorithmic accountability and political-ad transparency, common abroad, remain largely absent here.

5.5 Institutional Limitations

The DPB's centralised model stretches its capacity, focusing attention on high-profile cases while systemic, smaller-scale issues may slip through. A cooperative model with state-level boards could improve oversight, as seen in the EU or India's pollution control mechanisms.

5.6 Technological and Electoral Risks

Disinformation, algorithmic amplification, hidden campaign financing, and foreign interference increasingly influence Indian elections. Platforms currently have no clear obligation to audit their algorithms or disclose political ad sponsors, making these risks harder to address.

Interpretation: In short, India has laid the foundation for digital data governance, but enforcement gaps, low public awareness, and opaque technology limit its effectiveness in protecting electoral integrity.

The findings reveal that while India's DPDP regime recognises data rights formally, enforcement gaps and the absence of explicit political-data safeguards weaken election protection in practice. The comparative review demonstrates that workable regulatory pathways already exist in the US, UK and EU models, forming a normative basis for Indian reform. These insights set the stage for the Conclusion, which outlines a phased roadmap to operationalise transparency, accountability, and institutional capacity within India's election law framework.

6. CONCLUSION AND SUGGESTIONS

India stands at a defining moment in its democratic evolution[38]. While the constitutional commitment to free expression, judicial oversight, and an established electoral framework provides a strong normative foundation, the rapid expansion of digital campaigning has outpaced existing regulatory mechanisms[39]. Current laws, particularly the DPDP Act and the RPA, do not adequately address algorithm-driven persuasion, micro-targeting, cross-platform misinformation, or opaque financing.[40] Without statutory imprint rules, algorithmic transparency mandates, and specialised oversight capacity, digital influence risks undermining voter autonomy and electoral fairness.

Comparative frameworks reveal how other democracies are adapting to the digital era. The United Kingdom mandates digital imprints on campaign material, the United States requires disclaimers on paid political ads, while the European Union's Digital Services Act introduces a deeper accountability model involving algorithmic audits and public ad repositories. These models illustrate a global shift from offline campaign regulation to digital-first governance centred on transparency, platform responsibility, and data-rights enforcement. India currently lacks these electoral-specific digital safeguards, but has the institutional capability and constitutional ethos to evolve.[41]

---

38 Vasudev Devadasan, "Conceptualising India's Safe Harbour in the Era of Platform Governance" 19(1) *Indian Journal of Law & Technology* (2024).

39 Nishith Desai Associates, *Social Media & Elections in India: The Regulatory Gap* (Policy Brief, 2023).

40 Saumya Chanda, "Data Privacy and Micro-Targeting in Indian Elections: A Doctrinal Gap Analysis" 18 *Indian Journal of Law & Technology* 75–101 (2022).

41 United Nations Development Programme, *Information Integrity for Electoral Institutions and Processes: Reference Manual* (2024).

Going forward, India's challenge is not only to regulate political advertising online but to create a policy ecosystem that protects voter privacy, ensures transparency in influence operations, and maintains speech freedom while preventing manipulation. A calibrated regulatory approach, neither laissez-faire nor restrictive, can secure electoral integrity in an algorithmic environment. The path forward requires legislative amendments, institutional redesign, and phased implementation supported by technical capacity and continuous oversight.

If aligned with global best practices and adapted to the domestic socio-political scale, India can transform digital campaigning into a space of accountability and democratic renewal rather than opacity and influence distortion. A structured roadmap, enforceable transparency norms, and research-backed platform obligations can ensure that technology strengthens and not weakens electoral legitimacy.

6.1 Recommendations

To operationalise regulatory reform, a phased, enforceable, and future-ready strategy is proposed:

A. Legal & Policy Reform

1. Introduce digital imprint legislation[42] requiring visible sponsor labels on all online political advertisements, including influencer-based and targeted ads.
2. Create a statutory political ad-disclosure framework under the RPA/MCC with mandatory reporting of funding, targeting parameters, duration, and expenditure.
3. Classify political/voter preference data as sensitive, restricting caste-religion-based micro-targeting without explicit consent.[43]
4. Mandate platform-maintained public ad libraries for research access, audit trails, and civic transparency.[44]

---

42 House of Commons Library, *Digital Imprints Under the Elections Act 2022* (UK Parliament, 2023).

43 *Supra* note 15.

44 United Nations Development Programme, *Information Integrity for Electoral Institutions and Processes: Reference Manual for UNDP Practitioners* (Global Policy Centre for Governance, 2024).

B. Institutional Architecture

1. Establish a Digital Election Monitoring Cell (DEMC) under the Election Commission, equipped with technical analysts[45], AI-tracking capabilities, and platform liaison authority.
2. Strengthen the Data Protection Board through independent membership rule-making capacity, and suo motu audit powers
3. In the long term, evaluate the creation of a dedicated Independent Digital Election Authority (IDEA) coordinating ECI, DPB, CERT-IN, and Competition Commission for integrated oversight.
4. Require annual transparency reports from major platforms detailing political ad reach, targeting logic, and algorithmic amplification.

C. Phased Roadmap

Timeline	Key Measures
0–2 Years (Immediate Reform)	Digital imprints; ad-registry; restraint on sensitive attribute micro-targeting; compulsory certification of online campaign material.
2–4 Years (Accountability Phase)	Algorithmic impact assessments during elections; platform transparency reports; State-level DPB branches for decentralised enforcement.
4+ Years (Structural Integration)	Harmonisation of DPDP, IT Act, and Election Law; operationalisation of IDEA; codification of digital electoral transparency principles.

D. Scope for Future Research

- Behavioural impact of targeted political ads on voter choice.
- Legal approach to deepfakes and AI-generated propaganda.
- Regional misinformation patterns in multilingual election environments.
- Development of automated monitoring dashboards for the ECI.

Ultimately, the question is not whether India will regulate digital campaigning, but how and whether such regulation will strengthen the democratic process without eroding the freedom that sustains it.

---

45 Vidhi Centre for Legal Policy, *Comments on the Draft Digital Personal Data Protection Rules* (March 2025).