International Journal for Research Trends in Social Science & Humanities
Volume 3, Issue 5
Sep-Oct 2025, PP 1-11

How political parties use AI and social media to target voters in India — impacts, and regulatory challenges

Dalganjan Singh
village vishma, post-aseh, district kannau,j uttar pradesh India 209729

Abstract- This paper examines how political parties and campaign actors in India deploy artificial intelligence (AI) and social media to target individual voters, evaluates the effects of such targeted information campaigns on voter behaviour and electoral outcomes, and analyses the regulatory and ethical challenges—especially around data privacy and AI governance—that arise in the Indian context. Drawing on published studies, Election Commission of India (ECI) guidance, investigative journalism, and legislative texts, the paper constructs a conceptual framework of political microtargeting in India, documents contemporary tactics (data harvesting, predictive modelling, message personalization, use of closed-messaging platforms and influencer networks, and automated content generation), and assesses impacts (persuasion, mobilization/demobilization, selective information exposure, and polarisation). The paper then examines India's legal landscape, focusing on the Digital Personal Data Protection Act (DPDPA) and ECI rules, and identifies gaps in regulation, enforcement challenges posed by platform practices and cross-border data flows, algorithmic opacity, and limitations of existing election law. The paper concludes with policy recommendations for transparency, stronger data governance for political processes, platform accountability, auditability of AI systems used in political communication, and electoral best practices to protect democratic deliberation.

Keywords - AI, microtargeting, political advertising, social media, misinformation, data privacy, Digital Personal Data Protection Act, Election Commission of India, algorithmic transparency, India elections.

I. Introduction

The 21st-century electoral campaign has shifted from mass rallies and poster-driven persuasion to data-driven microtargeting and digitally-mediated persuasion. In India — the world's largest democracy with diverse sociolinguistic electorates and an increasingly digital public sphere — political actors have rapidly adopted social media platforms, messaging apps, and analytics tools to shape political communication. Recent Indian election cycles have shown intensive use of social platforms (public-facing and private), targeted digital advertising, and campaign analytics that use large datasets to segment voters and deliver tailored content. Simultaneously, advances in generative AI lower the costs of producing realistic audio-visual content, synthetic text, and personalised messaging at scale. These twin trends raise urgent questions: how exactly are political parties using AI and social media to target voters in India, what measurable effects do such campaigns have on electoral behaviour and outcomes, and what regulatory and ethical safeguards are necessary to protect citizen privacy and democratic integrity?

This paper systematically addresses these questions. Section 1 reviews the literature and empirical reports on political microtargeting and AI in India. Section 2 maps the technical and operational practices used by parties and affiliated actors. Section 3 analyses impacts on voter behaviour and electoral outcomes, drawing on empirical studies and case reports. Section 4 assesses India's regulatory framework, including the Digital Personal Data Protection Act (DPDPA), Election Commission guidelines, and platform policies, and identifies critical gaps and enforcement constraints. Section 5 offers policy and technical recommendations for regulators, election authorities, platforms, and civil society. The conclusion summarises the main findings and suggests priorities for future research and policy action.

II. Literature and Evidence Review

Scholarly literature on political microtargeting — largely developed in the US and Europe — indicates that advanced analytics and targeted messaging can increase persuasion and turnout when campaigns use precise audience segmentation and persuasive creatives. Studies of Indian elections (especially 2019 and 2024 cycles) document extensive use of digital platforms both for broadcasting and targeted outreach; independent researchers and watchdog groups reported AI-generated content and targeted ads that sometimes violated platform policies or evaded detection. Investigative reporting has uncovered instances where political ads crossing lines (including hate speech) were approved and distributed on major platforms, highlighting platform-review failures and the potential for harm when automated systems are abused. The Election Commission of India (ECI) publicly recognised the challenges posed by manipulated content and the misuse of social media for electoral campaigning and issued guidance to promote transparency and ethical use. Scholarly and policy reviews emphasise the dual nature of AI: it can improve campaign efficiency and voter outreach while also amplifying misinformation and enabling covert behavioural influence if used without safeguards.
(Key load-bearing sources cited here: ECI guidance; investigative reporting on platform failures; academic analyses of online political advertising in India.)

How political parties use AI and social media to target individual voters in India
This section synthesises the main tactics and technologies in use, organised across data inputs, analytics and modelling, message production and delivery channels, and orchestration.
Data inputs: what data campaigns use
Political microtargeting depends on rich datasets. The major inputs include:

- Publicly available voter rolls and demographic data: Parties combine official electoral rolls (name, age, polling station) with census and local administrative information to build baseline voter lists.
- Social media and platform metadata: Public profiles, likes, shares, follower networks, engagement metrics, and responses to past posts on platforms such as Facebook, Instagram, X (Twitter), and YouTube.
- Proprietary consumer data and commercial data brokers: Where available, consumer purchase data, telecom metadata (call and SMS patterns), and other commercial attributes can be combined to infer socio-economic status and behaviours.

- Direct collection via outreach: Door-to-door canvassing, party membership drives, event registrations, and service-camp registrations that collect phone numbers, names, and other details. Allegations and reports indicate political volunteers sometimes obtain sensitive data under the guise of welfare assistance.
- WhatsApp and private messaging ecosystems: Because WhatsApp is heavily used in India, social networks built on phone contacts, broadcast lists, and community admins are critical nodes for message diffusion. Private groups are rich sources of qualitative sentiment and allow hyper-local targeting.
- Combining these sources creates detailed individual or micro-segment profiles useful for tailored messaging.

Analytics and AI models used

Political actors increasingly deploy a pipeline of analytics tools and AI models:

- Descriptive and predictive analytics: Segmentation algorithms (clustering), propensity-to-vote and propensity-to-convert models, and lookalike modelling (identifying uncontacted voters similar to known supporters).
- Natural language processing (NLP) and sentiment analysis: To monitor conversations, detect trending themes, and classify voters' sentiment on issues. This informs topical targeting (which messages will resonate in which micro-regions and demographics).
- Recommendation systems and personalization engines: Similar to e-commerce personalization, these systems decide which creative to show to which user, and when, aiming to maximise engagement or persuasion.
- A/B testing and causal inference methods: Campaign teams run variant testing to discover which messages, tones, and images work best for particular segments, sometimes applying simple causal methods to infer what changes behaviour.
- Generative AI tools: For content creation — generating slogans, translations into local dialects, text messages, image variants, synthetic video/audio snippets, and chatbots to interact with supporters. The rising availability of generative models reduces production costs and speeds up micro-personalisation.

These tools may be used in-house (by party data teams), by affiliated consultancies/advertising agencies, or via third-party vendors.

Message production and thematic tailoring

Messages are tailored across multiple axes:

- Issue framing: Economic welfare, caste or identity appeals, nationalism, local grievances, or service delivery messaging — chosen to match segment priorities.
- Affective tone: Emotional content (fear, pride, anger, hope) is calibrated using prior testing.
- Linguistic and cultural localization: Use of local languages, idioms, and culturally resonant symbols.
- Narrative micro-targeting: Deploying narratives designed to resonate with subgroups (e.g., farmers in specific districts, urban young professionals, religious communities).
- Generative AI aids rapid variant-generation (multilingual captions, image templates), enabling thousands of near-unique creatives.

Delivery channels and diffusion strategies

Delivery uses a mix of public platforms and private networks:

- Paid social advertising (Facebook/Instagram, YouTube, X): Targeted ads using platform targeting tools (demographics, interests, lookalikes). Studies show heavy use of Facebook ad library in Indian campaigns.
- Organic social media posts and influencer amplification: Candidate posts amplified by networks of influencers, regional opinion leaders, or coordinated pages.
- WhatsApp broadcasts and community admins: Hyperlocal diffusion through WhatsApp groups and broadcast lists; messages here often evade public moderation.
- SMS and robocalls: Targeted text messages and pre-recorded calls to phone numbers tailored by segment.
- Call centres and chatbots: For persuasion, GOTV (get-out-the-vote) reminders, and addressing voter queries.

A key operational tactic is message cascades: seeding content publicly, having influencer nodes amplify it, and then pushing it into private groups where moderation is weaker and trust among recipients increases perceived credibility.

Covert tactics, automation and bots

Campaigns may exploit automation and semi-automated methods:

- Botnets / automated accounts: For artificial amplification, trend manipulation, or harassment of opponents.
- Coordinated inauthentic behaviour: Networks of accounts that mimic grassroots activity but are centrally coordinated.
- Use of anonymised or faux grassroots pages: To present targeted narratives as independent citizen movements.

Investigations have documented approvals of problematic political ads and the presence of manipulated content on platforms, underscoring the difficulty of detecting AI-manufactured or scaled content.

III. Impacts on voter behaviour and electoral outcomes

Determining precise causal effects of targeted campaigns on electoral outcomes is methodologically challenging because of confounding variables, simultaneous offline campaigning, and limited access to platform-level exposure data. Nonetheless, evidence and theory indicate several plausible impacts:

Persuasion (converting undecided voters)

Targeted persuasive messages can change opinions when they are well-calibrated to recipients' latent preferences. Microtargeting allows campaigns to deliver pro-attitudinal framing or corrective narratives to narrowly defined groups, increasing the probability of persuasion relative to broadcast ads. A/B testing and lookalike strategies increase the efficiency of persuasion budgets.

Empirical evidence from political advertising research suggests measurable but often modest persuasion effects per exposed voter; aggregated across millions of micro-targeted exposures, however, small per-person effects can become electorally significant. Studies of online advertising in India documented extensive investment and strategic deployment, especially in competitive constituencies.

Mobilisation and demobilisation (get-out-the-vote and suppression)

Microtargeted messages are powerful for voter mobilisation — personalised turnout reminders timed before polling, transportation offers, or appeals framed on civic duty. Conversely, targeted misinformation can demobilise or confuse specific groups (for instance, falsely informing a community about polling logistics). Campaigns that identify likely non-voters and either mobilise or suppress them can influence turnout composition and therefore results.

Information environment, selective exposure and echo chambers

Personalisation tailors information feeds, which can produce filter bubbles — users receive more homogeneous information aligned with their predispositions. In a linguistically and socially segmented polity, microtargeting can produce different electorates that inhabit distinct informational universes. This fragmentation reduces shared factual baselines and can increase polarisation.

Emotional and identity-based effects

Micro-targeted identity appeals (caste, religion, language) can activate group loyalties and outgroup fears, increasing polarisation and potentially inciting conflict. Reports from recent elections showed instances where divisive targeted messages circulated and contributed to heightened communal rhetoric online. Investigations found AI-manipulated political adverts that included inflammatory content which briefly circulated on major platforms.

Misinformation amplification and trust erosion

AI enables rapid generation of misleading or fabricated content. When such content is targeted to susceptible subgroups through private channels, the combination is potent: believable synthetic content + trusted social context = high persuasive potential. Over time, repeated exposure to tailored misinformation erodes public trust in institutions and media.

Empirical limitations and measurement challenges

Two major empirical constraints complicate causal attribution:

- Data access: Researchers often lack platform-level exposure data; platform transparency tools are limited and sometimes incomplete.
- Confounding offline activities: Parties simultaneously run door-to-door and event-based campaigns; separating online causal effects requires carefully designed field experiments or access to granular exposure logs.

Despite these limits, case studies, ad-library audits, and post-election surveys collectively indicate that targeted digital campaigns have non-trivial impacts, especially in tightly contested seats and when used for targeted mobilization or narrative seeding.

IV. Regulatory and ethical challenges in India

This section examines India’s legal and regulatory regime as it pertains to political targeting, with emphasis on data privacy, AI ethics, election law, and platform accountability.

The Digital Personal Data Protection Act (DPDPA/DPDPA 2023): coverage and limitations

India enacted a statutory framework for digital personal data protection recently. The Digital Personal Data Protection Act (DPDPA) establishes duties of data fiduciaries, data subject rights, and certain restrictions on processing. Key relevant points:

- Scope: The law applies to processing of digital personal data in India and includes provisions on lawful processing, consent, data minimisation, and cross-border transfers (subject to conditions).
- Special categories and children: The Act restricts behavioural monitoring and targeted advertising directed at children and requires verifiable consent for processing children's data.
- Significant Data Fiduciaries (SDFs): Entities that process large amounts of data or sensitive categories may have enhanced obligations (audit, DPIA, etc.).
- Enforcement and penalties: The law creates mechanisms for penalties and redress, but operational enforcement regimes, rule-making, and implementation details will determine effectiveness.

Limitations for political targeting:

- The Act regulates data fiduciaries (commercial and non-commercial) but does not explicitly create a bespoke regulatory regime governing political persuasion or political advertising. Political actors collecting and processing elector-related data could be covered, but enforcement against parties or volunteer networks — particularly informal ones — is harder. The Act’s impact hinges on how regulators classify political campaigning and whether political parties are treated as data fiduciaries with compliance obligations. Practical enforcement is complicated by the political nature of actors and the prevalence of private-messaging diffusion that is hard to monitor.

Election law, ECI guidance and practical limits

The Election Commission of India (ECI) has long-standing Model Code of Conduct provisions and has issued guidance on responsible social media use during elections. In 2024, ECI released advisory material addressing manipulated content and social media campaigns, urging parties to adhere to MCC and transparency norms. However, the ECI’s jurisdictional reach is constrained when it comes to real-time moderation of private-platform activity and cross-border platform practices.

Platform self-regulation and auditability

Major platforms have ad libraries and transparency tools, but independent audits and third-party access remain limited. Investigative reports showed examples of platform failures to block harmful AI-manipulated political ads during critical periods. Platform ad-targeting tools sometimes allow micro-segmentation that can be abused; disclosure of who funded political ads and to whom they were targeted is often partial. Platform policies vary, and enforcement is reactive and opaque.

Cross-border flows, vendor ecosystems, and political actors

Political campaigns increasingly depend on vendors, consultancies, and cross-border toolkits. Cross-border data flows complicate enforcement of national data protection rules and create jurisdictional gaps. Foreign-based platforms processing Indian data may resist local enforcement or shift data processing offshore. DPDPA includes provisions for cross-border transfers, but governance mechanisms and international cooperation are required for practical oversight.

AI ethics: opacity, explainability and algorithmic harms

AI systems — recommendation algorithms, generative models, and predictive classifiers — often lack explainability. When used for political targeting, opaque models make it difficult to determine why certain voters received specific content or to audit whether algorithms systematically discriminate or manipulate. Ethical concerns include lack of informed consent, behavioural targeting without transparent opt-outs, and adverse impacts on disadvantaged groups. Public-interest mandates for algorithmic impact assessments (AIA) or independent algorithmic audits could help, but legal basis and enforcement mechanisms are nascent.

Enforcement practicalities and political economy constraints

Even where rules exist, political will to rigorously enforce restrictions against powerful parties or influential campaign vendors can be limited. Election-time urgency, rapid content diffusion across private channels, and resource constraints in regulators complicate proactive monitoring. The ECI can issue guidelines and warnings, but policing thousands of private-group messages or detecting AI-generated synthetic content in real-time is technologically and logistically hard.

Policy recommendations and institutional responses

Given the observed practices and regulatory gaps, this section offers practical, implementable recommendations across several actors: lawmakers/regulators, election authorities, platforms, civil society and researchers, and political actors themselves.

For lawmakers and regulators (legislative & administrative)

- Clarify political campaigning within data law: Explicitly define treatments for political actors within the DPDPA (or accompanying rules) — e.g., require political parties and paid campaign vendors to register as data fiduciaries and comply with certain transparency obligations when processing voter data.
- Mandate targeted-ad disclosure and archive: Require platforms to provide a public, searchable ad library for political ads including targeting criteria (demographics, geography, interests), sponsor identity, spend, and impressions. Granular exposure records should be accessible to authorised researchers under privacy-preserving arrangements.
- Algorithmic impact assessments (AIAs): Require SDFs and platforms to conduct and publish AIAs for algorithmic systems used in political advertising and content ranking, with third-party audit options.
- Limits on sensitive profiling: Prohibit profiling based on sensitive attributes (religion, caste, health, sexual orientation) for political persuasion; strengthen penalties for violations.
- Cross-border enforcement cooperation: Negotiate MOUs with major platforms and foreign authorities to enable rapid content takedowns and forensic access where necessary.

For the Election Commission of India

- Enhanced transparency during elections: Require campaigns to disclose data-collection drives and data sources when using targeted digital communication; publish guidance on acceptable use and sanctions for covert data-harvesting for electoral purposes.
- Digital rapid-response unit: Invest in a technical cell that coordinates with platforms to flag and remove inflammatory or manipulated political content during election periods.
- Public awareness campaigns: Educate voters about targeted misinformation, how to verify sources, and strategies to check suspicious messages (especially on WhatsApp and other private channels). Evidence shows that media-literacy interventions can reduce susceptibility to misinformation.
- Third-party research access: Create a regulated access mechanism for independent researchers to study platform data (ad libraries, exposure metadata) under strong privacy safeguards.

For platforms

- Granular ad-targeting transparency: Provide not only who paid for an ad but also aggregated targeting parameters (age ranges, locations, interests) and impression distributions.
- Higher scrutiny for political creatives: Strengthen human review for political ads flagged for possible manipulation; improve detection of AI-generated media and label synthetic content.
- Rate limits and provenance tags: Place provenance metadata on content to indicate origin (sponsored vs organic) and tag AI-generated content where detectable.
- Support for independent audits: Allow vetted researchers and regulators to audit ad-delivery algorithms and targeting logs in a privacy-protective manner.

For civil society and researchers

- Independent monitoring consortia: Support groups that monitor ad libraries, platform moderation practices, and the diffusion of targeted content, publishing timely audits during election cycles.
- Media literacy and community inoculation: Run local-language interventions and inoculation campaigns in susceptible regions to reduce the impact of tailored misinformation.
- Ethical research partnerships: Encourage collaborations with platforms that provide privacy-preserving data slices to enable causal research on microtargeting effects.

For political actors and campaign practitioners

- Ethical codes for campaigning: Parties should adopt internal ethical standards banning deceptive AI-generated content, respecting privacy rights, and ensuring consent for data collection for electoral purposes.

- Transparent procurement: Disclose use of third-party data vendors and analytics providers; allow audits by election authorities.
- Avoidance of sensitive profiling: Refrain from designing campaigns that target voters based on protected characteristics, and favour issue-based persuasion.

Normative and technical considerations

Balancing free speech and electoral integrity

Regulatory responses must balance freedom of political speech (a cornerstone of democratic contestation) with the need to prevent covert and manipulative tactics that undermine fair competition and informed consent. Simple prohibition of political speech is neither desirable nor feasible; instead, rules should focus on transparency, accountability, consent, and restrictions on invasive profiling.

Technical feasibility of transparency and audits

Implementing ad-targeting transparency and AI audits requires platforms to devise privacy-preserving logging and researcher-access mechanisms. Differential privacy, secure multi-party computation, and vetted data enclaves can enable auditability without exposing personal data. Regulators and researchers should invest in capacity building for technical audits.

Designing corrective interventions for private messaging ecosystems

WhatsApp and similar apps are end-to-end encrypted, complicating content moderation. Public-interest strategies should emphasise upstream interventions: limiting bulk-messaging capabilities, labelling forwarded content, reducing virality by limiting forwarding chains (measures already partially attempted on some platforms), and community education. Where illegal content or violence-inciting messages exist, platforms should cooperate with lawful requests from authorised authorities, subject to due process and rights safeguards.

Research agenda and measurement priorities

To evaluate the true impacts of AI-driven targeted campaigns in India, researchers and policymakers should prioritise:

- Causal field experiments: Collaborations with parties or non-partisan civic actors to run randomized interventions (ethical constraints apply) that test targeted messaging effects on turnout and preferences.
- Exposure measurement: Secure access mechanisms to platform exposure data (aggregated and privacy-protected) for independent evaluation.
- Longitudinal studies: Track trust, polarisation, and information ecosystems over time across different language and regional settings.
- Ad-library audits: Systematic collection and analysis of political ads, sponsors, creatives, and declared targeting to detect patterns and irregularities.
- Synthetic content detection research: Invest in detection methods tuned to Indian languages and multimodal content.

V. Conclusion

AI and social media are reshaping political campaigning in India. Parties and campaign actors use data-rich profiles, predictive models, and increasingly accessible generative AI tools to microtarget voters with tailored messages across public and private digital channels. These practices can improve outreach efficiency and mobilise supporters effectively, but they also raise serious democratic risks: targeted misinformation, erosion of common factual ground, emotional manipulation along identity lines, and privacy violations.

India has begun to construct legal and regulatory responses. The Digital Personal Data Protection Act provides a general data governance framework; the Election Commission has produced guidance for social media conduct; platforms maintain ad libraries and policies. However, meaningful oversight of microtargeting requires sharper statutory clarity on political actors' obligations, more transparent platform-level disclosures (targeting criteria, ad reach), algorithmic auditing, capacity-building at election authorities, and cooperative arrangements for cross-border enforcement. Civil society and research communities have vital roles in monitoring and public education.

The core policy thrust should be proportional: preserve robust political speech while demanding transparency, consent, and safeguards against manipulative profiling and covert AI-enabled disinformation. Adequate technical mechanisms (privacy-preserving audits, provenance labels, improved synthetic-content detection) combined with legal mandates for disclosure and targeted restrictions (e.g., banning profiling on sensitive attributes) can help sustain a healthier digital public sphere in which voters can exercise informed choice.

Objectives of this paper

- To characterise how political actors in India deploy AI and social media tools for voter targeting.
- To synthesise empirical evidence on the impacts of targeted information campaigns on voter behaviour and electoral outcomes.
- To analyse the regulatory environment—data protection law, election rules, and platform governance—relevant to political microtargeting in India.
- To identify major ethical and enforcement challenges.
- To propose policy, technical, and institutional recommendations to safeguard democratic processes while respecting free political speech.

References

1. Election Commission of India. Responsible and ethical use of social media. Advisory documents on social media and elections (2024).
2. PRS Legislative Research. The Digital Personal Data Protection Bill, 2023 — bill summary and analysis.

3. The Guardian. Revealed: Meta approved political ads in India that incited violence (investigative report, 2024).
4. Al Jazeera Institute. Elections and Misinformation – India Case Study (analysis of misinformation, 2024).

5. WAPOR / ad-audit research. Online Political Advertising: Evidence from India (study of Facebook/Instagram ad libraries, 2019 & 2024 focuses).
6. AzB Partners / legal commentary. Digital Personal Data Protection Act, 2023 – Key Highlights (practical notes on legal implications).
7. Time Magazine. How Modi's Supporters Used Social Media to Spread Disinformation During the Elections (reporting & analysis, 2024).
8. Institute for Freedom (Friedrich Naumann Foundation). AI and its influence on India’s 2024 elections (policy paper, 2024).
9. Academic articles and reviews on AI in political campaigns and regulation (selected):
10. ○ Dash, A. (2024). Political Promotion Over Social Media and Voters' Voting Behaviour (journal study).
11. ○ Arndt et al. (2024). Online Political Advertising Research: Evidence from India (ad-library analysis).
12. Appendix: Practical checklist for regulators and practitioners
13. Require public disclosure of political ad sponsors and aggregate targeting parameters.
14. Mandate provenance labels for synthetic content and invest in detection research.
15. Strengthen DPDPA implementation with clear rules on political data processing and SDF obligations.
16. ECI to set up a technical rapid-response unit and researcher-access protocol.
17. Civil society-run ad-library audits and local-language media literacy campaigns should be funded and scaled.