INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DATA PRIVACY AND ELECTIONS IN INDIA: MICROTARGETING AND THE INVISIBLE VOTER

AUTHORED BY - MR. HEMANT KULKARNI[1]

Abstract

The convergence of big data analytics, behavioural psychology, and electoral politics has produced a phenomenon that fundamentally threatens the integrity of democratic participation in India. Microtargeting, the practice of deploying algorithmically curated political messaging to precisely identified voter segments based on granular personal data, has transformed Indian elections from exercises in public deliberation into orchestrated campaigns of personalized persuasion. Yet the legal framework governing this practice remains conspicuously underdeveloped. This paper examines the architecture of political microtargeting in India, the data ecosystems that sustain it, and the constitutional and statutory vacuum within which it currently operates. Drawing on the Supreme Court's landmark recognition of informational privacy as a fundamental right under Article 21 in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the paper argues that the unchecked harvesting and deployment of voter data for electoral manipulation constitutes not only a statutory violation but a constitutional affront. The paper critically engages with the Digital Personal Data Protection Act, 2023, the Representation of the People Act, 1951, and the Election Commission of India's regulatory instruments, identifying critical lacunae that allow political actors to operate as invisible architects of manufactured consent. It concludes by proposing a framework of electoral data rights that centers voter autonomy, mandates algorithmic transparency, and reconstitutes the relationship between political technology and democratic legitimacy.

Keywords: Microtargeting, Electoral Privacy, DPDPA 2023, Voter Profiling, Informational Autonomy, Puttaswamy, Election Commission of India, Political Data Brokers, Cambridge Analytica, Democratic Integrity

[1] Third Year Student, School of Law, CHRIST University, Bangalore.

ISSN: 2582-6433

I. INTRODUCTION

There is something quietly alarming about the way contemporary Indian elections are fought. The rallies are still grand, the speeches still impassioned, and the crowds still enormous, but underneath the visible spectacle of democratic participation runs a parallel, largely invisible war for the voter's attention, anxieties, and identity. This war is waged not with posters or pamphlets but with petabytes of personal data, psychographic algorithms, and precision-targeted digital advertisements designed to reach specific voters with specific messages crafted to exploit specific vulnerabilities. The voter, in this paradigm, is not an autonomous citizen exercising informed judgment. She is a data point, profiled, predicted, and persuaded.

This paper concerns itself with microtargeting: the practice of using personal data, often collected without meaningful consent, to identify and separately target sub-segments of the electorate with customized political messaging. While microtargeting originated in the United States, most notoriously in the Barack Obama campaigns of 2008 and 2012, before reaching its dark nadir in the Cambridge Analytica scandal of 2018[2], it has migrated forcefully into the Indian political landscape. In a country with over 900 million registered voters, twelve major social media platforms operating at scale, and a Jio-driven data revolution[3] that has brought cheap internet to previously unreached demographics, the conditions for electoral microtargeting are arguably more potent than anywhere else in the world.

The legal system that must grapple with this reality is caught in a state of productive confusion. On one hand, the Supreme Court of India, in its nine-judge bench decision in *Justice K.S. Puttaswamy (Retd.) v. Union of India,*[4] has unambiguously declared privacy a fundamental right, including its informational dimension. On the other, the legislative and regulatory apparatus, particularly the newly enacted Digital Personal Data Protection Act, 2023[5], carves out exemptions for state actors and leaves the political domain in an uncomfortable grey zone. The Election Commission of India has issued guidelines on paid political advertisements online,[6] but these address transparency in ad spending rather than the underlying data infrastructure that makes microtargeting possible.

[2]Carole Cadwalladr & Emma Graham-Harrison, Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach, The Guardian (Mar. 17, 2018).
[3]Arjun Kharpal, India's Jio Had 160 Million Subscribers in First Year, CNBC (Sep. 5, 2017).
[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 [hereinafter Puttaswamy].
[5]Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament (India) [hereinafter DPDPA].
[6]Election Commission of India, Compendium of Instructions on Social Media (2019) [hereinafter ECI Social Media Guidelines].

ISSN: 2582-6433

This paper proceeds in several stages. Section II maps the technological and organizational ecosystem of political microtargeting in India. Section III analyses the constitutional foundations of electoral data privacy, anchored in Puttaswamy and the emergent doctrine of informational autonomy. Section IV subjects the Digital Personal Data Protection Act, 2023 to critical scrutiny, with particular attention to its exemptions and its treatment, or non-treatment, of political data processing. Section V examines the Representation of the People Act, 1951, and the Election Commission's regulatory framework, identifying structural limitations in their approach to data-driven electioneering. Section VI surveys comparative models from the European Union and Canada. Section VII proposes a normative and institutional framework for protecting the invisible voter. Section VIII concludes.

II. THE MICROTARGETING ECOSYSTEM IN INDIAN ELECTIONS

A. From Mass Communication to Personalized Persuasion

Electoral communication in India has historically operated on a broadcast model. Political parties communicated through rallies, newspapers, radio, and eventually television, media that spoke to large, undifferentiated audiences. The message was necessarily general, calibrated to the widest possible appeal within an ideological framework. The emergence of social media platforms, and particularly the smartphone revolution catalyzed by Reliance Jio's entry in 2016, fundamentally disrupted this model. By 2019, India had approximately 340 million WhatsApp users, over 300 million Facebook users, and a rapidly expanding YouTube audience. More importantly, these platforms offered political actors something broadcast media never could: the ability to identify individual users, understand their preferences, and deliver tailored messages at industrial scale.

Microtargeting exploits the granular data profiles that social media platforms construct through continuous user surveillance. Every search, every like, every share, every purchase, and every geographic movement is logged and aggregated into a behavioral profile that predicts with remarkable accuracy an individual's political leanings, emotional vulnerabilities, and susceptibility to particular kinds of messaging. Political campaigns purchase access to these profiles, directly through platform advertising tools or indirectly through data brokers, and use them to segment the electorate into microsegments that might number in the hundreds of thousands in a large constituency.

B. The Indian Data Infrastructure

The microtargeting infrastructure in India rests on several interlocking data sources.

ISSN: 2582-6433

First, and most foundationally, are the voter rolls maintained by the Election Commission of India. These rolls contain the names, ages, addresses, and photographs of over 950 million voters across the country. While the rolls are nominally public documents — available for inspection to any citizen and downloadable in digital form[7], their aggregation and integration with other datasets creates a surveillance potential that was never contemplated when they were first compiled in the paper era.

Second, political parties in India have invested substantially in their own proprietary voter databases. The Bharatiya Janata Party's NaMo App, launched ahead of the 2014 general election, collected detailed information about its users including their locations, phone contacts, and browsing habits. By 2019, the app reportedly had over fifty million users, each of whom had consented, in the thin, take-it-or-leave-it sense that characterizes digital consent, to broad data sharing with the party's analytics machinery. The Indian National Congress operated its own data intelligence unit, which reportedly collaborated with international political technology firms.

C. Cambridge Analytica and the Indian Dimension

The global reckoning with political microtargeting arrived with the Cambridge Analytica scandal of 2018. The firm, which had worked on the Brexit Leave campaign and the Trump 2016 presidential campaign, was revealed to have harvested the Facebook data of approximately 87 million users without their meaningful consent, using it to construct psychographic profiles for targeted political advertising.[8] What received less international attention was the firm's substantial operations in India. Cambridge Analytica and its parent company SCL Group had reportedly worked with multiple Indian political parties, conducting constituency-level voter profiling and targeting operations across several state elections.[9] Internal SCL documents reportedly referenced work in states including Bihar, Uttar Pradesh, and Andhra Pradesh.

The Indian response to these revelations was notable for its inadequacy. A notice was issued to Facebook by the Ministry of Electronics and Information Technology, but no independent investigation was conducted into the Indian electoral applications of the harvested data. No political party was required to disclose its relationship with Cambridge Analytica or similar firms. The Information Technology Act, 2000, which was the primary data protection

[7]Registration of Electors Rules, 1960, Rule 26 (providing that electoral rolls shall be available for public inspection).
[9]Nikhil Pahwa, Cambridge Analytica and India: What We Know So Far, Medianama (Apr. 3, 2018).

ISSN: 2582-6433

legislation at the time, provided no meaningful mechanism for regulating political data processing. The episode illustrated with uncomfortable clarity the gap between the sophistication of the data economy exploiting Indian voters and the legal instruments available to protect them.

D. WhatsApp and the Dark Social Problem

A distinctive feature of the Indian microtargeting landscape is the role of WhatsApp as a political communication platform. Unlike Facebook or YouTube, where advertising is formally regulated and at least nominally transparent, WhatsApp operates through encrypted private messaging. Political content, including targeted misinformation, spreads through networks of WhatsApp groups that are invisible to regulators, researchers, and the platforms themselves. The Oxford Internet Institute's Computational Propaganda Project has documented the systematic use of coordinated WhatsApp networks in Indian state and national elections, with the BJP's IT Cell reportedly managing over 3.2 million WhatsApp groups during the 2019 election.[10][11]

The "dark social" problem, political communication through private, unmonitored channels, poses a particular challenge for any regulatory response to microtargeting. Traditional advertising regulation assumes that political communications are broadcast or at least semi-public; it has no framework for the targeted deployment of politically inflected content through encrypted personal messaging. This gap is not merely technical; it reflects a fundamental mismatch between the architecture of contemporary digital communication and the assumptions embedded in electoral law.

III. CONSTITUTIONAL FOUNDATIONS OF ELECTORAL DATA PRIVACY

A. Privacy as Fundamental Right: The Puttaswamy Framework

The constitutional foundation for data privacy in India was firmly established by the Supreme Court's nine-judge bench in *Justice K.S. Puttaswamy (Retd.) v. Union of India.*[12] The court held unanimously that the right to privacy is a fundamental right protected under Article 21 of the Constitution, overruling the earlier decisions in *M.P. Sharma v. Satish Chandra* and

[10]Samantha Bradshaw & Philip N. Howard, The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, Oxford Internet Institute Working Paper (2019).
[11]OII Report, supra note 6, at 14-17 (documenting coordinated WhatsApp networks and estimated group count).

ISSN: 2582-6433

Kharak Singh v. State of Uttar Pradesh[13] to the extent they held otherwise. The significance of this holding for electoral data privacy cannot be overstated: it means that the state's capacity to collect, process, and share personal information — including voter data — is constitutionally constrained.

Justice D.Y. Chandrachud's lead opinion in *Puttaswamy* articulated what has become the foundational taxonomy of privacy interests in Indian constitutional law. Among these, informational privacy — the right of individuals to control information about themselves — was identified as a core component of the right to privacy.[14] The opinion expressly recognised that an individual's autonomy over personal data is constitutionally protected, and that the sanctity of private communications must be preserved against both state and private intrusion.

For electoral microtargeting, the most consequential aspect of *Puttaswamy* is the court's analysis of data as a bearer of personality and autonomy. The aggregation of individually innocuous data points into a comprehensive profile that predicts political behaviour represents, in constitutional terms, an appropriation of the voter's epistemic self — her political identity, beliefs, and vulnerabilities — without her genuine consent. This is not merely a technical privacy violation; it is an assault on the conditions of democratic autonomy that Article 21, read in its fullest sense, is designed to protect.

B. The Right to Vote and Electoral Integrity

The Supreme Court has recognised the right to vote as a constitutional right, though one created by statute rather than directly guaranteed by the Constitution. In *People's Union for Civil Liberties v. Union of India,*[15] the court held that the right to vote includes the right to know about the candidates, the principle of voters' right to information. This jurisprudential strand, while developed in the context of criminal antecedents' disclosure, has implications for the informational environment within which voting decisions are made.

If voters have a constitutional right to know, it is at least arguable that they have a corresponding right not to be manipulated by informational environments engineered to exploit their psychological vulnerabilities. Microtargeting, at its most sophisticated, does not merely inform voters of a candidate's positions; it identifies the emotional triggers most likely to

[13]M.P. Sharma v. Satish Chandra, AIR 1954 SC 300; Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295 (both overruled to the extent they denied privacy as a fundamental right).
[14]Puttaswamy, supra note 1, ¶¶ 178-181 (per Chandrachud, J.) (holding that the right to privacy encompasses informational autonomy as a core dimension of Article 21).
[15]People's Union for Civil Liberties v. Union of India, (2003) 4 SCC 399, ¶ 78 [hereinafter PUCL] (recognising voters' right to know material information about candidates).

ISSN: 2582-6433

produce a desired voting behavior in a specific individual and deploys messaging calculated to activate those triggers. This is manipulation masquerading as communication, and its systematic deployment undermines the deliberative conditions that give electoral democracy its legitimacy.[16]

Article 19(1)(a) provides an additional constitutional dimension.[17] The freedom of speech and expression includes the right to receive information and to form opinions in conditions of epistemic integrity. When the informational environment of an election is systematically distorted through microtargeted messaging, where different voters receive different, often contradictory, political communications, the public sphere that Article 19(1)(a) is designed to protect ceases to function. Voters cannot deliberate together if they inhabit algorithmically curated informational bubbles that share no common content.

IV. THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: PROMISES AND OMISSIONS

A. The Architecture of the Act

The Digital Personal Data Protection Act, 2023, enacted after a six-year legislative journey that produced multiple draft bills and a landmark Supreme Court intervention, represents India's most comprehensive attempt to regulate the collection and processing of personal data. The Act establishes a framework of data principal rights and data fiduciary obligations, creates the Data Protection Board of India as an adjudicatory body, and prescribes consent as the primary basis for lawful data processing. These are meaningful legislative achievements that bring India into a broadly comparable position with international data protection regimes.[18]

However, the Act is characterized by significant exemptions and limitations that create a substantial electoral privacy gap. The most consequential of these is found in Section 17, which exempts state instrumentalities from significant portions of the Act in the interests of sovereignty, public order, and national security.[19]

[16]PUCL, supra note 13, ¶ 65 (discussing the constitutional basis of the right to vote as derived from statute but protected by constitutional values of free and fair elections).
[17]Constitution of India art. 19(1)(a) (guaranteeing the freedom of speech and expression, which the Supreme Court has consistently held encompasses the right to receive information).
[18]B.N. Srikrishna Committee, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) (Personal Data Protection Bill 2018 draft and report).
[19]DPDPA, supra note 2, § 17 (exempting state instrumentalities from portions of the Act in the interests of sovereignty, public order, and national security).

ISSN: 2582-6433

B. The Political Party Problem

The Act's most glaring omission in the electoral context is its failure to address political parties as a distinct category of data processor. Political parties occupy an unusual legal position in India: they are neither private companies subject to commercial data protection obligations nor state organs subject to constitutional data rights constraints. The Act treats them as private data fiduciaries for the purpose of data processing obligations,[20] but provides them with no special responsibilities commensurate with the sensitivity of the electoral data they process and the particular public interest at stake in electoral integrity.

This is not merely an academic concern. Political parties in India routinely collect, aggregate, and deploy voter data at a scale and sophistication that rivals or exceeds the data processing activities of major commercial enterprises. The BJP's NaMo App, the Congress party's data analytics operations, and the various state-level party IT cells constitute a distributed political data infrastructure of considerable power. Yet the DPDPA 2023 imposes no party-specific transparency obligations, no restrictions on the types of data that may be used for political targeting, and no requirement that voters be informed when they are the subject of microtargeting campaigns.

C. Consent: Thin and Thick

The Act's consent framework, while formally robust, is practically inadequate to the challenges of electoral data processing. The Act requires that consent be free, specific, informed, unconditional, and unambiguous.[21] In theory, this standard should preclude the kind of broad, blanket consent that characterizes most political app and platform data collection. In practice, however, the enforcement of meaningful consent in digital environments remains an unresolved challenge across every data protection jurisdiction in the world.

The problem is structural. The data that fuels electoral microtargeting is not typically collected through a single, identifiable consent transaction. It accumulates across dozens or hundreds of digital interactions, some explicitly political, many entirely commercial, each of which may have generated a nominal consent that covered the data collection in question but could not have anticipated its eventual aggregation into a political profile. A voter who consents to share location data with a navigation app, browsing history with a news platform, and contact

[20]DPDPA, supra note 2, § 2(i) (definition of "data fiduciary" — notably, the definition encompasses any person who determines the purpose and means of processing personal data, which would include political parties in respect of their voter data operations).

[21]DPDPA, supra note 2, § 9 (consent requirements mandating that consent be free, specific, informed, unconditional, and unambiguous).

ISSN: 2582-6433

details with an e-commerce site has not consented to have these data streams combined, enriched, and sold to a political party for use in a targeted persuasion campaign. The Act's consent framework, focused on the collection event rather than the downstream processing chain, cannot adequately address this aggregation problem.

V. THE REPRESENTATION OF THE PEOPLE ACT, 1951 AND THE ELECTION COMMISSION'S FRAMEWORK

A. The Anachronistic Architecture of Electoral Law

The Representation of the People Act, 1951, is the foundational statute of Indian electoral law. Drafted in a world without computers, let alone social media or algorithmic political advertising, it governs candidate registration, election expenses, corrupt practices, and electoral offences through a framework that is substantially untouched by the digital revolution. The Act's provisions on election expenses, for instance, require candidates to disclose expenditure on "advertisements"[22], a category developed with newspaper and poster advertising in mind and stretched uncomfortably to accommodate digital advertising expenditure, but wholly unequipped to address the cost and opacity of data procurement for microtargeting campaigns.

Section 123 of the Act defines "corrupt practices" in electoral law.[23] It includes bribery, undue influence, promotion of enmity on grounds of religion, caste or community, and the use of government machinery for electoral advantage. Notably absent from this catalogue, and this absence was excusable in 1951 but is inexcusable today, is any recognition of data manipulation, psychographic targeting, or the systematic deployment of personal data to engineer voter behavior as a corrupt or impermissible electoral practice. The manipulation of voters through unauthorized personal data processing is not a corrupt practice under Indian law. It is not even a regulated practice.

B. The Model Code of Conduct's Digital Extension

The Election Commission of India has made some efforts to address digital electioneering through extensions of the Model Code of Conduct and through specific guidelines on social media and political advertising. In 2019, the Commission required political

[22]RPA, supra note 3, § 77 (election expenses — candidates required to maintain accounts of expenses incurred in connection with the election).
[23]RPA, supra note 3, § 123 (defining "corrupt practices" for electoral purposes — the catalogue does not include data manipulation or psychographic targeting).

ISSN: 2582-6433

parties to obtain pre-certification for political advertisements on electronic media, including digital platforms, through a Media Certification and Monitoring Committee process.[24] This was a meaningful step toward advertising transparency, but it targeted the advertisement itself rather than the underlying data infrastructure.

The Commission's 2019 social media guidelines required candidates and political parties to submit details of their social media accounts and expenditure on political advertisements on digital platforms.[25] These guidelines created a formal accountability mechanism that did not previously exist. However, they do not require disclosure of data sources used for microtargeting, do not mandate disclosure of the targeting parameters applied in political advertising campaigns, and do not extend to organic, as opposed to paid, political content, including the network of WhatsApp groups that constitute the most significant channel of targeted political communication in India.

C. Voter Roll Data: Public Document, Private Commodity

The Election Commission's management of voter roll data raises its own set of concerns. Voter rolls are public documents under the Registration of Electors Rules, 1960, and are available for public inspection and download.[26]

However, the public nature of voter roll data has been systematically exploited by political actors to build the foundational layer of microtargeting databases. When voter roll data is combined with commercial data sources, social media profiles, and community-level information, it produces a profile of individual voters that was never contemplated by the Registration of Electors Rules and that would constitute a serious invasion of privacy if collected through any other means. The Commission has no framework for restricting the use of voter roll data for commercial or political profiling purposes, and no technical controls on the downstream use of data obtained from its official sources.

VI. TOWARD A FRAMEWORK OF ELECTORAL DATA RIGHTS

A. Reconstituting the Voter as Data Subject

Any serious legal response to electoral microtargeting in India must begin by reconstituting the voter as an active data subject with enforceable rights, rather than a passive

[24]Election Commission of India, Media Certification and Monitoring Committee Guidelines for Political Advertisement on Electronic and Social Media (2019) (requiring pre-certification of political advertisements on electronic media including digital platforms).
[25]ECI Social Media Guidelines, supra note 23, at 8-11 (requiring political parties to submit social media account details and digital advertising expenditure disclosures).

ISSN: 2582-6433

object of political data processing. This reconstitution requires both statutory amendment and institutional reform. At the statutory level, the DPDPA 2023 should be amended to include political parties within its definition of significant data fiduciaries, imposing enhanced transparency, accountability, and purpose limitation obligations on their electoral data processing activities.[27][28]

Political parties should be required to publish annual data protection impact assessments of their electoral data operations, including the sources of data used, the targeting parameters applied, and the third-party contractors engaged in data processing. Beyond the DPDPA, the Representation of the People Act should be amended to create a category of prohibited electoral data practices. At minimum, this category should include: the processing of voter data obtained without informed and specific consent for political microtargeting purposes; the acquisition of electoral data from commercial data brokers without voter consent; the use of psychographic profiling techniques that exploit psychological vulnerabilities for political persuasion; and the deployment of automated decision-making systems to target voters with political messages without disclosure to the targeted voter.

B. Algorithmic Transparency in Electoral Advertising

The invisibility of microtargeting to its targets is not a technical inevitability; it is a regulatory choice. Platforms that serve political advertisements already maintain detailed records of the targeting parameters used in each campaign. The European Union's political advertising regulation provides a model: platforms must maintain a public repository of political advertisements, including the targeting parameters used, the population reached, and the expenditure incurred.[29]

An Indian political advertising transparency framework should require platforms operating in India to maintain a public repository of political advertisements during election periods, including the targeting criteria applied. This requirement should extend to paid political content, sponsored content, and content amplified through coordination networks. The Election Commission should be designated as the competent authority to receive, publish, and audit political advertising data, with the power to require platforms to produce this data and to sanction non-compliance.

[27]Subhashish Bhadra, Voter Data and Privacy: An Examination of the Indian Electoral Framework, 14 Indian J. L. & Tech. 112, 118-125 (2018).
[28]Pranesh Prakash & Nayantara Ranganathan, The Privacy Paradox in India's Data Protection Bill, Economic & Political Weekly (Aug. 17, 2019).

ISSN: 2582-6433

C. Data Minimization and Purpose Limitation

The principle of data minimization, that only data necessary for a specified, legitimate purpose should be collected — has a particularly important application in the electoral context. The comprehensive voter profiles that fuel microtargeting extend far beyond any legitimate political communication purpose. A political party communicating its policy positions to a voter needs to know that voter's constituency and perhaps her language preference; it does not need her psychographic profile, her browsing history, her inferred religious identity, or her behavioral triggers.

An electoral data minimization framework should establish a permitted purpose limitation for political data processing, specifying the types of personal data that may legitimately be collected and used for political communication and prohibiting the collection or processing of data beyond this scope. This framework should draw a clear distinction between voluntary engagement data, information that a voter actively provides to a party through membership, donation, or direct contact, and behavioral inference data gathered through surveillance of the voter's digital activities. The former has a clear legitimate basis; the latter does not.[30][31]

The voter roll should be treated as a distinct category of electoral infrastructure data, subject to enhanced purpose limitation restrictions. Entities that obtain voter roll data should be required to commit to purpose limitations that prohibit its combination with commercial data sources for profiling purposes. The Election Commission should develop technical standards for voter roll data use that enforce these limitations, including contractual obligations on entities receiving official voter data.

VII. CONCLUSION

The invisible voter is not a metaphor. She is the product of a legal vacuum that has allowed political actors to transform the most intimate details of citizens' digital lives into instruments of electoral manipulation, without consent, without transparency, and without accountability. The constitutional foundations for protection are present: Puttaswamy's recognition of informational privacy as a fundamental right, the right to vote's implicit guarantee of a deliberatively authentic electoral environment, and Article 19's protection of a genuinely free epistemic public sphere together provide a robust constitutional basis for

[30]Usha Ramanathan, A Jurisprudence of Identity and Surveillance, 3 Seminar 583, 591 (2016).
[31]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power 293-315 (2019).

ISSN: 2582-6433

electoral data rights. What is missing is the statutory and institutional architecture to give these rights practical effect.

The case for urgency is compelling. India's 2024 general election was the largest democratic exercise in human history, engaging nearly a billion eligible voters. The sophistication of political microtargeting operations in that election dwarfed anything that preceded it. The next election cycle will bring further advances in artificial intelligence-enabled behavioral prediction, deepfake-assisted personalized messaging, and real-time psychographic profiling that will make the current generation of microtargeting tools look primitive by comparison.

India's constitutional commitment to democracy is not merely procedural. It encompasses the substantive conditions of democratic participation: an informed citizenry, an authentic public sphere, and the protection of individual autonomy against manipulation by those who seek power. Microtargeting, as currently practiced, threatens all three. The law has the tools to respond. The question is whether the political will exists to deploy them in defense of the voter who, in the data economy of modern elections, has become all too invisible.