

Chapter - II

THE POLITICS YOU NEVER SAW: MICROTARGETING AND THE MANUFACTURE OF MISINFORMED VOTERS

BY

Soham Gupta & Prabhas Kumar

Abstract

In today's information economy, fake news takes many forms. One of its less discussed but structurally most destructive forms is electoral misinformation driven by microtargeting. This practice has transformed political communication from a public contest of ideas into a fragmented marketplace of personalised promises. Campaigns abuse behavioural and psychographic data to selectively present conflicting versions of their manifesto—promising welfare to one community while assuring fiscal restraint to another. This selective disclosure shapes multiple political realities, leading to widely misinformed citizens.

Our chapter analyses this practice, emphasising that the harm done by strategic omission manipulates electoral choice while remaining legally invisible. Existing Indian frameworks—the Model Code of Conduct, the Representation of the People Act, and the newly enacted DPDP Act—are architecturally designed for the "visible spectacle" of public campaigning and fail to address persuasion in the private digital domain. Drawing from the structural failures of US transparency models and EU content regulations, the chapter warns of a "regulatory blind spot." We propose that rather than policing truth, the law must enforce procedural safeguards to restore the shared field of contestation essential for democratic legitimacy.

Keywords: Electoral Microtargeting, Strategic Omission, Indian Election Law, Algorithmic Persuasion, Digital Undue Influence

Electoral Harm Without Falsehood: Reframing “Fake News” in the Age of Microtargeting

In the Indian democracy, while legal discourse focuses on public debates and rallies, a more damning possibility unfolds on the personal screens of over 500 million Indian WhatsApp and Facebook users¹. Due to growing digitisation and the addictive nature of these channels, the broader public discourse has been silently overshadowed by private, invisible feeds. Today, the loudest campaigns are run on these personalised channels, yet no one else hears them.² To understand this silent noise, we must first define the engine driving it: “microtargeting”.

At the simplest level, microtargeting utilises vast aggregates of personal data, such as browsing history, location patterns, and purchasing habits, to categorise audiences and serve them hyper-personalised ads to influence consumer behaviour. If you search for shoes, your algorithm will serve you with ads for discounts on sneakers. However, Electoral Microtargeting weaponises this commercial tool for voter manipulation.³ By processing thousands of data points, sourced from an already digitally illiterate populace, from electricity bills to caste affiliation, even to “likes” on social media, political actors then capitalise and build psychometric profiles that, to a reasonable degree, predict a voter’s fears, prejudices, and triggers⁴. Once these profiles are established, the campaign no longer needs to make anodyne unified promises to the public through the regulated mainstream media. Instead, it can now generate thousands of unique ad variations, each calibrated to a specific individual’s psychological profile, capitalising on their fears and prejudices, providing far greater penetration within vulnerable voter bases, due to these bolder, unregulated campaigns.

This marks a stark divergence from the “traditional methods” of campaigning and outreach. Within the contours of these traditional methods, a candidate cannot promise industrial development in corporate lobbies while simultaneously promising forest protection to tribal communities in the same campaign without being exposed. But within the unregulated digital realm, electoral microtargeting allows for “strategic omission”. A young gig-worker sees a promise about digital labour rights, while a rural landowner in the same constituency sees a promise about protecting land banks. Neither knows what the other has been shown.

¹ WANotifier, ‘WhatsApp Statistics 2025: Usage Trends and Demographics’ (WANotifier, 8 December 2025) accessed 20 December 2025; DemandSage, ‘WhatsApp User Base Report 2025’ (DemandSage, December 2025) accessed 20 December 2025.

² Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs 2019).

³ Frederik Zuiderveen Borgesius and others, ‘Online Political Microtargeting: Promises and Threats for Democracy’ (2018) 14(1) *Utrecht Law Review* 82.

⁴ Divij Joshi, ‘Data Privacy and Elections in India: Microtargeting the Unseen Collective’ (2022) 18(2) *Indian Journal of Law and Technology* 115.

This allows for fragmentation among voters based not on differing opinions but on differing versions of facts and reality as portrayed by these curated channels. Past instances like the Cambridge Analytica scandal demonstrate how actors harvest data to suppress turnouts and fan polarisation. This fear is further exacerbated by the current unprecedented growth in the utilisation of AI tools by these campaigns. During the 2024 general elections, more than 50 million AI-generated calls, which utilised voice clones to simulate personal relationships with voters, were made during the 2024 election cycle⁵. Research highlights how this “unawareness”, voters' inability to see the conflicting messages sent to others, is an essential condition for effective voter manipulation.⁶

The Existing Indian legal framework, from the Model Code of Conduct to the Representation of the People Act, is built on the presumption of visibility. This chapter argues that unchecked microtargeting is not just a privacy violation but a fundamental breach of democratic legitimacy. It manufactures misinformed voters not by lying to them, but by denying them the shared informational baseline necessary to make a meaningful choice.⁷

What Is Structurally New? From Targeted Politics to Uncontestable Persuasion

To regulate a harm, the law must first distinguish it from standard accepted practice. A common, often cynical objection to regulating microtargeting is the claim that “politics has always been targeted”. Critics, and indeed, legal defences for big tech often argue that political parties have effectively “microtargeted” Indian voters for decades, not with algorithms or AI, but simply through local intermediaries, caste associations, and regional manifestos. If a candidate speaks about crop prices in a rural APMC mandi and urban infrastructure in a city hall, are they not “segmenting” the electorate? This section argues that while the *intent* to segment has been continuous, the existing *structure* of digital persuasion represents a far more dangerous break from the past.⁸ We must distinguish between Traditional Political Targeting and Algorithmic Microtargeting.

Historically, Indian elections have been fought based on distinct community appeals. It should be considered as a feature, not a bug, of our diverse democracy that a candidate speaks one language to a weaver’s colony in Varanasi and another to a trader’s association in Mumbai. However, this

⁵ TechPolicy Press, ‘India’s Experiments with AI in the 2024 Elections’ (TechPolicy, 25 September 2024); The Hindu, ‘Deepfakes and Democracy: The 50 Million Call Benchmark’ (The Hindu, 29 March 2024).

⁶ Freek van Gils, Wieland Müller and Jens Prüfer, ‘Microtargeting, Voters’ Unawareness, and Democracy’ (2025) 41(2) Journal of Law, Economics, and Organization 634; Internet Freedom Foundation, ‘The Privacy Deficit in Indian Elections’ (IFF Working Papers, 2024).

⁷ Ujjwala Uppaluri and Dharmaraj Pal, ‘Electoral Democracy and the Right to Know: A Judicial Review’ (2019) 12 NUJS L Rev 1.

⁸ Philip N Howard and others, ‘The Political Economy of Social Media in India’ (2023) 15(3) Oxford Journal of Legal Studies.

traditional form of political targeting operated under a crucial structural constraint: “Audibility/Visibility”. When a politician stands on a podium at a rally, irrespective of whether he is addressing 500 people or 50,000, his speech enters the, as Habermas would put it, the “public sphere”.⁹ Even if the message is tailored to a specific caste or region, it is delivered within a public forum, accessible to all.

This form of physical targeting is automatically constrained by three layers of democratic accountability that microtargeting destroys.

First is “Visibility”. The Election Commission’s videographers, the press, and the general public witness and record these promises¹⁰. If a candidate makes an inflammatory statement or a legally actionable promise (such as bribery), it becomes a “Headline.” The law can see it because the medium is public. The discourse regarding it also operates in the Public Sphere. The second constraint is the “Reputational Constraint”. Since the message is public, it implicitly carries a cost. A party cannot promise *total* prohibition of alcohol to one group and *subsidized* liquor licenses to another in the same district without running the risk of the contradiction being exposed by the media or the opposition. The fear of being called a hypocrite and losing credibility among the voter base, a key factor within democratic setups, acts as a regulatory deterrent.¹¹

Third, and most vitally for our analysis, is “Contestability”. In traditional campaigning, the Opposition hears what the Incumbent says.¹² If Party A makes a false claim in a rally, Party B has the opportunity to rebut it in the next news cycle. The democratic process is essentially then a “clash of narratives” where the voter judges the winner of the argument. Therefore, traditional targeting, no matter how divisive, remained “contestable”. It existed within a shared reality where contradictions could be flagged, and lies could be challenged. A form of objectivity could be established.¹³ The black letter of law, specifically in context of Indian electoral setup, the Model Code of Conduct, was designed for this world. It served its purpose sufficiently well. It polices the “noise” of the rally and the “ink” of the pamphlet. It assumes that if a harm occurs, it will occur in the open, generating a headline that the law can then address. But what happens when the campaign moves from the podium to the pocket? What happens when the “Headline” disappears?

⁹ Jürgen Habermas, *The Structural Transformation of the Public Sphere* (MIT Press 1989)

¹⁰ Election Commission of India, ‘Manual on Model Code of Conduct’ (ECI 2019) Document 21/MCC/2019.

¹¹ Frederik Zuiderveen Borgesius and others, ‘Online Political Microtargeting: Promises and Threats for Democracy’ (2018) 14(1) *Utrecht Law Review* 82.

¹² Cass Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton University Press 2017).

¹³ Burkhard Schipper and Hee Yeul Woo, ‘Political Awareness, Microtargeting of Voters, and Negative Electoral Campaigning’ (2019) 14(1) *Quarterly Journal of Political Science* 41.

This is where Political Microtargeting (referred to as PTMC hereon) steps in. PTMC is fundamentally differentiated from the traditional practices, and to understand this, we need to first understand what actually happens in a scenario containing PTMC. Thus, we look at the hypothetical town of “Rajneeti”. Now, Rajneeti has two main parties competing for electoral seats, where party ‘A’ holds traditional targeted campaigns to be superior, while party ‘B’ is ready to innovate and try out new methods. So, in the elections of 2025, A starts by analysing the demographics through surveys and voter profiles. It drafts a district-wise manifesto, schedules rallies calibrated to caste and occupational composition, and trains its local leaders to emphasise different issues in different constituencies. Every promise is spoken aloud, every speech is recorded, every slogan is repeatable by the Opposition and reportable by the press. Party A’s strategy is segmented, but it is *legible*.

On the other hand, Party B takes a new mode. Party B begins not with districts or communities, but with *data exhaust*.¹⁴ It purchases voter datasets from data brokers, harvests engagement metrics from social media platforms, scrapes WhatsApp group memberships, analyses language preferences, browsing histories, consumer behaviour, religious content consumption, grievance posts, and past voting cues. Each voter in Rajneeti is no longer primarily a member of a caste, ward, or profession, but a probabilistic profile. Then, using machines, messages are drafted for each voter, students are sent the promise of a new education scheme, employees are sent the promise of higher pensions, businesses are sent the promise of easier and cheaper employee procurement, tribals are sent the promise of stronger land rights, industries are promised more area to mine and set up machinery, while a staunch supporter of the party is served no message, just silence. These clusters are continuously updated as voters scroll, like, pause, or forward content. Unlike Party A’s static segmentation, Party B’s targeting is adaptive, iterative, and opaque.

The first political idea that collapses with this practice is visibility. None of these messages became headlines. No videographer records them. No journalist sees the full picture. Each message is privately delivered to a pocket, disappears after 24 hours, and leaves no public trace. Even if a message is inflammatory, false, or legally impermissible, it is structurally invisible to regulators. This in itself makes these messages dangerous, eroding away the political accountability as each promise shifts from the public sphere to the personalised bubble of each person. Contradiction no longer is a threat to the political party as it weaponises it to be agreeable to more people. Contradictions and promises are never subject to public judgment, and reputation, a variable of this judgment of the

¹⁴ Philip N Howard, ‘The Political Economy of Social Media in India’ (2023) 15(3) Oxford Journal of Legal Studies 45.

shared exposure, becomes fragmented into millions of private impressions. No voter can tell if they are being lied to, as they no longer know what the other person has been told.

Most dangerously, PTMC destroys contestability. Party A never hears Party B's messages. There is nothing to rebut. No false claim can be challenged if it is never publicly made. The democratic process ceases to be a contest of ideas and becomes a contest of influence operations, where success is measured not by persuasion in public debate but by behavioural nudges executed in private. Party B observes voters continuously, while voters observe Party B only through curated, personalised fragments. The epistemic playing field collapses.¹⁵ In Rajneeti, voters no longer deliberate within a shared reality. They pass through parallel informational worlds, each one quietly calibrated to their fears, prejudices, and emotional triggers. Elections are no longer fought in the public sphere but inside millions of sealed private psychological spaces. The story of Rajneeti is not merely hypothetical; it mirrors documented realities. The Cambridge Analytica scandal demonstrated the scale of psychographic profiling, while the 2019 and 2024 Indian elections highlighted how WhatsApp moves political messaging into encrypted networks entirely outside public scrutiny.

Political microtargeting thus dismantles the structural conditions for democratic accountability. It eliminates visibility by relocating persuasion to private feeds and fragments reputation by allowing contradictory promises to coexist without judgment. Most dangerously, it destroys contestability. When regulators, the press, and opponents cannot see the message, there is nothing to rebut. Elections cease to be a public contest of ideas, devolving into isolated influence operations where voters respond to curated narratives engineered to remain unseen and unaccountable.

Strategic Omission as Electoral Misinformation: How Parallel Political Realities Are Manufactured

If visibility was the first democratic casualty of political microtargeting, omission is what finishes the job. Unlike false claims or inflammatory speeches, omission leaves nothing behind. It generates no headline.¹⁶ It invites no rebuttal. It triggers no immediate legal response. And yet, it is through this carefully engineered silence that political microtargeting manufactures electoral misinformation without ever having to speak an untruth.

¹⁵ Md Ishtiaq Hossain, 'The Algorithmic Public Sphere: Rethinking Journalism, Communication, and Democracy in the Digital Era' (2025) ResearchGate.

¹⁶ Tom Dobber and others, 'Political Microtargeting: Towards a Pragmatic Approach' (2023) 12(1) Internet Policy Review.

Strategic omission must therefore be understood not as accidental silence or mere rhetorical discretion, but as a deliberate form of electoral communication. It involves the targeted withholding of issue positions, trade-offs, or priorities from particular segments of the electorate, even as those same positions are openly disclosed to others. The defining feature of this practice is not falsity, but selective visibility.¹⁷ The harm does not lie in voters being told something wrong. It lies in voters being shown only a fragment of the political reality they are being asked to choose from.

This distinguishes strategic omission from deception: deception relies on falsehoods; omission uses truthful fragments made misleading by design. A voter may receive only accurate messages and yet remain fundamentally misinformed about the political project they are endorsing.¹⁸ A campaign may truthfully promise welfare expansion to one segment, infrastructure growth to another, and fiscal restraint to a third, while never disclosing the trade-offs that make these commitments mutually incompatible.

It is equally distinct from persuasion. Traditional persuasion operates within a shared communicative field. Different audiences may hear different emphases, but the underlying content remains broadly common and publicly contestable. Strategic omission fractures this field itself. The electorate no longer encounters one political programme interpreted differently, but multiple versions of reality, each insulated from the others.¹⁹ Nor is this merely a matter of framing. Framing selects interpretive lenses over common facts. Strategic omission removes facts from shared circulation altogether.

This is how omission becomes misinformation without falsehood. Conventional accounts of misinformation focus on error: voters are misled because they are induced to believe something untrue. Strategic omission produces harm through informational incompleteness under conditions of asymmetry. Voters cannot know what has been omitted, nor can they infer it through ordinary political engagement, because the missing information exists only in parallel, inaccessible channels.²⁰

The consequence is a sharp divergence between individual accuracy and collective intelligibility. Individually, voters may form reasonable beliefs based on the information presented to them. Collectively, however, the electorate loses the capacity to evaluate trade-offs, detect contradictions,

¹⁷ Ellen P Goodman, 'Digital Information Fidelity and Friction' (2020) Knight First Amendment Institute.

¹⁸ Claes de Vreese and others, 'The Datafication of Campaigning' in *Digital Democracy, Analogue Politics* (Oxford University Press 2018).

¹⁹ Michael Bennett and Shanto Iyengar, 'A New Era of Minimal Effects? The Changing Foundations of Political Communication' (2008) 58(4) *Journal of Communication* 707

²⁰ S Nageeb Ali and others, 'Electoral Competition with Strategic Disclosure' (2019) 10(3) *Games* 29.

or assign responsibility. Elections cease to aggregate preferences over a shared political offer and instead aggregate reactions to fragmented narratives.

This harm is not reducible to voter manipulation or autonomy loss. It is a structural failure of electoral aggregation itself. Electoral law has historically assumed that political promises are publicly observable, that voters can compare competing claims across the electorate, and that elections aggregate preferences over a common set of representations. These assumptions tolerate exaggeration and rhetoric, but they require comparability.

Strategic omission undermines these assumptions without violating any explicit rule. The conduct may remain formally lawful, yet it defeats the functional premises upon which electoral accountability depends. Traditional targeting differentiated audiences within a public sphere. Microtargeting, through omission, insulates audiences from one another.

The cumulative effect is the manufacture of parallel political realities. Different voters encounter different issue hierarchies, different silences around costs, and different implied priorities. No single voter sees the full political programme, and no institution can reconstruct it in real time. Accountability collapses because promises cannot be collectively evaluated.²¹ Mandates become indeterminate because it is unclear which version of the political project has been endorsed.

Elections, in such a system, no longer aggregate preferences over a common set of claims; they aggregate responses to fragmented, privately curated political narratives that are individually truthful yet collectively unintelligible.

Existing electoral law does not know how to see this harm. Strategic omission triggers none of its traditional categories. It is therefore rendered legally invisible, even as it corrodes the conditions of electoral accountability. The next section shows how Indian electoral doctrine inherits this blindness, treating microtargeted communication as benign speech differentiation rather than as a failure of electoral integrity.

The Indian Regulatory Blind Spot: Why Electoral Law Cannot See Private Persuasion

Electoral microtargeting represents a clear structural break from traditional politics, yet our legal framework remains stuck in the past. Despite *prima facie* comprehensiveness, the Indian electoral regime still remains architecturally designed only for regulating the “visible spectacles” of electoral

²¹ W Lance Bennett and Shanto Iyengar, ‘A New Era of Minimal Effects? The Changing Foundations of Political Communication’ (2008) 58(4) *Journal of Communication* 707.

campaigning.²² It assumes that this political persuasion generally occurs through public, verifiable mediums such as rallies or newspapers. Consequently, when this persuasion shifts to the private, infinite scrolls of smartphones, a evident "regulatory blind spot" emerges. This is not due to any regulatory oversight or flaws in the enforcement of statutes, but rather it exists due to a fundamental design failure within our laws, which are still stuck in the past.

As visible from the Model Code of Conduct (MCC) suffers from a fatal "category error" because it mistakenly correlates visibility with persuasion. Its provisions, such as the ban on casteist and communal appeals or the mandatory "Silence Period" (48 hours before polling), depend heavily on the physical visibility of these offences²³. In the physical world, violations are public events recorded by the Election Commission, even visible to the opposition. However, In the digital realm, microtargeting creates a "verification vacuum."²⁴ For instance, a "dark ad" which incites fear within a specific demographic on WhatsApp is wholly invisible to the regulator, seen only by the voters who are already primed to accept it as true. Furthermore, modern algorithmic delivery mechanisms render the Silence Period infructuous, as programmatic ads continue running on personal feeds via remote servers, thereby bypassing the ban. This opacity violates the voter's fundamental Right to know by reducing the entire electorate to mere passive recipients of these politically curated realities.²⁵ By regulating only the *noise* of the election while leaving the *signal* unchecked, the MCC effectively nullifies the informed consent essential for a valid democratic mandate.

The "hard law" doesn't fare any better. *Section 123(2)* of the RPA defines "undue influence" as interference with electoral rights²⁶. However, the Supreme Court in *Shiv Kirpal Singh v. V.V. Giri* has restricted this definition to visible threats like physical injury or spiritual censure.²⁷ However, the modern emerging variant, "Digital undue influence", operates through informational distortion, through targeted suppression campaigns using false polling data rather than physical coercion, thereby not being within the definition's ambit. This blindness extends to hate speech regulation, namely *Section 196* of the Bharatiya Nyaya Sanhita, 2023 (formerly *IPC 153A*), which criminalises promoting enmity between groups. The law presupposes a public element within the act of hate speech²⁸. However, in the age of microtargeting, hatred is seeded through encrypted, curated channels

²² Ujjwala Uppaluri and Dharmaraj Pal, 'Electoral Democracy and the Right to Know: A Judicial Review' (2019) 12 NUJS L Rev 1.

²³ *Abhiram Singh v CD Commachen* [2017] 2 SCC 629 (SC).

²⁴ Nathaniel Persily, 'The Internet's Challenge to Democracy: Framing the Problem and Assessing Reforms' (2019) Kofi Annan Commission on Elections and Democracy in the Digital Age.

²⁵ *Shreya Singhal v Union of India* [2015] 5 SCC 1; Constitution of India 1950, art 19(1)(a).

²⁶ Representation of the People Act 1951, s 123(2).

²⁷ *Shiv Kirpal Singh v VV Giri* [1970] 2 SCC 567 (SC).

²⁸ Bharatiya Nyaya Sanhita 2023, s 196.

like WhatsApp and Facebook. The State cannot regulate or prosecute what it cannot witness. Similarly, Section 127A of the RPA, originally designed to prevent anonymous pamphleteering, has been rendered obsolete by "shadow committees" and programmatic exchanges that leave no clear financial or evidentiary trace²⁹, leaving the statute regulating *paper* while elections unfold on *pixels*. Even if it is caught in time, due to anonymity, the attribution of responsibility becomes almost impossible.

Nonetheless, the most critical failure by far lies within the text of the Digital Personal Data Protection (DPDP) Act, 2023. Instead of shielding voters as intended, it contrarily empowers microtargeters. Section 17(2)(a) of the Act exempts "publicly available personal data" entirely from any protection, effectively legalising the scraping of social media profiles by these entities³⁰. Allowing them to treat a public tweet as consent for psychometric profiling. This aspect of legislation clearly violates the principle of informational self-determination as established by the bench in *Justice K.S. Puttaswamy v. Union of India*. Privacy, the Court held, follows the *individual*, not the *platform*.³¹

Further, the Act fails to explicitly protect "inferences," the subjective profiles derived from raw data. The core harm of microtargeting lies not in raw data but in predictive labels like "neurotic" or "susceptible to communal triggers."³² While early drafts of the act recognised inferences as personal data, the final Act omits them.³³ This allows political strategists to shield manipulative profiles as "trade secrets," protecting the *input* while leaving the *output* unregulated. Finally, the Act ignores "collective privacy." By treating data as a transactional asset between individuals and fiduciaries, it fails to address how microtargeting fragments the *demos* into incompatible realities.³⁴ India risks creating a regulatory scarecrow: visible enough to claim authority, but hollow enough for manipulation to pass through. Until the law forces persuasion back into the public sphere and recognizes inferences as protected data, the democratic mandate remains compromised at the point of formation.

Regulating Invisible Persuasion: Comparative Failures and Procedural Remedies

When the law attempts to regulate political microtargeting, it does so using instincts developed in a very different democratic environment. These instincts are not misguided. They are inherited. They

²⁹ Representation of the People Act 1951, s 127A.

³⁰ Digital Personal Data Protection Act 2023, s 17(2)(a).

³¹ Justice KS Puttaswamy (Retd) v Union of India [2017] 10 SCC 1

³² Vidhi Centre for Legal Policy, 'Securing Neuro-Privacy: Regulating the Mental Commons' (Vidhi 2024).

³³ Committee of Experts under the Chairmanship of Justice B N Srikrishna, A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (Ministry of Electronics and Information Technology 2018) 24.

³⁴ Balakrishnan Rajagopal, 'The Architecture of Invisibility: Digital Influence in the Global South' (2023) 34 European Journal of International Law 789.

come from a time when persuasion was loud, public, and contestable. The problem is not that the law has responded too slowly. It is that the law has responded to the wrong thing.

Across jurisdictions, three regulatory responses repeat themselves. The first is transparency. In the US, post-2016, platforms introduced ad libraries to reveal funding and targeting. The hope was that visibility would ensure accountability. During the 2020 and 2024 elections, journalists relied heavily on these tools. And yet, something crucial was missing. The libraries showed ads one by one. They never showed the whole campaign.³⁵ A welfare promise shown to one community and a fiscal restraint promise shown to another never appeared side by side. Nothing looked contradictory because nothing was ever visible together. India is already moving in this direction. The Election Commission's recent emphasis on platform cooperation, voluntary disclosures, and advertising transparency mirrors this American instinct. It creates visibility. It does not create comparability. The harm remains untouched.

The second instinct is restraint. In the United States, the constitutional free speech doctrine has made regulators deeply cautious.³⁶ Political targeting is treated as political expression. Segmentation is viewed as a strategy. Courts intervene only when the content is clearly unlawful. This has allowed microtargeting to flourish while remaining legally invisible.³⁷ India is not bound by the First Amendment, but the hesitation is familiar. Courts are wary of regulating political speech. Regulators step back. And the most powerful form of persuasion quietly fills the space.

The third instinct is content control. The European Union has gone furthest here. Through the Digital Services Act, the EU attempted to regulate misinformation, restrict sensitive data use, and force disclosure.³⁸ On paper, this looks decisive. In practice, it produced an unexpected result. Faced with compliance burdens, Meta and Google chose to withdraw paid political advertising from the EU entirely. Political persuasion did not stop. It simply moved to unregulated spaces like influencers and encrypted messaging.³⁹

Across these systems, the failure is consistent. Transparency assumes harm lies in secrecy. Restraint assumes segmentation is benign. Content regulation assumes harm lies in falsity. Strategic omission fits none of these categories. It operates through selective truth. Through silence. Through fragmentation. Even perfect enforcement of existing rules cannot surface what was never disclosed.

³⁵ Paddy Leerssen and others, 'Platform Ad Archives: Promises and Pitfalls' (2019) 8(4) Internet Policy Review.

³⁶ *Washington Post v McManus*, 944 F 3d 506 (4th Cir 2019).

³⁷ *Citizens United v Federal Election Commission* 558 US 310 (2010)

³⁸ Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising [2024] OJ L.

³⁹ Catalina Goanta and Sofia Ranchordás, *The Regulation of Social Media Influencers* (Edward Elgar Publishing 2020).

For India, this comparative experience matters deeply. Our electoral law is built around visibility. The Model Code of Conduct regulates rallies, speeches, posters, pamphlets, wall writing. It regulates what can be seen, heard, photographed, and reported. It assumes that persuasion happens in public. It assumes that if something goes wrong, it will happen loudly. It will spill into the newspapers. It will become a headline. Political microtargeting breaks this assumption completely, and yet it does so without breaking a single black-letter rule.

This means the regulatory question itself has to change. The question is not what political actors are saying. It is not even whether they are lying. Those are questions the law knows how to ask. The harder question is whether elections are still taking place within a shared field of contestation. Indian election law already understands this logic, even if it has never had to apply it here. Spending limits exist not to judge content, but to preserve fairness. Silence periods exist not to censor speech, but to protect deliberation. The law intervenes not because speech is dangerous, but because elections are fragile.⁴⁰

The same logic must apply now. Procedural safeguards must ensure that political persuasion does not dissolve into millions of untraceable fragments. Oversight bodies must be able to see the informational terrain on which elections are actually fought. Rival campaigns must be able to hear what is being promised elsewhere, even if it is not being promised to them. This is not about saving voters from manipulation. That is a weaker claim. It is about preserving the structure within which political disagreement can still occur. The harm, then, is not privacy. It is not persuasion. It is not falsity. It is the slow, quiet collapse of shared political reality. Where political persuasion becomes invisible and non-comparable, Indian electoral law is entitled to intervene. Not to police truth. But to restore the conditions under which democracy can still recognise itself.

-----*****-----

⁴⁰ Secretary, Ministry of Information and Broadcasting v Cricket Association of Bengal (1995) 2 SCC 161