POLICY ACCESS

SOCIAL MEDIA AND ELECTORAL BEHAVIOUR

IMPACT OF DIGITAL CAMPAIGNING AND MISINFORMATION ON VOTER PERCEPTION

Introduction

Social media has transformed political campaigning in the past decade, enabling parties to bypass traditional media and directly reach voters. In India's 2014 general election, often called the first "social media election", the Bharatiya Janata Party (BJP) leveraged platforms like Facebook, Twitter, and YouTube to connect with millions of voters.[1] By 2019, social media had become deeply embedded in India's electoral process, with those platforms serving not just as outreach channels but as primary spaces where political narratives, campaign messaging, and voter mobilisation occurred at scale.[2] Globally, events such as the Cambridge Analytica scandal in the 2016 U.S. presidential election have highlighted the darker side of these trends. Cambridge Analytica's misuse of Facebook data to profile and target U.S. voters showed how psychographic micro-targeting could be weaponised to influence perceptions.[3] The same election saw an onslaught of "fake news" on social media and even foreign interference, underscoring how easily misinformation can spread online. These examples, from India's WhatsApp-fueled campaigns to data analytics in America, illustrate a new paradigm in which digital campaigning can decisively shape public discourse. This report examines that paradigm, asking how digital campaigning and misinformation influence voter perception, and what policy interventions are needed to safeguard democratic integrity.

Digital Campaigning

- **Data-Driven Micro-Targeting:** Modern political campaigns use big data analytics to tailor messages to specific demographics and even individual voters. Instead of one-size-fits-all messaging, campaigns deploy micro-targeted ads designed for narrow audiences. In the United States, Cambridge Analytica famously pioneered psychographic targeting by harvesting Facebook profiles to predict personality traits, then delivering customized political ads exploiting those traits.[3] This precision targeting can make campaign messages unreachable to the broader public, as only the intended niche audience sees them. While micro-targeting improves efficiency in reaching voters, it raises transparency concerns. These personalized ads, often called dark ads, are visible only to select users and thus escape the scrutiny that traditional mass media ads would receive. Observers have warned that undisclosed online campaign ads and sponsored posts make it harder for the public (and regulators) to know who is behind the messaging.[4]

- **Influencers and Digital War Rooms:** Alongside targeted ads, parties now mobilize armies of online influencers and volunteers to amplify their narratives. Major parties operate centralized social media command centers, sometimes dubbed digital war rooms, to coordinate strategy and respond in real time. For instance, after being outplayed online in 2014, the opposition Congress Party set up digital war rooms by 2019 where teams monitored trends and crafted rapid social-·media responses.[5] In one such war room in Rajasthan,Congress staff and volunteers designed campaign graphics and blasted instructions via WhatsApp to thousands of local workers.[5] This influencer-driven model turns supporters into campaign messengers, from grassroots volunteers and party devotees to paid social media influencers, all working in tandem to shape the narrative. However, the line can blur between genuine grassroots enthusiasm and coordinated propaganda, and spread of polarizing content and sometimes harassment, complicating the online civic space.

- **Messaging Apps and Algorithmic Amplification:** Political campaigns now exploit virtually every online platform to reach voters, including private messaging apps. For example, in Brazil, WhatsApp groups became a major campaign tool, allowing parties to broadcast messages to micro-targeted community clusters. During Brazil's 2018 election, consultants flooded WhatsApp with campaign messages and partisan rumors, a tactic so influential that WhatsApp had to limit mass-forwarding to stem misinformation.[1] The appeal of messaging apps lies in their encrypted, peer-to-peer nature, a recommendation shared in a trusted family or community group can carry more weight than a public post. However, this closed network dynamic also sidesteps transparency and accountability. Social media algorithms on public platforms tend to amplify content that drives engagement, often sensational or emotionally charged posts. Research confirms that divisive political content is boosted by algorithms because controversy and outrage spur clicks and shares.[6] Campaign strategists are well aware of this feedback loop. They may coordinate a surge of posts or retweets to push a chosen narrative into trending topics, or time the release of provocative videos to maximize virality. The result is that extreme viewpoints or misleading claims can gain disproportionate visibility.

Misinformation and Manipulation

Social media's influence on elections comes with a flip side. The ease of spreading misinformation that distorts voter perceptions. Online platforms often function as echo chambers, meaning personalized information bubbles where users mainly encounter posts that reinforce their existing beliefs. This happens through self-selection (people follow like-minded pages and groups) as well as algorithmic curation (platforms feed users' content similar to what they've already liked or clicked).[6] Over time, insulated information environments harden opinions and exacerbate political polarization. Voters in opposing camps may live in entirely different factual universes online. Studies have found that confirmation bias and the "illusory truth effect" make people more likely to believe repeated claims, even if false.[6]

Misinformation exploits these biases, for example, extreme or emotive claims, when echoed frequently across someone's feed, start to feel credible. In election contexts, rumours and fake news can thus take on a life of their own. India's experience offers a cautionary tale, as in recent years, false messages on social media have incited real-world violence. A series of mob lynchings linked to false WhatsApp rumours about child kidnappers resulted in at least 18 deaths across India between April and July 2018, highlighting how quickly misinformation can trigger real-world violence.[7] A newly emerging threat in this domain is the use of deepfakes and synthetic media in politics. Deepfakes are AI-generated video or audio clips that convincingly mimic real people, for example, making a candidate appear to say something they never did. In early 2020, the BJP experimented with a deepfake campaign video in Delhi, using AI to have a party leader speak in different languages he doesn't actually speak.[8] While in this case it was presented as a novel outreach tool, it demonstrated the disruptive potential of deepfakes.

Maliciously deployed, a deepfake could be used to spread a damaging lie about an opponent on the eve of an election, too late to refute effectively. Once such a video goes viral, many voters may see it before any clarification emerges, and some fraction will believe it even after it's exposed as fake. Election authorities are just beginning to grapple with this problem. In India, the Election Commission issued an advisory in 2024 urging parties not to use deepfakes or misleading manipulated media in campaigns.[9] Yet enforcing such guidance is difficult. Much election-related disinformation falls into a gray area. It may be unethical and harmful to the public's understanding, but it isn't always illegal. Democracies protect political speech, even offensive or false speech, to a wide extent under free expression rights. We can say that current practices to counter digital misinformation in elections might not be the most effective. Fact-checkers and platforms can debunk individual hoaxes, and agencies like the Election Commission of India can issue warnings, but large gaps persist.

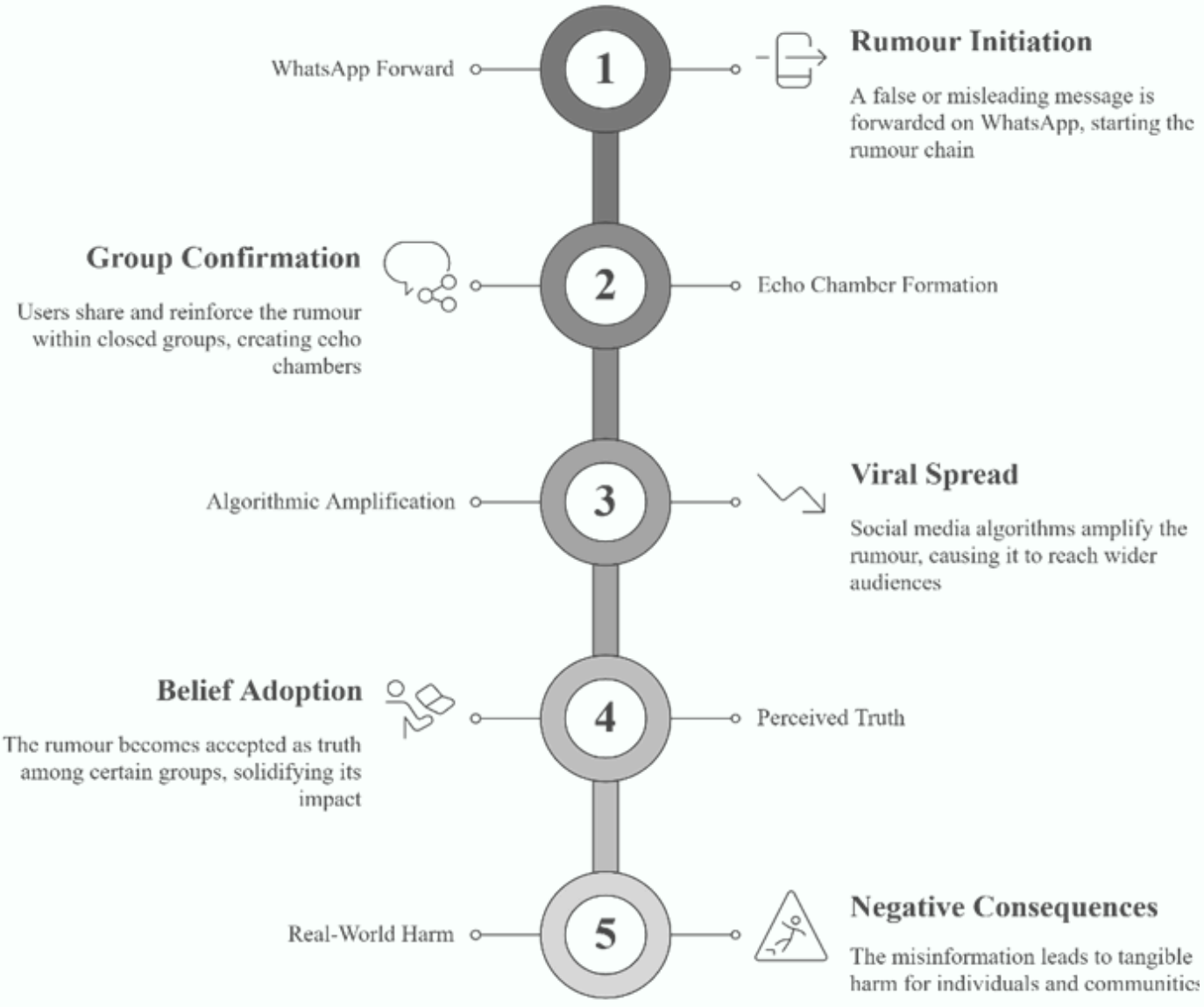

Fig.: The Cycle of Misinformation Spread (Author)

Policy Gaps in Regulation and Enforcement

Limits of Election Codes: Election regulators worldwide have been racing to update rules for the digital age, but enforcement is lagging. In India, the Election Commission's Model Code of Conduct (MCC), a voluntary code that guides campaign behavior, has been extended to cover social media activity. Candidates must now declare their official social media accounts to the Commission, and political ads on social platforms require pre-certification.[10] In 2024, the Election Commission issued a formal advisory directing all recognized political parties to avoid using deepfakes, manipulated media, and patently false information on their social media channels. The advisory emphasized that such synthetically altered content can mislead voters, deepen social divisions, and undermine trust in the electoral process. It required parties to remove any detected deepfake audio or video within 3 hours and to identify and warn the individuals responsible within the organization.[9] These steps marked progress, but their impact has been limited. The MCC remains essentially a gentleman's agreement without force of law, so its digital provisions rely on party goodwill and public pressure rather than penalties.

Platform Liability and Free Speech Trade-offs: Governments have also tried to make social media companies more accountable, but with mixed results. India's Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021, introduced some obligations for tech platforms, for example, requiring them to remove illegal content within 36 hours of a government order and to appoint local grievance officers.[11] The rules empower authorities to demand takedown of posts that violate laws (such as content inciting violence or spreading false information about voting procedures) and even to ask platforms to identify the originator of mass-forwarded messages in serious cases. These provisions aim to curb viral misinformation (e.g., the source of a dangerous WhatsApp rumor). However, significant enforcement and scope limitations persist, for instance, WhatsApp has strongly resisted the traceability mandate, arguing that undermining end-to-end encryption would harm privacy for millions of users.

Global Approaches - The EU vs. The U.S.: Globally, democracies are experimenting with different approaches to regulate digital campaigning. The European Union's Digital Services Act (DSA), fully in force since 2024, places systemic obligations on major platforms like Meta and Google, requiring them to assess risks to democratic processes, publish transparency reports, provide researcher access, and maintain public ad archives.[12] While it does not ban "fake news," the DSA formalizes platform responsibility for limiting harmful content. In contrast, the United States' strong First Amendment protections prevent the government from compelling platforms to remove even false political speech. Content moderation remains largely voluntary and is treated as a platform's own editorial right.[3] As a result, U.S. policy focuses more on ad labelling and transparency than removal of misinformation. These differing approaches show that democracies are still searching for effective ways to protect elections in the digital age, and significant regulatory gaps remain across models.

Recommendations

To safeguard elections in the era of digital campaigning and viral misinformation, a multifaceted approach is needed. Key policy-level recommendations are summarized in the table below. Each of these recommendations needs careful consideration. However, taken together, they offer a roadmap for strengthening transparency, oversight, and public resilience in the digital political arena.

Table: Summary of Key Policy Recommendations

Policy Recommendation	Details
Mandate transparency for online political ads	All online political advertisements should clearly identify their sponsor and funding source, similar to disclaimers on TV/radio ads. Platforms must maintain public ad archives with details of each political ad (content, target audience, money spent, etc.) updated in real time. This transparency shines light on "dark ads" and deters disinformation by enabling scrutiny. It allows regulators, journalists, and voters to see who is trying to influence whom.[4]
Strengthen real-time monitoring & fact-checking	Election authorities should partner with independent fact-checkers and civil society organizations to monitor online content and swiftly debunk falsehoods. Collaborative models have shown promise in the EU, such partnerships have improved resilience against disinformation.[12] While not everyone reached by a rumor will see the correction, creating an official counter-narrative limits the spread and provides a basis for removing or down-ranking proven false content.
Invest in digital literacy for voters	In the long run, the best defense is a more informed electorate. Governments, election commissions, and educators should launch digital literacy initiatives focusing on how to verify online information and think critically about social media content. Research consistently finds that higher digital literacy reduces susceptibility to falsehoods.[6] By immunizing voters against fake news and manipulative content, such programs strengthen democracy from the ground up.
Create an independent digital election watchdog	Governments should consider empowering an independent body to focus exclusively on monitoring and managing digital campaign activity. This Election Communications Watchdog would be non-partisan and staffed by tech experts, legal experts, and civil society representatives in addition to election officials. Its roles could include coordinating with social media platforms on campaign-period rules, investigating major incidents of online interference, and auditing platform algorithms post-election to assess their impact on political content visibility.
Enforce accountability for bots and fake accounts	Many disinformation campaigns rely on fake social media accounts, automated bots, and troll farms to amplify their messages. There is a need to crack down on these "force multipliers" of false information. Policy steps could include imposing higher penalties on political actors who are caught using bots or coordinated fake accounts to influence an election.

Conclusion

Digital campaigning has undoubtedly energized democracy by engaging new voters and enabling real-time dialogue between leaders and citizens. At the same time, it has blurred traditional boundaries between domestic and foreign influence, between factual debate and fabricated propaganda, and between open persuasion and opaque manipulation. The experiences of elections in India, the United States, Brazil, and elsewhere make clear that electoral institutions must adapt swiftly to this new reality. Protecting democratic integrity now requires continuous, evidence-based policy innovation that keeps pace with technological change. Regulations must be nuanced and strong enough to curb the harmful impacts of micro-targeting and misinformation, yet careful to uphold core free speech values. Going forward, all stakeholders share responsibility for fostering a transparent, truth-oriented information ecosystem. By implementing forward-looking reforms such as ad transparency, independent oversight, rapid fact-checking response, and voter education, we can harness the benefits of social media for democracy while mitigating its dangers. The challenge is ongoing, but the imperative is clear: to ensure that in the digital age, elections remain fair contests of ideas rather than races to manipulate perception.

BIBLIOGRAPHY

- V. Tyagi, (2025), The role of social media in shaping voter behaviour: A case study of India's 2014 and 2019 elections, International Journal of Creative Research Thoughts, 13(5).[
- S. Banaji & R. Bhat, (2019), How did social media impact India's 2019 general election?, Economic & Political Weekly Engage, 4(19), https://www.epw.in/engage/article/how-did-social-media-impact-india-2019-general-election.
- E. Oddleifson (2020), The effects of modern data analytics in electoral politics: Cambridge Analytica's suppression of voter agency and the implications for global politics, Political Science Undergraduate Review, 5(1), https://doi.org/10.29173/psur130.
- Campaign Legal Center. (n.d.). Digital ad disclosure, Retrieved November 15, 2025, from https://campaignlegal.org/democracyu/transparency/digital-ad-disclosure
- Kalra, A. (2018, December 20). An online battle for 900 million hearts and minds – India braces for 2019 election. Reuters. https://www.reuters.com/article/india-election-socialmedia-idUSKCN1OJ0DP.
- A., Edmans, & S., Murray, (2024, November 1), How misinformation and bias shapes what we believe, Think at London Business School, https://www.london.edu/think/how-misinformation-and-bias-shapes-what-we-believe.
- BBC News, (2018, July 17), WhatsApp violence: India lynchings on suspicion of child kidnapping, https://www.bbc.com/news/world-asia-india-44897714
- M., Alavi, (2020, February 20), BJP shared deepfake video on WhatsApp during Delhi campaign, NDTV, https://www.ndtv.com/india-news/in-bjps-deepfake-video-shared-on-whatsapp-manoj-tiwari-speaks-in-2-languages-2182923
- Express News Service, (2024, May 7), Election Commission to parties: Don't post deepfakes, misleading info on social media, The Indian Express, https://indianexpress.com/elections/election-commission-deepfakes-social-media-misinformation-mcc-9312006/ .
- Scroll.in, (2019, March 21), Election Commission may want to enforce Model Code of Conduct on social media, but it won't be easy, https://scroll.in/article/916517/election-commission-may-want-to-enforce-model-code-of-conduct-on-social-media-but-it-wont-be-easy
- Ministry of Electronics and Information Technology, (2023), Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Updated as of 06 April 2023), Government of India, https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf
- S., Calabrese, & J., Müller, (2025), The election year 2024 and tech policy around the world: What lessons for the European Union?, International Institute for Democracy and Electoral Assistance (International IDEA).

About Policy Access :

Policy Access partners with businesses to navigate India's complex policy and regulatory landscape through a blend of deep government insight, technical expertise, and on-ground execution.

Our strength lies in the diverse experience of our team including former government officials, public policy specialists, sector experts, and industry leaders who bring decades of hands-on experience in policymaking, regulatory engagement, narrative building and market access.

Headquartered in Gurugram, we work across multiple states and with stakeholders nationwide, enabling businesses to confidently scale in one of the world's most dynamic policy environments

Scan to know more about us !