TAKSHASHILA INSTITUTION

# Tensions Between Social Media and Democracy

**Bharat Sharma, Satya Sahu, Sachin Kalbag**

**Takshashila Discussion Document 2024-09**
**Version 0.5, May 2024**

This document is a compendium of two Working Papers presented at the April 2024 Internal Conference organised by the Takshashila Institution on the theme of democracy and social media. The papers featured in this document cover two aspects – institutional approaches taken to election misinformation, malinformation, and disinformation, and how technology increasingly impacts elections today.

***Recommended Citation:***
Bharat Sharma, Satya Sahu and Sachin Kalbag , "*Tensions Between Social Media and Democracy*", Takshashila Internal Conference Compendium Document No. 2024-09, April 2024, The Takshashila Institution.

# Executive Summary



**Sarthak Pradhan**

Social media's extensive reach, accessibility, and capacity to facilitate mass participation make it a preferred platform for people to stay informed about their surroundings and engage in discussions. Consequently, social media can significantly influence an individual's perspective on various issues, including their political choices. In other words, social media can potentially shape the course of democracy. In our endeavour to understand the relationship between social media and democracy, the Takshashila Institution hosted a conference on 24th April 2024. This document is a compendium of select curated working papers presented during the conference. In his paper, Bharat Sharma explores the current institutional mechanisms for dealing with misinformation, disinformation, and malinformation (MDM). He analyses the institutional responses to election MDM in different jurisdictions such as India, Finland, the European Union, and the United States and recommends the best course of action. Satya S. Sahu and Sachin Kalbag analyse technology's intricate and multifaceted influence on elections and political decision-making. They examine how various technologies are being leveraged by political parties. Furthermore, they explore how the dynamic interplay between political parties and governmental structures shapes India's

technological ecosystem. We welcome comments that build on and add to the ideas in this document. If you have any feedback, please contact us at research@takshashila.org.in.

**Authors**

Bharat Sharma is a Quad Studies Research Analyst with the Indo-Pacific Studies Programme at the Takshashila Institution.

Satya S Sahu is a Research Analyst with the High-Technology Geopolitics Programme at the Takshashila Institution.

Sachin Kalbag is a Senior Fellow (Information Policy and Governance) at the Takshashila Institution

# Table of Contents

# Institutional Approaches to Election MDM

**Bharat Sharma**

This paper considers institutional responses to rising activities regarding information manipulation, particularly in the context of social media's role in this domain. Four national/supranational entities are considered for this purpose: India, Finland, the European Union, and the United States.

India has been chosen because its study may offer interesting insights regarding how electoral information manipulation is tackled for a country possessing the world's largest electorate, with the coincidence of significant internet penetration and social media users. Finland is studied in the context of being one of the most resilient democracies whose citizens are considered most immune to information manipulation.

While the US does not have a dedicated section, its approach towards AI-linked disinformation is noted. The European Union's civil society response to significant vulnerabilities and highly complex geopolitical

environments — particularly noting the extent of Russian disinformation operations in EU countries — may offer a suitable example for ideal institutional mechanisms. Finally, the paper then focuses on extrapolating key institutional mechanisms that may offer insights regarding how election information manipulation may be combatted.

# Introduction: Disinformation as Threat

Manipulated information — misinformation, disinformation, and malinformation ("MDM") — has risen to be one of the biggest threats to social and political orders across the world. 'Misinformation' refers to false information that is not intended to cause harm. 'Disinformation' refers to false information intended to manipulate, cause damage and guide people, organisations, and countries in the wrong direction. Malinformation, lastly, refers to information that stems from the truth but is often exaggerated in a way that from the truth but is often exaggerated in way that misleads and causes potential harm.

As part of the Global Risks 2024 report, the World Economic Forum (WEF) called "misinformation and disinformation" the most severe global risk anticipated over the next two years, indicating that it may sharpen societal and political divides. In particular, the WEF notes that the widespread use of MDM — and tools to disseminate it — "may undermine the legitimacy of newly elected governments" risking violent unrest, terrorism, and social upheaval.

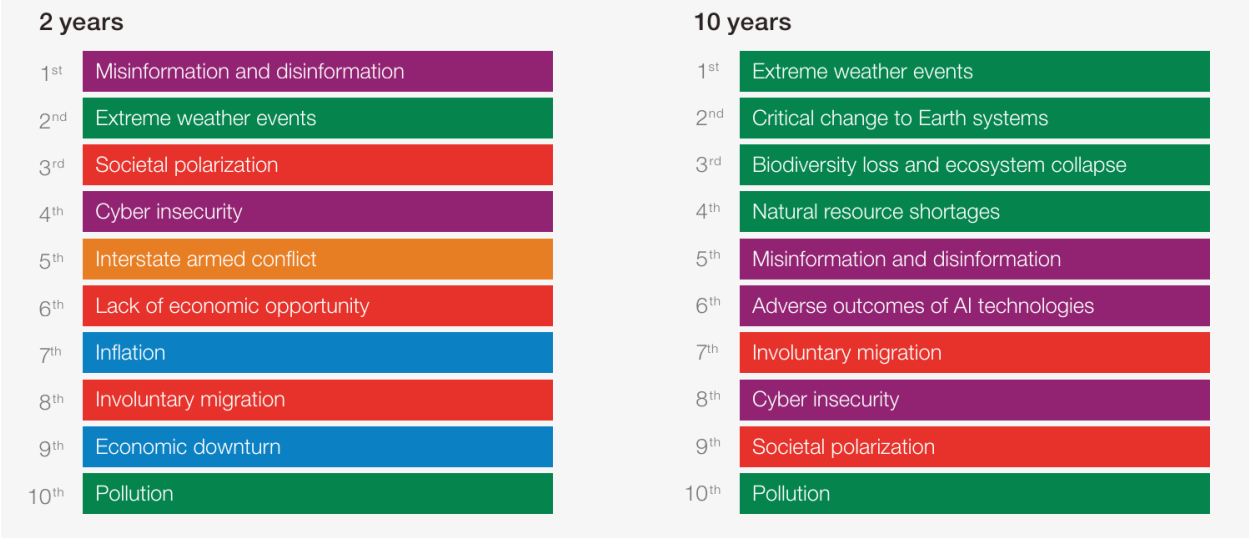



Figure: WEF's *The Global Risks Report 2024*

Democracies, in particular, are hostage to the risks of MDM, given that electoral integrity is a key component of any democratic polity. MDM substantively interferes with voters' ability to understand and participate in political processes, thereby undermining processes through which voters participate democratically. Disinformation, in particular, is a threat to deliberative democracy, in the context of healthy communication systems being hampered.

The prevalence of MDM cannot be isolated from the overarching information-security environment. A *weak* environment may be defined as the ability of a society to understand reality around them correctly, validate methods of knowledge, and place certain models in certain contexts. The "weakness" of such an environment is defined as a society generally lacking such an ability, or being poor at it.

MDM operations, campaigns, or strategies do not respect national boundaries, and have come to possess a foreign-interventionist approach, along with being increasingly intertwined with geopolitics. Key examples include Russian interference in the US presidential elections in 2016 through disinformation campaigns. More recently, analyses by Microsoft conclude that AI-led MDM efforts by China may be aimed at affecting elections in India, South Korea, and the United States, although the success of such campaigns remains low. International relations scholars have viewed MDM in the context of security efforts by state actors to influence the opponent states' domestic environments.

A weak information-security environment also has downstream consequences. Health misinformation in the context of the COVID-19 pandemic may be thought to have emerged from an insecure environment societal MDM, or societal polarisation may result from certain false beliefs regarding what it means for one community to live with another.

Similarly, election-linked MDM ("election MDM") undermines what it means to be a voter in a democratic polity. Election MDM may be defined as MDM resulting from the context of election campaigns and may involve political content such as political advertisements. Political disinformation in particular is a vital strategy to mobilise the electorate. For instance, in the context of the Brexit elections, a group of researchers concluded that the Brexit result was "predictable through the social media, and public opinions about Brexit were likely to be manipulated by bots." In addressing the specific case of election MDM, one cannot understate the relevance of addressing the vulnerabilities present in the larger environment in which context-specific MDM cases operate.

In this context, this paper considers four national/supranational *institutional* responses to election MDM and to the overall information-security environment in which they operate, particularly in the context of current or nearing election periods in these regions. These are India, Finland, the European Union, and the United States. This paper also considers *social media* as the primary case for a study to analyse election MDM. This is primarily because the rise in election MDM has been noted in the same breath as the rise in social media penetration across the world. In Georgia, for instance, the impact of disinformation campaigns multiplied as the country's rate of internet penetration doubled between 2013 and 2020. The WEF's Global Risks report considers disinformation as the gravest risk to India,

considering the number of Indians online, and who have access to social media. Technologies like social media advance the volume, reach and efficacy of falsified information, with flows more difficult to track, attribute and control.

# European Union

The production and dissemination of disinformation is a growing concern for EU countries. The European Union recognises that the "exposure of citizens to large scale [d]isinformation, including misleading or outright false information, is a major challenge for Europe" and that "[Europe's] open democratic societies depend on public debates that allow well-informed citizens to express their will through free and fair political processes".

The European Commission notes that disinformation needs to be "counterbalanced" by enhanced media literacy and awareness on the part of the institutions, the media, as well as other relevant stakeholders and citizens. Attention is especially devoted to foreign entities to undermine the EU election, especially Russian disinformation and propaganda operations. It also recognises that the spread of MDM can have a range of harmful consequences, "...such as threatening [European] democracies, polarising debates, and putting the health, security and environment of EU citizens at risk. In 2023, the EU uncovered 750 disinformation campaigns and categorised foreign influence campaigns as a "security threat". The EU

recognises that disinformation impairs freedom of expression, as well as the right of citizens to hold opinions…".

Key amongst the EU's efforts to combat these campaigns has been a coordinated response from countries, institutions, online platforms, news media, and citizens. In particular, the European Democracy Action Plan outlines obligations and accountability for social media companies, the Code of Practice on Disinformation (2018), and a Strengthened Code of Practice on Disinformation (2022), codes which together bring different stakeholders to sign up for voluntary commitments to counter disinformation.

The Commission in 2018 considered self-regulation of (online) platforms for their efforts to tackle disinformation, along with an effective implementation and monitoring framework. This included a range of institutional mechanisms concerning transparency regarding the origin of information, promoting diversity and fostering the credibility of information. The Commission stressed strengthening fact-checking, collective knowledge, and monitoring capacity of disinformation, noting that fact-checkers were an "integral element in the media value chain, verifying and assessing the credibility of content based on facts and evidence", and stressed

the need for them to operate on the basis of high standards.[1] In sum, it recognised quality journalism is an essential element of a democratic society.

*Specifically* with regard to election MDM, the Commission recognises that disinformation "...now forms part of a wider array of tools used to manipulate electoral processes, such as hacking or defacing websites or gaining access to and leaking personal information about politicians". Furthermore, "encouraged…competent national authorities to identify best practices for the identification, mitigation, and management of risks to the electoral process from cyberattacks and disinformation. It especially recognises the role that education and media literacy play in regulating societies to disinformation. The 'Code of Practice on Disinformation' is a set of guidelines that flow from these broad principles.

While the Code broadly pertains to strengthening the broader information-security environment, election MDM has received substantial focus in the renewed code published in 2022. The Code contains commitments establishing structural indicators to assess online platforms that allow the EU to measure the overall impact of the Code on Disinformation. It covers other new types of MDM tools like fake accounts, bots or malicious

[1] The Commission notes the International Fact-Checking Network Code of Principles in this regard.

deep fakes. It also contains provisions for the empowerment of fact-checkers, extending fact-checking coverage across all EU Member States and languages, and ensuring that platforms will make a more consistent use of fact-checking on their services.

The Code's signatories commit to "cooperating and coordinating their work during elections, when the threat of disinformation campaigns is particularly high." This includes establishing a "rapid response system" to ensure swift and effective cooperation between platforms, civil society organisations, and fact-checkers during election periods. The institution of the Transparency Centre, which is accessible to citizens, portrays implementation of the Code's measures. Most recently, the Digital Services Act (DSA) involved more stringent commitments for online platforms.

# India

According to the Global Risks Report, India is most vulnerable to disinformation amongst the three forms of manipulation of information. A report from Microsoft's Threat Analysis Centre (MTAC) emphasises a potential involvement of "Chinese cyber and influence actors in influencing these elections through the creation and dissemination of AI-generated content via social media platforms".

In the context of election MDM, Election Commissioners of India recognised that media, especially social media, had become a key form of information dissemination, and therefore, "...new ways and means devised to affect the course of elections are on the rise". In this vein, the Election Commission of India (ECI) notes that a "two fold relationship" with the media — Media Facilitation and Media Management.

The Media Certification and Monitoring Committee (MCMC) at the District level and State level monitors media for issues with regard to political advertisements; with regard to social media, candidates and political parties are required to pre-certify political ads before release on social media websites. The Model Code of Conduct (MCC) and related instructions are

applicable to social media content by candidates and political parties. Although, any political content in the form of messages/content/photos/videos uploaded on blogs/social media platforms "will not be treated as political advertisements".

The institution of a Social Media Expert in the Committee, who shall assist the Committee in the "matter of certification of political advertisements proposed to be published on social media platforms". Specifically with regard to social media ("electronic media"), the ECI agreed upon a Voluntary Code of Ethics in 2019, applicable to all General and Assembly elections. The Code's fundamental provisions pertain to voluntary obligations on platforms to undertake voter awareness campaigns on electoral laws and other election-related instructions, the institution of a high-priority and dedicated grievance redressal channel, and is committed to facilitating transparency in paid political advertisements.

The Internet and Mobile Association of India (IAMAI) coordinates with social media and ECI during elections to monitor social media for violations etc. At the ECI (state level), Social Media Nodal officers are appointed for escalation of violation of MCC, or ECI-issued instructions; at the state commission level.


Source: Election Commission of India

The ECI has also instituted a 'Social Media Cell' to work under the overall supervision of the Social Media Officer, towards minimising the spread of fake news and disinformation campaigns and subsequent fact check/response on social media handles, voter awareness campaigns on social media platforms throughout the year, and disseminating content that is in respective state/local language. The Cell will also collaborate with social media teams of the Press Information Bureau, public broadcasters AIR and Doordarshan, State DIPR in the State/region for amplification of content. The ECI has issued standard operation procedures (SOPs) for timely action on election-MDM on social media, beginning through identifying "objectionable content". A quick response team has been instituted to counter MDM at all levels. A permanent media cell has been established to work throughout the year to inform the media of factually correct details on a real-time basis.

With regard to MDM concerned with the government (which may be non-electoral in character), the Government of India notified a "Fact Check Unit" (FCU) under the Press Information Bureau (PIB) in March 2024. Under the concerned legislation, the FCU is responsible for identifying "fake", "false" or "misleading" information regarding "any business of the central government". Legal challenges to the constitutionality of the notified legislation are, however, are ongoing.

# Finland

In the 2023 Media Literacy Index, which compares 47 European and OECD countries, Finland has been ranked at the top (since 2017) in its efforts to resist fake news through media freedom, education, and trust in people. The context in which electoral-related media-literacy institutional processes have progressed is a comprehensive effort by the Finnish government regarding the importance of media literacy. Moreover, efforts to tackle election MDM involve institutional mechanisms that are based on the larger context of specific frameworks in place to achieve democratic goals by the Finnish government.

The Ministry of Education and Culture came up with a media literacy programme for school children, defining media education as "art and cultural heritage education, the system of art education and increasingly also media education reinforce the underpinning of culture", and in 2020, added that "art, cultural heritage and media education has a more visible place in society".

The Finnish government launched the Media Literacy Policy in 2019, and works to, among other things, promote media literacy covering all types

of media and recognises that "media literacy has become an important element of civic competence that contributes…a good meaningful life". It also recognises that media literate people can protect themselves from threats like the systematic and targeted dissemination of disinformation and anti-democratic messages, hate speech and mediated sexual harassment. The primary objective is to "promote people's willingness and ability to act actively and responsibly in media culture, and thus reinforce desire future trends."

Media education was been defined as a cross-curricular theme in the upper secondary curriculum in 2004. For instance, during early childhood education and care, children are exposed to media education through curious experimentation and play, and empathise with stories and process them by means of personal expression and creativity. In elementary school, stories are examined, and analysed, and children learn how to use media safely. In higher grades, media literacy is taught through, among other things, learning how to evaluate the reliability of social media content as a source of information, and the effects that media can have on individuals.

With regard to election MDM, the Ministry of Justice, the Finnish election authority, specifically emphasises the significance of children's, adolescents' as well as adults' media literacy as a factor that aids Finland's democratic credentials. A number of actors work together to implement the

Media Education policy, like the Finnish Competition and Consumer Authority, the Prime Minister's Office, the Ministry of Justice, and the Ministry of Education and Culture. Certain aspects of Finland's Youth Policy consider media education to be an integral part of skilling programmes. In this context, long-term educational measures may be thought of as an alternative to a more context-specific and controversial content-moderation regulatory approach.

# Taking Stock: Institutional Mechanisms to Combat Election-MDM

Institutional mechanisms that hinge on content moderation are tricky in the democratic context. A heavy reliance on it sits uneasily with rights to freedom of expression and access to information, in cases where what is construed as "fake" or "misleading" does not involve water-tight definitions. In variations of this step involving content-moderation, access to the internet — i.e. access to social media websites like X (formerly Twitter) — has been curtailed to avoid MDM leading to wide public unrest (For example, Pakistan). Therefore, while content moderation and regulation are one part of the answer, a more comprehensive institutional toolkit needs to be developed to combat election MDM. Below three recommendations are presented, which are extrapolated from the responses considered above.

### *I. Medium-to-long-term media-literacy strategies; robust civil society mechanisms*

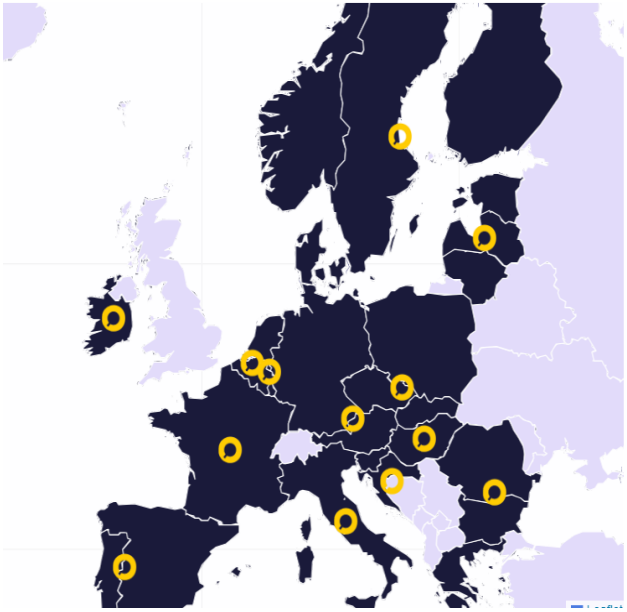
Tackling election MDM necessarily involves an approach to the information-security environment in which information manipulation poses a threat. As the case from Finland shows, a dedicated medium- and long-term approach that views the environment of the voter holistically (i.e. as a consumer of media) is key. Such an approach requires collaboration between election authorities and institutions concerned with technology, youth empowerment, and education.

In the short term, the EU example is enlightening. Robust civil society organisations, particularly fact-checking organisations, aid institutional capacity in combatting election MDM. In the European case, the European Digital Media Observatory (EDMO) is a civil-society-led, independent consortium hosted by the European University Institute in Florence, Italy, and is the largest interdisciplinary network in the world to counter disinformation. The centre is part of the European Commission's action against disinformation, and is primarily aimed at working in four areas:

1. Improving Detection
2. Coordinating Responses

3. Working with online platforms and industry
4. Raising awareness and empowering citizens to respond to disinformation online

Most importantly, the EDMO works to support public authorities "in the monitoring of the policies put in place by online platforms to limit the spread and the impact of disinformation", including fact-checking support. It works to strengthen collaboration amongst fact-checkers, media literacy experts and academic researchers to tackle online disinformation. Currently, the EDMO consists of "hubs" across all 27 EU countries as well as Norway, which work towards detecting and analysing disinformation campaigns, and organising media literacy activities at national or multinational levels.



Source: https://edmo.eu/about-us/edmo-hubs/

One of the EDMO's focus areas is the European 2024 elections, and an "EDMO Task Force on 2024 European Elections" that works to "provide useful information and tools to promote an honest European debate in the run-up to the elections". In India, SHAKTI and the Misinformation Democratic Alliance (MDA) can be thought of as robust civil society responses, although a *network* or a *hub* is lacking.

The EU example emphasises a multi-stakeholder approach to fact-checking — as well as an overarching approach to combat disinformation —

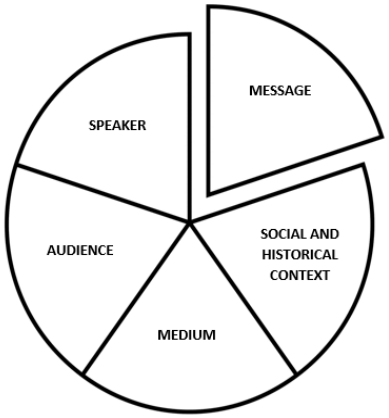
must include is essential. Institutional mechanisms are needed to make the consultative fact-checking process more inclusive and holistic. One key guiding question behind this approach is the assumption that an inclusive approach will ensure the responsibility of fact-checkers and reliability in the process. The larger idea is how we can ensure that fact-checking processes are sufficiently networked and various consultative processes are in place.

## II. *What constitutes a necessary response to MDM? Transparency regarding content that is harmful*

The ways in which MDM, particularly election MDM, constitutes public harm (i.e. its potential to cause public harm) are context-dependent. Institutions and institutional bodies are guided by context-specific knowledge of what constitutes harm with respect to, let's say, a viral X tweet. The local context for a Chief Electoral Officer in Madhya Pradesh with respect to what constitutes "objectionable" content is very different from the context in which the election officer in the Central Denmark Region of Denmark operates.

There is considerable debate about where disinformation begins, how hate speech is intertwined with disinformation, and how different authorities — national or international — define and assess it. Such an exercise is bound to be complex since each country's understanding of what constitutes "harm" or "public interest" would vary. A useful term to understand MDM that relates to public harm is "dangerous speech", defined as:

Any form of expression (speech, text, or images) that can increase the risk that its audience will condone or commit violence against members of another group.




Source: Dangerous Speech Project

The Government of India ("GoI") defines 'fake news' broadly as a "piece of information that…must be busted publicly for the larger benefit of the people of India", and is factually incorrect that is spread intentionally or unintentionally…that can deceive or manipulate the audience…". The consultative process regarding establishing public interest, in this case, involves "investigation and verification from official and authoritative sources". Recently, the social media intermediary X said that it disagreed with the Government of India's executive orders to act on specific accounts and posts, and "[maintained] that freedom of expression should extend to these posts". Moreover, the FCU's definitions of what constitutes "fake" or what concerns "business of the central government" is not defined. One crucial implication, therefore, it is unclear what procedure will adopted by the Unit in its day-to-day functioning, aside from its efforts to use technological tools and verify from concerned "Government of India [organisations]" to ensure there exist multiple layers of cross-checking.

Independence and transparency regarding these definitions are crucial, prompting us to understand how public authorities, social media companies, and citizens (in some sense, responsible for self-regulation) understand the impact of MDM. In India, institutional coordinative mechanisms that serve exactly this collaborative approach are required. A transparent and independent civil society-wide consultation is required to deeply understand

what guides "dangerous speech" in the Indian context, and importantly requires local engagement at state and district levels.

*III. Election authorities' collaborative approaches; model conduct for social media; stress on regulation of emerging and critical technologies such as AI*

Election-period rules and regulations need to accurately respond to election MDM. In the specific Indian case, the Model Code of Conduct (MCC) works as a way to institutionalise a method of regulating how election campaigning is done, and for the purposes of the paper, how the media is used for campaigning purposes

First, election regulations and guidelines must increasingly focus on social media as a critical tool used for political campaigns year-round: While India's ECI notes this — calling social media the fifth pillar of democracy (rather than simply "media") — the MCC does not robustly reflect this. An MCC revolving around political campaigning and electoral activities on social media is the need, which importantly presents robust guidelines that possess strong monitoring and accountability frameworks for how political parties use social media during election periods.

Second, ECI's efforts to curb election MDM lack a focus on the impact of emerging technologies on elections, like deepfakes and AI-generated MDM. In the United States, the Federal Communications Commission

(FCC) announced that calls made with voices generated with the help of AI — "robocalls" — targeted consumers illegally. The decision followed a political disinformation campaign in New Hampshire's presidential primary elections that involved robocalls impersonating US President Biden asking voters not to vote.

Deepfakes have been used to influence politics and elections in the United Kingdom, Bangladesh, Nigeria, Sudan and Slovakia. In the Indian context, AI-generated deepfakes are considered key to social media disinformation campaigns by political parties, and have evoked concern from the government. The Union government has issued advisories regarding the impact of these technologies (rather than taking a regulatory approach), specifically noting growing concerns around deepfakes.

One way to combat election-related, AI-linked MDM is developing institutional manpower and capacity to detect deepfakes, along with robust standards around how social media intermediaries must tackle deepfakes. For instance, the ECI's efforts in the context of the 2024 General Elections lack any recognition of the use of AI in election-related MDM. Along with a social media expert, for instance, the ECI should include AI experts as part of its media cells who are skilled in identifying deepfakes. In the US, elections officials use and deploy AI tools for "algorithmic decision-making" in

election contexts, sparking concern regarding the responsible and safe use of these tools by state election officials.

In this context, the United States' Cybersecurity and Infrastructure Security Agency (CISA) offers training to election stakeholders on the usage of AI. This requires greater collaboration between election authorities and external stakeholders like civil society organisations and experts to develop an approach to AI. This has been the case in Minnesota where the election office worked with local and federal partners to monitor and respond to inaccuracies that may result in conspiracy theories, in the context of AI use in elections.

# Conclusion

Weak information-security environments have led to the proliferation of MDM, particularly election MDM, which has raised concerns about election integrity and democracy. The spread of social media has also created significant vulnerabilities in the way information is disseminated across networks.

Four institutional responses to MDM, particularly election MDM, were considered, largely focusing on a regulatory approach emphasising strong accountability and monitoring frameworks (EU), media-literacy initiatives (Finland), election-related governance structure India), and response to AI use in elections (US). Extrapolating from these responses, the paper considers three institutional mechanisms that may be used to combat election MDM. The first focuses on robust civil society mechanisms as well as medium-to-long-term media literacy strategies. In this vein, the EU's EDMO and its role have been emphasised.

The second stresses the *need* for mechanisms which aid our understanding of what constitutes "harm" or "dangerousness" when it comes to speech, particularly online speech. The third discusses the regulation of

election MDM by election authorities through building an ideal code of conduct, and is placed in the Indian context.

# Technology, Elections and Political Decision-Making in the Information Age

**Satya S. Sahu and Sachin Kalbag**

## Introduction

From social media platforms shaping public discourse to artificial intelligence (AI) tools generating targeted propaganda, technology's impact on elections and political decision-making is profound and multifaceted. Technology, in its various forms, has become deeply intertwined with the political process in the information age. This research paper examines two key dimensions of this complex relationship — **first**, how various sets of technologies are being leveraged as political tools by political parties in the context of elections; and **second**, how political parties interact with and influence governments to shape the technological landscape to their advantage.

The scope of analysis covers a range of digital technologies that have emerged as significant forces in the political arena over the past decade. These include social media and online platforms, data analytics, artificial intelligence systems capable of generating deepfakes and micro-targeted messaging, and examples like Geographic Information Systems (GIS) technology used to organise campaigns and mobilise voters.

The authors' goal in analysing the first dimension is to briefly showcase ways in which political actors can harness the power of technology to achieve goals ranging from voter persuasion, turnout, and polarisation to the spread of misinformation and conspiracy theories. At the same time, technology can also empower voters to make informed decisions, as well as increase engagement and participation in the electoral process.

The second dimension covers the interplay between political parties and governments in shaping the technological ecosystem. This includes analysing efforts by parties to influence laws and regulations around issues like data privacy, content moderation on social media, and anti-trust actions against big tech companies. The paper studies how political capture of the regulatory agenda in technology policy can skew the playing field and impact electoral competitiveness and institutions.

The paper has certain limitations. The rapid pace of technological change means that the landscape is constantly evolving, making it difficult to capture the most cutting-edge developments comprehensively. However, in an effort to address this, the authors attempt to create a framework that maps how different sets of technologies may be used for specific political/election processes from now into the future.

# Politics and Elections in the Information Age

## Characteristics of the Information Age

Before we begin to chart the different ways in which technology and information will likely transform elections and political processes, strategies, and decision-making, we must understand the contemporary context where we are already seeing such a transformation underway. The information age, emerging at the turn of the century, continues to shape our world today and is accelerating at a breakneck pace. Broadly speaking, the defining feature of this period is the rapid development and widespread adoption of digital technologies, such as computers, the internet, mobile devices, and automation, which have revolutionised the way we communicate, work, learn, and interact with one another. In other words, these technologies have

changed and will continue to change the manner in which information is created, stored, shared, and consumed.

We can break these defining characteristics down further. **First** and most obviously, the information age is marked by the digitisation of information and the increasing importance of data as a resource and commodity. The knowledge economy and information-based industries that emerge from rapid advancement and innovation in computing, AI, telecommunications, etc., leverage data to create economic value.

**Second**, the aforementioned technological advancements drive the expansion of digital networks that transcend geographical boundaries, allowing for instantaneous information exchange, the rapid spread of ideas, and the formation of global communities. The positive implications of such open hyperconnectivity, such as the democratisation of knowledge, are tempered by the negatives, such as the viral dissemination of misinformation.

**Third**, such technological advancements arose and were adopted within a relatively short span of time, ensuring that their impact was disruptive for traditional economic, social, and political structures. Long-

standing business models, social interactions, and power dynamics have to adapt to a digitally mediated reality or perish. While again, this creates new opportunities, it also poses challenges, such as the concentration of power in a few dominant technology platforms.

**Finally**, and perhaps most importantly, the information age poses pressing and hitherto unaddressed concerns around cognitive overload and autonomy, degrees of privacy and security, and the spread of misinformation that can manipulate public opinion *en masse* and undermine trust in institutions.

# Politics and Elections

In the realm of politics, the information age has transformed how campaigns are run, how citizens engage in the political process, and how information shapes public opinion and electoral outcomes. While new technologies can create new opportunities for political mobilisation, grassroots organising, and facilitate direct communication between leaders and constituents, they can also open new avenues for voter manipulation, micro-targeting, and foreign interference that can distort democratic processes. We list a few examples of both below.

Political campaigns are increasingly relying on digital tools for organising, fundraising, and voter outreach. Social media platforms, targeted online advertising, etc., are indispensable tools for candidates now. The 2008 Obama presidential campaign pioneered harnessing the power of these tools, and since then, the use of data analytics to micro-target specific voter segments has only grown more sophisticated.

Political communication has also adapted astonishingly to the speed and reach of online information flows. 24/7 news cycles and the viral nature of social media accelerate the pace at which narratives spread, evolve, and die. Political actors and institutions must now contend with barrages of real-time reactions, fact-checks, and counter-narratives. While this may make it harder to control messaging, it has also ensured that such actors constantly cultivate rapid response capabilities. Moreover, the fragmentation of the monopoly of legacy media and the concurrent rise of algorithmically curated content feeds have contributed to the formation of ideological echo chambers and filter bubbles. Combined with the rapid news cycle, people increasingly consume news and political content aligned for maximum engagement (i.e. content that primarily aligns with their existing beliefs). This makes it harder to establish a shared understanding of facts and bridge partisan divides, leading to extreme political polarisation and subsequently, undermining efforts for compromise and consensus-building.

The low cost and global reach of digital platforms make it easier for both domestic and foreign actors to manipulate public opinion with an explosion of political misinformation and disinformation. As entire strategies are crafted around the amplification of mis/dis-information by bots and fake accounts, urgent questions form about how to safeguard the integrity of elections and counter the effects of such information on democratic discourse.

At the same time, technological progress continuously expands opportunities for citizens to participate directly in the political process, beyond even just voting. Online activism, crowdfunding, and digital petitions have given rise to new forms of grassroots mobilisation and interest group advocacy. However, concerns abound regarding whether these movements can translate into sustained offline engagement (especially combined with the aforementioned rapid news cycles) and whether special interests can co-opt them behind the scenes.

# The Future

Looking ahead, the continued evolution of digital technologies, such as AI, Augmented/Virtual Reality (AR/VR) etc., will likely exacerbate and complicate these trends.

One major development will be the increasing sophistication and pervasiveness of AI and machine learning in political campaigns. AI-driven technologies and tools will enable automated generation and micro-targeting of political content including personalised ads, social media posts, and synthetic media like deepfakes. This could make it even harder for voters to distinguish between authentic and manipulated information (especially as they are constantly under an information overload as they navigate social media etc). This will further erode the shared basis for reasoned political deliberation.

As the deployment of AI becomes more commonplace for voter analysis and engagement metrics, pressing questions about data privacy, consent and algorithmic bias will become more prominent. Campaigns will hoover up more and more granular data about voter behaviour, preferences, and psychological profiles on a scale that continues to grow exponentially. The more data collected, the more the risk of its misuse and exploitation.

This will mean a concurrent call for ensuring transparency and accountability in algorithms and AI tools used in campaigns, with perhaps techno-legal solutions.

A trend that is already well underway, will be the blurring of boundaries between domestic and foreign election interference, as state and non-state actors both exploit the global reach and anonymity provided by new tools of information operations (IO), such as bots, trolls, leaks etc. The tactics involved will become more sophisticated and harder to detect.

As more political activity moves online, the role of tech platforms as *de facto* gatekeepers and arbiters of political speech has come under intense and growing scrutiny. Debates over content moderation, algorithmic curation, and political advertising will intensify, as policymakers grapple with how to balance free expression with the need to combat misinformation and extremism. Traditional conceptions of the relationship between private corporations and government will have to be revamped and re-examined. The European Union's Digital Services Act is an example of such legislation, placing obligations on platforms to mitigate the risks of disinformation or election manipulation. We suspect more instances of legislation like this will emerge in other jurisdictions.

The future will also see more proliferative use of technologies to enhance citizen participation and deliberation beyond elections. Online fora, virtual town halls, and budgeting platforms will enable more direct inputs for political manifestos, and policymaking. However, ensuring that these tools are inclusive, secure, and resistant to manipulation or capture will continue to be an enduring challenge.

Finally, democratic and electoral institutions will need to adapt to the realities of the information age, even as they attempt to preserve the core value of the rule of law. Institutions will recognise that this adaptation will not happen without a sustained effort to build both digital literacy, and "critical thinking skills" (for lack of a better word) among citizens, so that they can navigate the complexities of the burgeoning information ecosystem. This will also likely require a fundamental reconception of public discourse and accountability.

The choices made to tackle these challenges and opportunities today will shape the trajectory of politics and elections for decades to come, and will ultimately determine whether the information age strengthens or erodes the resilience of democratic society.

# I. A Framework for Understanding Technological Use-Cases by Political Parties

How different technologies can affect political decision-making and elections in the future is an exercise in speculation. At the same time, if we map technological use cases in politics and elections vis-a-vis broad sets of technologies, it would help reliably assess the impact of a future technology as well. These use cases are contemporary and contextual, and provide us a window into the decision-making process, if not the actual use of future technology.

### Means Vs. Ends: Political Decision-making in the Electoral Process

Political decision-making by political parties within the context of elections can be broadly divided into four categories:

a. **Information Operations (Propaganda)**: Information Operations (IO) is one of the most prominent ways in which technology is being leveraged by political parties. Put simply, it is the dissemination of information to influence public opinion and shape political narratives. Social media platforms in particular have become a key battleground for shaping public opinion and narratives. Political parties and campaigns can use social media to directly reach voters, share their messages and policy positions, and mobilise their

supporters. At the same time, social media is also increasingly being weaponised to spread disinformation, conspiracy theories, and hyper-partisan content. In the 2016 US presidential election, a sweeping and systematic social media disinformation campaign undermined support for Hillary Clinton and helped elect Donald Trump. More recently in India's 2019 general elections, political parties like the BJP and the Congress leveraged text messaging services such as Whatsapp to generate electoral propaganda on a massive scale. Whatsapp's centrality to the Indian social media and messaging ecosystem means that it has a massive electoral impact given its ~500 million strong user base here. Research has shown that information floating on public Whatsapp groups have both significant amounts of "junk news", and communally polarising messages, designed to achieve virality and contribute to disinformation. Parties are also increasingly using AI to automate the creation and distribution of propaganda. As AI-powered deepfake videos, hyper-realistic fake images and Large Language Models (LLMs) continue to advance and become more accessible, the potential for AI-driven propaganda to distort elections is a growing concern.

b. **Canvassing (Identification and Persuasion)**: Political parties also leverage various technologies to identify, target, and interact with voters for canvassing. Extensive voter databases, digital advertising platforms, and smartphone apps allow campaigns to microtarget customised messages to specific voters with unprecedented precision.

In the US, both Democrats and Republicans maintain detailed voter files from public sources, as well as data points bought from commercial vendors. This data is used to model individual voters and predict which candidates they are likely to support. This voter data can be used to conduct targeted canvassing, both online and offline. Campaigns may show certain messages only to young female voters or highlight a candidate's military service to certain veteran households. In India, too, several political parties have used Big Data to understand granular details of their voter base and targeting outreach in their language. This is especially true of the 2024 general election. For example, Prime Minister Narendra Modi's speech at the Kashi Tamil Sangamam in December 2023 was delivered in Varanasi in Uttar Pradesh for Tamil-speaking visitors. Prime Minister Modi spoke in Hindi, but was simultaneously translated into Tamil, thanks to AI-generated dubbing.

c. **Analytics (strategy-making):** Big data analytics and machine learning leverage large volumes of data from polls, donor databases, social media and other market sources. This informs campaign strategy and decision-making constantly as political parties aim to gain a competitive edge. Leading campaigns in the US presidential election cultivated large in-house data science and analytics teams which conducted advanced modelling to forecast election results, optimise

resource allocation, and run simulations to stress-test strategy. Social media analytics allow campaigns to measure the reach and impact of their messaging, identify greater opportunities for persuasion, and track how voters are discussing candidates and issues in real-time, sometimes being trusted as a better measure of sentiment over exit-polling. In India, the BJP has invested heavily in building data analytics capabilities. The party uses tools like the NaMo app to collect data on millions of supporters. When this data is layered over other data points sourced from government data sets, surveys, and social media data, it provides the BJP with extremely granular insights on the electorate to inform their strategy.

d. **Voter Empowerment**: While much of the focus is on how parties are using technology to influence voters, digital tools are also creating new avenues for voters to engage with campaigns and the political process. Innovations like secure online voting systems or blockchain-based voting platforms are already under consideration. Voter-driven political engagement and activism on social media have been around for quite some time now. Along with other digital organising platforms, they allow voters to more easily find and connect with like-minded citizens, discuss issues they care about, and coordinate their political activities. Google, Twitter, and Snapchat designed and offered tools to educate voters, and increase awareness; options that became

> even more critical as Covid-19 disrupted many in-person voter engagement efforts. During the 2020 US elections, Democrat campaigns innovated new ways to mobilise supporters online within the constraints of the pandemic, such as virtual rallies etc. However, major social media platforms are designed to maximise engagement and revenue, not to foster healthy political discourse or provide factual information. The fact remains that political parties and campaigns still have far greater financial and technological resources to leverage data and digital platforms to influence voters.

These use cases can be mapped against any broad set of technologies; in this paper, we use three examples: AI, Social Media, and miscellaneous technologies like GIS or Blockchain, which can help with accountability, empower voters, and inform political strategy.

AI (incorporating generative AI, machine learning and big data analytics) can be employed across all four use-cases, with varying implications. In Information Operations, AI can generate targeted propaganda and deepfakes, thereby amplifying the spread of disinformation and impacting electoral integrity. For canvassing, AI can help identify and persuade voters as it informs microtargeting efforts, effectively manipulating public opinion. In

analytics, AI can process vast amounts of data to inform campaign strategies, but the opacity of these systems raises questions about ethical sourcing of data, and transparency. Finally, generative AI can empower voters by democratising access to information and lowering language barriers. Civil Society can use the entire gamut of AI-based technologies to educate voters and encourage political participation.

Social media platforms, with their opaque algorithms, often based on exploiting dark patterns, play a significant role in Information Operations by amplifying certain messages and targeting specific demographics. They can also be used for canvassing, as political parties identify and engage potential supporters. Social media analytics can provide valuable insights for campaign strategy-making amidst similar concerns about privacy and manipulation.

Finally, different technologies like GIS, can be leveraged across all four use-cases as well. For instance, GIS can enhance accountability and voter education by providing access to new and relevant information about electoral processes, real-time election data, polling locations/district demographics etc. At the same time, political parties can also use GIS for targeted campaigning and resource allocation (such as finding the best places to host events or put up advertising etc).

# Mapping The Framework

| Use Case → ↓ Tech | Information Operations (Propaganda) | Canvassing (Identification and Persuasion) | Analytics (Strategy-making) | Voter Empowerment |
|---|---|---|---|---|
| AI (Generative AI, Machine Learning, and Data Analytics) | Generate persuasive, targeted propaganda, including deepfakes and synthetic media, to manipulate public opinion | Leverage machine learning algorithms to identify likely supporters based on demographic, psychographic, and | Process and analyse vast amounts of structured and unstructured data from multiple sources, including social media, surveys, and public | Provide voters with personalised information and resources, such as voting guides, candidate comparisons, and policy explainers, based on their individual needs and preferences. |

| | | | | |
|---|---|---|---|---|
| | and sow confusion.<br><br>Automate the creation and dissemination of disinformation at scale, making it harder to detect and counter.<br><br>Analyse user data to identify vulnerabilities and craft personalised narratives that | behavioural data.<br><br>Use generative AI to create personalised messaging and content that resonates with voters, increasing the outreach effectiveness.<br><br>Optimise resource allocation and canvassing strategies based on real-time | records, to gain insights into voter preferences and behaviour.<br><br>Develop predictive models to forecast election outcomes, identify key swing voters, and simulate the impact of campaign strategies.<br>Monitor and adapt to changes in public | Use generative AI to create accessible and engaging content that helps voters understand complex issues and make informed decisions<br><br>Analyse voter data to identify, target individuals at risk of being deceived or demobilised by disinfo campaigns |

| | | | | |
|---|---|---|---|---|
| | exploit cognitive biases | data analysis and predictive modelling. | sentiment and opinion in real-time, enabling more agile and responsive campaign decision-making | |
| Social Media (dark patterns and algorithms) | Amplify messages and narratives through coordinated campaigns, bot networks, and targeted advertising, leveraging the viral nature of social media to | Leverage social media data, including user profiles, interests, and behaviours, to identify potential supporters and build targeted outreach lists. | Monitor social media conversations and sentiment to gauge public opinion, track the spread of information, and identify emerging narratives and issues. | Provide voters with accurate and reliable information through official and verified social media channels, countering disinformation and promoting transparency. |

| | | | | |
|---|---|---|---|---|
| | reach a wide audience.<br><br>Exploit algorithmic biases and filter bubbles to target specific demographics and communities with tailored disinformation, exacerbating social divisions and undermining trust in institutions. | Use social media advertising platforms to deliver personalised messages and calls to action, optimising for engagement and conversion rates.<br><br>Encourage supporters to share campaign content and participate in online activism, amplifying the reach and | Analyse social media metrics, such as engagement rates and follower growth, to measure the effectiveness of campaign messaging and adjust strategies accordingly.<br><br>Use social media data to build detailed voter profiles and segment | Encourage voter participation and engagement through social media campaigns, and online voter registration initiatives.<br><br>Use social media platforms to facilitate dialogue and feedback between voters and candidates, increasing accountability and trust in the electoral process. |

| | | | | |
|---|---|---|---|---|
| | Use dark patterns, such as false urgency and social proof, to manipulate users' emotions and behaviours, increasing the effectiveness of propaganda efforts. | impact of canvassing efforts. | audiences based on their preferences, behaviours, and influenceability. | |
| Miscellaneous Technologies (GIS) | Develop fact-checking tools and platforms that leverage GIS data to verify the accuracy of claims and | Use GIS data to optimise canvassing routes and resource allocation, ensuring that outreach efforts | Leverage GIS data to verify voter registration information, such as addresses and district assignments, | Provide voters with accessible, interactive maps and tools that display polling locations, ballot drop boxes, and other essential |

| | | | | |
|---|---|---|---|---|
| | counter misinformation. | are targeted and efficient.<br><br>Integrate GIS data with voter files and other databases to create comprehensive voter profiles and identify key geographic areas for canvassing.<br><br>Develop interactive maps and dashboards that allow campaign | reducing the risk of errors and irregularities.<br><br>Use GIS analysis to identify potential barriers to voting, such as long distances to polling locations or inadequate transportation options, and develop targeted interventions. | voting information.<br><br>Use GIS data to create personalised voting guides and resources, such as directions to polling places and estimated wait times, empowering voters to participate.<br><br>Develop GIS-powered platforms that allow voters to |

| | | | | |
|---|---|---|---|---|
| | | staff to track canvassing progress and adapt strategies in real-time. | Integrate GIS data with other sources, such as census records and voting histories, to create detailed models of voter turnout and preferences. | report issues or irregularities, such as long lines or voter intimidation, increasing transparency and accountability in the electoral process. |
| Miscellaneous Technologies (Blockchain) | Develop decentralised fact-checking and content moderation platforms that leverage blockchain's immutability | Use blockchain-based identity solutions to securely store and manage voter data, enabling more efficient and | Implement blockchain-based systems for securely storing and sharing voter data across different databases and | Provide voters with blockchain-based identity solutions that enable secure, convenient access to voting information and resources while |

| | | | | |
|---|---|---|---|---|
| | and transparency to counter disinformation and promote trust in information sources.<br><br>Use blockchain-based identity solutions to verify the authenticity of user accounts and prevent the spread of propaganda through fake | targeted canvassing efforts while protecting privacy.<br><br>Develop blockchain-based platforms for secure, transparent campaign finance management, ensuring that funds are used appropriately and in compliance with regulations. | platforms, reducing the risk of errors, inconsistencies, and data breaches.<br><br>Develop blockchain-based analytics platforms that enable secure, privacy-preserving data sharing and analysis among multiple stakeholders, such as campaigns, researchers, and | protecting against fraud and identity theft.<br><br>Use blockchain technology to create tamper-proof, auditable records of voter registration, ballot casting, and vote counting, increasing trust and confidence in the electoral process.<br><br>Develop blockchain-based platforms for |

| | | | | |
|---|---|---|---|---|
| | profiles and bot networks.<br><br>Implement blockchain-based reputation systems that incentivise the creation and sharing of accurate, reliable information and penalise the spread of disinformation. | Leverage blockchain's decentralised nature to facilitate secure, tamper-proof communication and coordination among campaign staff and volunteers. | election officials. | secure, transparent crowdfunding and campaign finance, enabling voters to support candidates and causes they believe in while ensuring accountability and compliance with regulations |

# II. How Ruling Political Parties Entrench and Consolidate Power Using Technology

## Controlling Access to Information

**By labelling certain sources of data/ information as approved/correct/genuine or by controlling access to alternative and independent sources of data and information:** On March 20, 2024, the Government of India notified the Press Information Bureau's (PIB) Fact Check Unit under the IT Rules, 2021. The Fact Check Unit (FCU) under PIB was established in November 2019 with a stated objective of acting as a deterrent to creators and disseminators of fake news and misinformation. According to the PIB, "It also provides people with an easy avenue to report suspicious and questionable information pertaining to the Government of India.The FCU is mandated to counter misinformation on Government policies, initiatives and schemes either suo motu or under a reference via complaints. The FCU actively monitors, detects, and counters disinformation

campaigns, ensuring that false information about the Government is promptly exposed and corrected." However, in reality, it often becomes a weapon in the hands of the ruling party.

**In March 2020,** just a few days before Covid-19 was declared a pandemic, two Kerala-based news channels — MediaOne and Asianet — were suspended by the Ministry of Information and Broadcasting for its coverage of the communal riots in North-east Delhi.

**In January 2024,** the Central government suspended the license of popular Marathi news channel Lokshahi for the second time in five months for what it called blatant and continuous violations of policy guidelines. Owners and editors pointed out that they were targeted because the channel's coverage is anti-BJP. In September 2023, the channel was suspended by the Ministry of Information and Broadcasting for airing a sting operation on BJP leader Kirit Somaiya where he was asking a woman for sexual favours.

**In April 2024,** the Central government asked YouTube, the world's largest video platform, to take down National Dastak, an independent Hindi-language news channel. National Dastak describes itself as a voice of Dalits,

Adivasis, farmers, women and oppressed people. It said in a statement that "the Union government is afraid of a news portal for the Dalits while lakhs of newspapers and television news channels are allowed to run. The Centre or YouTube has provided no reason for the action against the news portal." In an email addressed to National Dastak, YouTube said that it received a notice from the Ministry of Information and Broadcasting to take down the channel in compliance with Rule 15 (2) of the Information Technology Rules, 2021 with Section 69A of the Information Technology Act 2000.

**In December 2022,** the Central government announced that it had blocked 84 online news channels and 23 news websites for the year for violation of the programming code and advertising code. In 2021, that number was 22 news channels.

## III. Weakening Accountability Mechanisms

According to data provided by the Government of India, there was an 83% increase in rejection of Right to Information (RTI) applications in the 2020-21 on the grounds of "national security" by the Central government ministries during 2020-21 even though the overall rejection rate went down

by 2.95%. The role of the media, often the most effective accountability mechanism in a democracy, is called into question in India as it has not held the government accountable for its policy making, or the ruling party for allegedly polarising society. In fact, research suggests that the government led by Prime Minister Modi has systematically targeted journalists for simply doing their jobs.

# Building Narratives

In India, the BJP pioneered the use of social broadcast technology such as WhatsApp, Twitter, and Facebook to build narratives around its ideology, its government schemes, and its government's achievements. It does this by using a technology team — popularly called 'IT Cell' — which is trained in developing stories around the party's outreach objectives. Other political parties seem to have caught up with the BJP only in the last few years.

## Operative Technologies That Can Be Used

Since June 2020, India has banned hundreds of Chinese apps, citing national security concerns. The most talked-about ban was that of TikTok, a short video platform that has hundreds of millions of users worldwide. However, these bans were imposed with very little transparency and little or no public consultation. They were followed up by state orders—which went largely unquestioned—for internet service providers (ISPs) in India to filter out Indians' access to TikTok servers. These punitive measures have been often used to pressure homegrown technology or media companies from

creating an alternative narrative. One such example is the October 2023 arrest of Newsclick founder and editor Prabir Purkayastha in New Delhi for alleged Chinese links. Newsclick has been a strident anti-government website, holding the BJP and Prime Minister Narendra Modi accountable.

# Mapping The Framework

| Creating Information asymmetry by labelling certain sources of data/ information as approved/correct /genuine | Creating Information Asymmetry (controlling access to alternative and independent sources of data and information) | Weakening Accountability Mechanisms (Media, NGOs, Civil Society) | Narrative Building entrenching ruling party's philosophy and religious sensibility/ appropriation of figures |
|---|---|---|---|
| By forcing only one narrative using the PIB Fact Check Unit, the government has succeeded in throttling alternative | According to data provided by the Government of India, there was an 83% increase in rejection of | By threatening media channels and newspapers with financial | Using sophisticated call centre services and the so-called IT Cells, political parties have reached out to millions of voters before the first phase of the current parliamentary elections. |

| | | | |
|---|---|---|---|
| narratives or even analysis of numbers that it feels is in variance with the government narratives. Since March 2020, the Central government has suspended or banned several TV news channels for ostensibly violating programming or advertising codes, but these channels have alleged that it is mostly due to | Right to Information (RTI) applications in the 2020-21 on the grounds of "national security" by the Central government ministries during 2020-21 even though the overall rejection rate went down by 2.95%, revealed an analysis of the RTI | consequences, the government has pressured an already-stressed industry into toeing its line. Government advertising in newspapers and TV channels ranges from 20% to 60% of its ad revenue. | Political consultancy firms including Varahe Analytics and Association of Billion Minds have used thousands of employees to collect data, conduct surveys and give recommendations to the BJP leadership, sources said. The firms have provided information on governance feedback, ground intelligence and data-backed insights, the sources said. Jarvis Technology & Strategy Consulting is also providing technological support, conducting |

| | | | |
|---|---|---|---|
| their independent coverage.<br><br>Sources: 1. https://m.thewire.in/article/media/national-dastak-youtube-channel-block-press-freedom<br>2. https://www.newslaundry.com/2024/04/09/govt-asks-youtube-to-remove-journalist-turned-politicians-news-channel-cites-it-rules | applications by Hindustan Times. The government has banned scores of YouTube channels where "alternative" sources of information and analysis can be accessed.<br><br>Source: https://www.hindustantimes.com/india-news/83- | By threatening to withdraw advertising, as it happened in the case of The Times of India, The Telegraph and The Hindu, the government forces media outlets to stop questioning policies. | data mapping and managing call centres for the BJP with its 300 full-time workers and thousands of paid associates. Through 360 call centres, Jarvis is reaching out to as many as six million BJP workers every day, a Jarvis official said.<br><br>Source: https://www.thenationalnews.com/news/asia/2024/04/19/india-election-2024-bjp-congress-strategy/ |

| | | | |
|---|---|---|---|
| 3. https://scroll.in/latest/1061906/centre-suspends-licence-of-news-channel-lokshahi-marathi-for-second-time-in-five-months | increase-in-rejection-of-rti-applications-on-national-security-grounds-data-101646469748249.html | Source: https://thewire.in/media/modi-govt-freezes-ads-times-of-india-hindu-the-telegraph | |

# Conclusion

By analysing both how political parties leverage technologies as electoral tools and how they influence the broader electoral landscape by capturing vital aspects of certain technologies through policy, the authors have attempted to paint a comprehensive picture of the challenges and opportunities vis-a-vis politics and elections in the information age.

The paper outlined key domains where technology is being deployed for political ends: information operations and propaganda, canvassing, analytics and strategy formulation, and voter empowerment. In each area, the growing sophistication of AI, machine learning, and data analytics is enabling campaigns to target, manipulate, and mobilise voters with unprecedented precision and scale.

Concurrently, social media platforms have become battlegrounds, with coordinated disinformation campaigns, algorithmic filter bubbles, and viral messaging all contributing to a more polarised electorate.

Looking ahead however, the continued proliferation of Generative AI poses perhaps the greatest risks and uncertainties. The massive scale at which persuasive deepfakes, micro-targeted propaganda, and personalised voter

outreach can be deployed, especially when released close to election dates, means that it will be more difficult to cultivate a shared basis of facts/truth for the electorate at large. The viral nature of social media, and the constant obeisance to a volatile news cycle help rapidly spread such synthetic content, making containment difficult. Even the mere existence of deepfakes lead to a "*liar's dividend*" where real information will be dismissed as fake. Parties must both convince the electorate of the genuineness of their content and messaging, as well as raise public awareness regarding the presence of manipulated content; something they did not have to contend with prior to this stage of the Information age. The automation of content moderation, and fact-checking with counter-AI tools will become an increasingly vital countermeasure.

Another key concern is the growing power of tech platforms to shape political information ecosystems. As more campaigns and voters move online, the decisions these companies make regarding content algorithms, ad targeting, and user privacy will have far-reaching electoral consequences.

A by-product of the influence of such platforms would be the increasing influence of micro-influencers as well; individuals who do not belong to political parties, nor journalists but who maintain a significant online presence and a sizeable engaged audience. Political parties can either

leverage these individuals to deliver messages to these audiences or be at the receiving end of such a mobilised population.

The combination of AI-generated misinformation, voter profiling, and threats of election meddling could undermine public faith in the integrity of elections. If voters believe the information ecosystem is polluted with unreliable information or that the election process itself is compromised, it could delegitimise electoral results and weaken trust in democratic institutions.

Importantly, however, while it may seem like technology is operating as a top-down tool of political control wielded by political parties, it can also be a bottom-up means of civic empowerment. Technology can expand access to reliable information, facilitate collective action, and hold campaigns and electoral institutions more accountable.

However, sustaining public trust will also require a concomitant and concerted effort towards digital literacy, as cognitive overload is exacerbated in the information age.


The Takshashila Institution is an independent centre for research and education in public policy. It is a non-partisan, non-profit organisation that advocates the values of freedom, openness, tolerance, pluralism, and responsible citizenship. It seeks to transform India through better public policies, bridging the governance gap by developing better public servants, civil society leaders, professionals, and informed citizens.

Takshashila creates change by connecting good people, to good ideas and good networks. It produces independent policy research in a number of areas of governance, it grooms civic leaders through its online education programmes and engages in public discourse through its publications and digital media.