ABSTRACT

In the current moment of democratic upheaval, the role of technology has been gaining increasing space in the democratic debate due to its role both in facilitating political debates, as well as how users’ data is gathered and used. This article aims to discuss the relationship between democracy and the “algorithmic turn” – which the authors define as the “central and strategic role of data processing and automated reasoning in electoral processes, governance and decision making.” In doing so the authors help us understand how this phenomenon is influencing society – both positively and negatively – and what are the practical implications we see as a result.

KEYWORDS
Algorithms | Democracy | Elections | Governance
Democracy is at a turning point. On the one side, refreshing experiments in decentralisation and the horizontalisation of political processes are reinventing the boundaries of democracy, whether it be the rise of youth in formal politics in India and Mexico,1 the reclamation of community self-governance in urban spaces such as in the case of the networked Spanish municipalities,2 or the rise of a new DIY (Do it Yourself) citizen ethos.3 On the other, a range of developments – unanticipated electoral mandates that have stunned the pundits such as the US presidential election of 2016; an expanding trust deficit between state and citizen in many parts of the world4 and reduced faith in institutions of democracy;5 the quest for extra-institutional possibilities of leadership outside traditional venues of action such as government, unions, political parties etc;6 the polarisation of the public sphere, and a disconcerting collusion between the techno-capitalist class and the technocratic informational state – point to new challenges for democracy.7

With the invisible hand of technology increasingly revealing itself, citizenship itself is at a crossroads. Manipulated masterfully by data-driven tactics, citizens find themselves increasingly slotted into the respective sides of an ever growing and unforgiving ideology divide. However, with the ability to mobilise 140 characters and a handy hashtag, they have also managed to appropriate the digital landscape as a decisive frontier for all shades of civic engagement. From the #FeesMustFall movement student uprisings in South Africa8 to the protests against sexual violence against women and girls in India9 the online world seems to have secured its place as the stage for civic-public action.

This essay explores the role of the algorithmic turn – what we define here as the central and strategic role data processing and automated reasoning – basically, deployment of digital intelligence tactics – in electoral processes, governance and decision making – in relation to the democratic transition underway. We first discuss the ways in which digital intelligence is influencing and dictating voter behaviors and outcomes. Second, we look at the increasing role of data and algorithms in governance and policy decision processes and the implications for citizen rights. Lastly, we bring to fore some questions on the governance of such technological integration in democratic processes.10

1 • Your vote, their tech! How Big Data and big tech are making and unmaking elections

From the somewhat simplistic studies of the early days of mass media technologies such as the role of radio, film and newspapers in war time11 to more recent work that has looked at the role of cell phones and Big Data12 in elections,13 technology’s ability to diffuse key messages and propaganda by vested interests has been long acknowledged.

However, the tools and tactics of public sphere manipulation we are witnessing today are unprecedented. The unethical use of Big Data and machine learning14 to “game” the public sphere in pernicious ways marks a new point of departure. For example, through the intense
level of surveillance of voters afforded through digital tools, Artificial Intelligence (AI) allows political influence to move from public campaigns to private sentiment,15 a shift that repositions electoral politics from a spectacle that is overt to a script that is covert.

Also, as the Internet has grown, so has misinformation. It is often claimed that we live in times of “post-truth”. What this means is that as the virality, speed and reach of digital information increases, a mind-boggling multiplicity of narratives emerge that displace singular and authoritative grand narratives. The fact that we can choose which communities we want to be connected to means that the received wisdom of societies – the common knowledge and norms shared across communities – break down.16 In this flux, social and political sentiment of individuals and communities becomes vulnerable to manipulation and gaming.

In March 2018, as this piece was being written, the Guardian published the explosive news about how Cambridge Analytica, a once obscure data analytics firm, had – through harvesting Facebook users’ data - engineered victories for the Brexit Leave campaign in the UK and the Donald Trump campaign in the United States’ presidential elections.17 The exposé reveals not merely the large scale of manipulation of users that the techno-paradigm makes possible, but the real implications of behavioural and psychographic profiling and targeting of voters on actual electoral outcomes. The firm’s unscrupulous tactics included scraping (a form of automated data collection) and exploiting user data from Facebook without informed consent and offering monetary incentives for participating in quizzes that were cleverly disguised psychological probes.18 Further, this data was used to engage in polarized messaging and fake news dissemination.

Twitter assumed centre stage in the Mexican political theater in 2012. The failure of mainstream media to report on drug violence owing to threats from cartels had meant that Mexican citizens were already dependent on Twitter for news and updates. Campaigners for the parties in the general election, capitalised on this, spamming the network with thousands of bots19 that worked round the clock to promote particular new topics and make the trending topics list aligned with the interests of the campaigners, flooding the space with pointless “flame wars”20 that left no scope for deep engagement.21 What we see is that the technological structures of the day built into the media platforms widely used and abused in everyday politics directly have a bearing on how political processes and outcomes are shaped.

The 2017 French presidential elections showed just how extensive the use of bots can be. In May 2017, the Oxford Internet Institute conducted an analysis of the #MacronLeaks hashtag, which involved a data dump of the then presidential candidate’s email correspondence. It found that 50 per cent of the Twitter content consisting of leaked documents and falsified reports was generated by only three percent of the total number of Twitter accounts. These bot accounts were pushing out 1,500 unique tweets per hour garnering an average of 9,500 retweets. The study concluded that over 22.8 million Twitter users were exposed to this information every hour on election day in France.22
Older practices such as gerrymandering – the manipulation of the boundaries of an electoral constituency so as to bring political advantage for a particular party\textsuperscript{23} – have found new impetus in the predictive power of Big Data. Gerrymandering has been shown to contribute to increased political polarisation,\textsuperscript{24} with disproportionate impacts on the poor. Elected leaders in such polarised constituencies typically tend to avoid taking up issues about economic inequality.\textsuperscript{25} What may be inferred from the above discussion is that while data based electioneering can potentially bring new efficiencies and effectiveness to organising and campaigning, the fact that the technological platforms that define the public sphere today are controlled by the elite does not bear well for the system of electoral democracy as a whole. In theory, the digital intelligence extracted from data cuts down on human resource intensive work, allows for grassroots organisers to optimise their canvassing and can mitigate the distortions of big capital in elections by allowing candidates to reach their constituencies over social media, at literally no cost. However, if the Cambridge Analytica or the MacronLeaks episode shows us anything, it is that we are headed for a vastly different future, one in which voter behaviour is being manipulated towards particular outcomes that may reflect neither a democratic mandate nor informed choice.

These developments pose a crisis for the public sphere. Borrowing from Dewey, “publics” in a democracy are created through “indirect, extensive, enduring and serious consequences of conjoint and interacting behavior”.\textsuperscript{26} Gamed by capital and technology, the very formation of publics is at risk today, with citizen interaction driven into information echo chambers that reinforce and amplify deep bias, resulting in a banality that prevents deliberation and posing particular risks, especially to already marginalised populations.

\textbf{2 • Algorithm see, algorithm do}

While elections are flashpoints – newsworthy by their very nature - the everyday practices of democracy, routine and largely unremarkable, rarely grab the same kind of media attention. However, it is often the structures and practices of everyday citizen-state interaction that become critical in furthering the kind of institutional change that can ultimately contribute to make democracy transformative.

Undoubtedly, there are advantages and efficiencies that digitally mediated governance can afford, such as easier access to information and entitlements for the citizen, and greater transparency and responsiveness for state institutions. E-government arrangements can also help achieve the objectives of participatory governance. The rise of an online network of municipalities in Spain is an excellent example that demonstrates this.\textsuperscript{27} However, when state-citizen engagement goes online into digital modalities and governance architectures become digitalised, they do pose administrative and legislative challenges, with significant implications for citizen rights.\textsuperscript{28}
Today, around the world technologies of calculation and regulation are being deployed to enact and regulate their subjects – citizens, migrants, consumers, students, colleagues and many more.\textsuperscript{29} Algorithms define the information to be acted upon, engage in “social sorting”\textsuperscript{30} and create autonomous repertoires of action and reaction. “Algorithms ‘govern’ because they have the power to structure possibilities,” notes Ananny.\textsuperscript{31} Napoli even argues that algorithms have come to take the place of institutions “because of their power to structure behavior, influence preferences, guide consumption, produce content, signal quality, and sway commodification.”\textsuperscript{32}

The state itself can be read as an algorithmic assemblage, a complex web of technical actors, autonomous technologies and layers of data coming together to prevail over the ostensible fallibility and inefficiency of human intent. Data in this equation is not merely a source of knowledge, it becomes knowledge itself.\textsuperscript{33}

Consider, for example, Singapore. First developed to detect bird flu outbreaks, the Risk Assessment and Horizon Scanning (RAHS) system in Singapore – which pools data from an exhaustive set of private and public databases – has become the primary decision making tool of the state – from immigration policy, economic forecasts, school curriculum to gauging the nation’s “mood” using Facebook.\textsuperscript{34} This highly centralised, all encompassing system of surveillance does not find a comprehensive counter in citizen privacy frameworks.\textsuperscript{35} Chinese social media giant Baidu has partnered with the military on the China Brain project, to create a system of social credit and ranking for citizens based on their social media engagement\textsuperscript{36} which will mean that the social media activity of citizens can be monitored and surveilled through state sanction and have a direct impact upon their freedoms.

Notably, welfare decisions are increasingly turned over to data-driven decision making in India, Australia and the US, creating large-scale exclusions in a matter of a single click with punishing consequences for the poor and the marginalised.\textsuperscript{37} As Ananny notes, algorithms are “embedded within the sociotechnical structures; they are shaped by communities of practice, embodied in standards, and most visible when they fail.”\textsuperscript{38}

Global data regimes, whether state led databases such as the RAHS, or privately held by platform corporations are the latest in a line of systems that citizens do not get to vote for, but which end up shaping the significant policies that affect their lives. Global data partnerships have thus seen the large-scale infiltration of data capitalists into hitherto public systems. As a result of this, public infrastructure becomes reconfigured into privately held data enclaves. This poses serious concerns for public good and citizen accountability.\textsuperscript{39} Critical sectors such as education have metamorphosed into covert sites of data mining by programmes. Examples include Google Apps for Education (GAFE)\textsuperscript{40} and Pearson’s Learning Curve for large-scale modelling and predictive analytics,\textsuperscript{41} both of which pose new ethical challenges to institutional practices. This shift is also visible in health care, with ambitious “smart medicine” projects such as IBM’s Watson.\textsuperscript{42}
As data enabled decision making becomes normalised within public services and governance systems, it promotes a centralisation of authority and power. Facts are selectively mobilised to position political intent as techno-managerial objectivity, while local discretion and flexibility to deal with contextual claims of marginal citizens is eliminated. In India, for instance, machine-based decision making on entitlements on the basis of data sets that were incorrect, resulted in the large exclusions of people from welfare benefits. While hiccups in any system are to be anticipated, what made the issue untenable in this case was the fact that no recourse to technological failure or glitches were factored in, leaving citizens, many of them critically dependent on the schemes, disenfranchised on the basis of a completely automated decision, working on flawed data. Algorithmic welfare management, referring here to the practice of deploying technological and data based solutions to process and approve entitlements, uses the myth of the sanctity of data – positing it as a necessary and unfailing means to plug leakages and redeem democracy from undeserving citizens free riding on public resources.

So far as the evidence goes, the algorithmic turn in democracy, the manifestations of which have been discussed in earlier sections, is embedded in the rise of global to local structures of authoritarian capitalism, geared to preserve a neo-liberal consensus even if local interests are at peril. Fragmenting societies insidiously, disenfranchising marginal citizens systematically, and generating political distractions relentlessly, the technological assemblages based on data and digital intelligence present immense and urgent challenges for the future of human societies.

The legitimacy of the algorithmic turn has been aided by a meta narrative of technomodernity that all nations must embrace. Cast as neutral tools of economic progress and social advancement, digital technologies have acquired an aura of ungovernability. Big tech corporations often present AI tools that learn and adapt rapidly as an autonomous force far too complex to be understood completely. However, in a rapidly unfolding datafied world, the integration of digital intelligence needs to be rooted in frameworks of accountability, where social intent guides the appropriation of technology.

3 • Watching the watchmen – need for new frameworks

In light of recent events and developments emanating from the Frankenstein Internet of today, digital corporations have come out with public statements about better standards and industry norms for privacy. Google has revealed a set of AI principles – that will ostensibly “take into account a broad range of social and economic factors, and…proceed where (Google) believe(s) that the overall likely benefits substantially exceed the foreseeable risks and downsides.” The principles, coming as they are in response to public pressure and discontent of employees, may seem like a good first step, but whether the company is upholding its ethical commitment or not will be based on Google’s own assessment. Platform companies such as Facebook have also committed to developing ethical standards.
and AI and design based solutions for countering the above discussed problems of runaway technology. Bodies such as the Institute of Electrical and Electronics Engineers (IEEE) are actively working to develop standards and guidelines for ethical AI.49 While this is a welcome move, the democratic project in this moment of flux needs an overhaul of institutional norms and cultures. Deliberating and debating the ethics that are adequate to the twenty first century techno-paradigm needs to be followed by non-negotiable and preeminent steps to translate ethical reflections into clear norms and institutional frameworks and oversight.

For one, the public sphere today is in immediate need of fortification against the disruptions of big capital and technology if we are to correct the derailment of democratic processes. Policies that can effectively govern misinformation and social engineering are needed to ensure that the spirit of deliberation and political engagement is preserved. Some countries such as Malaysia,50 Ireland51 and Germany52 have responded to this crisis with legislation that can counter the spread of fake news and platform misuse through punitive measures. Others such as the US are pushing for greater transparency on online political advertisements with proposed legislation such as The Honest Ads Act.53 The wave of proposed regulation and legislation is a welcome sign that countries have woken up to see the writing on the wall. However, the fine line where platform vigilance can easily turn into institutional censorship will be the slippery slope one needs to watch out for.

There is thus, a slow but growing consensus that solutions are needed, in ways that enrich citizens’ social capital rather than infringe on their rights. Critical thinking and discerning consumption of meaningful content, in a technoscape full of falsehoods remains an important challenge and policies that advocate critical media and digital literacy in schools and institutions in this context will be a positive move.54

Policymaking must move from being reactive to actively future-proofing democracy against the autocratic tendencies and function creep of datafication and algorithmic governance. In the absence of clearly articulated norms and policies, algorithmic assemblages, being integrated rapidly into governance frameworks today, risk becoming stand-ins for policy.

Algorithms are limited when it comes to exhibiting nuance, negotiating trade-offs, or exercising the necessary discretion when needed.55 This lack of flexibility completely evacuates citizen rights to meaningful representation and participation. As an important building block of democracy in the digital age, digital intelligence needs to be imagined, calibrated, tested and recalibrated recursively through the prism of citizen rights within institutional frameworks of transparency and accountability.

We therefore need sound and well developed “technological due process”56 that can ensure fairness and preserve the domain of participatory rule making. The right to peer into the algorithmic black box, demand explanations and challenge automated decision making are critical to realise the right to be heard in the context of digitalised governance. The Right to Explanation in the EU General Data Protection & Regulation57 and the City of New
York’s decision to put in place a task force to examine “automated decision systems” in public administration are some positive moves in this direction. Furthermore, algorithmic accountability needs to be complemented with strong data protection frameworks that protect citizen rights, allow them control over their data and prevent unethical and unscrupulous data driven techniques and profiteering. Policies must strike the right balance between the concern for individual privacy-personal data and considerations of data as a collective good-having public value. This means some dimensions of data and digital intelligence are treated like public resources and subject to appropriate public oversight. This is non-negotiable if data driven governance is to truly reflect democratic intent, foster inclusive development and guarantee citizen rights.

Ultimately, it is human intent that determines the democratic design or lack thereof in any given technology. Digital intelligence and algorithmic assemblages can surveil, disenfranchise or discriminate, not because of objective metrics, but because they have not been subject to the necessary institutional oversight that underpins the realisation of socio-cultural ideals in contemporary democracies. The innovations of the future can foster equity and social justice only if the policies of today shape a mandate for digital systems that centres citizen agency and democratic accountability.

NOTES


10 • This essay, in addition to being informed by recent global political events and discourses, also draws from key learnings from a research project we undertook in 2016-17 titled, ‘Voice or chatter? Using a structuration framework towards a theory of ICT-mediated citizen engagement’ (Gurumurthy et al., “Voice or Chatter?”, 2017). Through case studies in eight countries in Asia, Africa and Europe, the study examined the complex and dynamic relationship between the structures of technology and the structures of democracy and the implications for citizen engagement and voice.

11 • Harold D. Lasswell, *Propaganda Technique in the World War* (Gloucester: Peter Smith, 1927).

12 • Big Data are extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behavior and interactions.


14 • The use of statistical techniques that allow computers to iteratively improve upon a given task through data inputs.


18 • *ibid*.

19 • Referring here to automated Twitter accounts that pick up and amplify messages and flood the Internet space.

20 • A lengthy exchange of angry or abusive messages between users of an online forum.


First Monday 22, no. 8 (2017).
28 • Ibid.
44 • Deepti Bharthur, “Voice or Chatter Case
ANITA GURUMURTHY – India
Anita Gurumurthy is a founding member and executive director of IT for Change, where she leads research collaborations and projects in relation to the network society, with a focus on governance, democracy and gender justice. Her work reflects a keen interest in southern frameworks and the political economy of Internet governance and data and surveillance. Anita engages actively with policy makers, practitioners, social movements activists and the academic community to expand and deepen conversations on the public policy imperatives of the intertwining of the digital in all spheres of life.

email: anita@itforchange.net

DEEPTI BHARTHUR – India
Deepti Bharthur is a Research Associate at IT for Change. She contributes to academic, action, and policy research in the areas of e-governance and digital citizenship, data economy, platforms and digital exclusions. She has also coordinated and co-developed design based digital interventions for gender training and leads fund-raising and grant development activities at the organisation.

email: deepti@itforchange.net

Received in April 2018.
Original in English.