Has digitisation weakened democracy's defences?

The overall digitisation social process involves more and more information and activities moving into digital formats, then going online, and potentially securing global distribution via the cloud. This is not a neutral process for liberal democracies' working. **Melissa-Ellen Dowling** *argues that while digitisation may enable new forms of participation, and cut some of the costs of citizens organising, it opens liberal democracies to new threats from hostile foreign powers and so far unregulated waves of disinformation.*

As digitisation progressively permeates democratic political structures, democracies around the world are becoming more vulnerable to foreign interference. The advent of 'digital era governance' in post-industrialised democracies has led to the adoption of a range of electronic processes for public participation in politics. In particular, we are seeing digital mechanisms beginning to infiltrate traditionally analogue forms of democratic participation in decision-making. From ballot paper scanning, electronic voting machines, online petitioning, virtual consultation hubs, to the widespread digitisation of the public sphere – public participation in decision-making is becoming increasingly digital.

The risks of digitisation to democracy stem largely from three core digital deficiencies, or what otherwise might be termed, 'digitally-amplified problems': inauthenticity, data insecurity, and disinformation. Digitisation not only provides a veil behind which malign foreign entities can shield their identities to covertly disrupt another country's politics, but also enables interference to occur at unprecedented levels. Take for example, the US 2016 presidential election – the Mueller Report concluded that Russia's Internet Research Agency and the GRU used a range of digital tactics to target the election: hacking, leaking, bots, trolls, deep fakes, and more on a mass scale reaching significant portions of the population.

However, it is not all bad news. Digitisation has improved public access to politics which strengthens the fundamentals of democracy such as participation, inclusion, and tolerance. This raises a dilemma. On the one hand, do we resist digitisation in the governance and voting space to protect our processes and institutions from foreign interference and digital risks, but in doing so put democracy at additional risk from within? On the other hand, by eschewing digitisation (e.g. sticking with paper and pencil methods in Westminster systems), we risk reducing the scale and scope of public political access and engagement – thereby creating a public sphere monopolised by the legacy media. This makes the political sphere look dated, over-attached to traditional methods. And it causes its own problems with respect to the information ecosystem and democracy.

In fact, we already have some answers to the digital democracy dilemma: strike a balance between digital and analogue mechanisms of public participation in politics. As the UK's Intelligence Security Committee found in its Russia Report, paper ballot papers in the Brexit referendum effectively safeguarded the process from direct interference such as ballot tampering. Similarly, in Australia, hard-copy ballots continue to be used in the smaller constituencies used for federal elections for the House of Representatives, while digital mechanisms for counting state-wide Senate votes are employed in conjunction with human cross-checking. Meanwhile, in the US, problems with electronic voting machines has led to the restoration of supplementary paper trail procedures in some states. Retaining certain analogue processes can therefore protect against the digital deficiency of data insecurity, while allowing us to reap the benefits of digital technology.

The disinformation malaise

Unfortunately, there is one digitally-amplified deficiency plaguing democracies that is not so easily overcome: disinformation. Although disinformation is nothing new, it has become more prevalent and harder to detect in the digital era. The rise of social media that partly characterised the 'second wave' of digital era governance, improves access to the public sphere not only for a polity's citizens and enterprises, but also potentially for malign foreign entities. Government agencies are necessarily now far more active on social media, because they recognise that if government's nodality is to be preserved, then their messages must reach citizens in locations where they are active anyway. The COVID-19 crises in the UK and many countries also focused on governments' use of digital apps to try to personalise notifications to citizens.

Date originally posted: 2020-11-30

Permalink: https://blogs.lse.ac.uk/politicsandpolicy/digitisation-democracy/

Blog homepage: https://blogs.lse.ac.uk/politicsandpolicy/

But what if factual and objective social media messages (including, hopefully, those from government) are in danger of being swamped by tainted, misleading or inaccurate information? Digitally-enabled disinformation poses a particularly challenging risk because of the very nature of liberal democracy as a system enshrining free and open communication and political expression. It is insidious in the way that it targets human cognitive beliefs and attitudes, rather than administrative physical processes that we see in cases of data breaches.

Companies such as Google, Twitter, Facebook, and Reddit have been criticised for their slow and imperfect response to disinformation spreading via their platforms. While some argue that increased social media regulation is necessary to curb the problem, extensive regulation of such instruments of the public sphere may inadvertently jeopardise the open discussion fundamental to liberal democracy. These tensions make the problem even more difficult to resolve.

One of the most concerning consequences of disinformation for democracy is that it has the potential to create a crisis of legitimacy. Disinformation can reduce the legitimacy of policy outputs, election outcomes, government, democratic processes, and democracy as a belief-system through:

- Tainting the preference formation phase of decision-making, potentially generating a trust deficit, or boosting an existing one, not just in government and governance processes, but also in fellow members of the polity. This may jeopardise crucial ingredients of democracy.
- Stimulating widespread distrust of the veracity of information, leading to a 'post-truth' order where either anything goes, or correct information is disbelieved, resulting in political apathy.
- Undermining political culture more broadly by corroding collective belief in democracy as an ideology.

Conclusions

In some respects, digitisation has enhanced democracy through improving access to politics via electronic forms of public engagement. Yet the current social progress to ever-more-digital nonetheless presents an acute challenge to democracy on a practical and ideological level. Retaining analogue components of democratic processes is relatively effective in mitigating risks posed by data insecurity in formal participatory contexts. However, as the informal public sphere continues to digitise, the critical point at which the public forms political preferences is vulnerable to disinformation propagated by malign foreign entities. The fabric of liberal democracy is inherently vulnerable by its own design.

About the Author

Melissa-Ellen Dowling is a postdoctoral researcher in the Department of Politics and International Relations in the University of Adelaide. She is the lead researcher on the University's Countering Foreign Interference project. Her main research interests are digital democracy and malign influence, foreign interference, and national security policy.

Photo by NeONBRAND on Unsplash.

Date originally posted: 2020-11-30

Permalink: https://blogs.lse.ac.uk/politicsandpolicy/digitisation-democracy/

Blog homepage: https://blogs.lse.ac.uk/politicsandpolicy/