

Can we trust the polls? How emerging technologies affect democracy

Kousuke Saito

Do technologies change how democracy works, or do democratic principles determine how technologies work?

With 2024 being a global election year — voters having gone to or set to head to polls in more than 60 countries — a great deal of attention is being paid to the relationship between emerging technologies and democracy. Needless to say, elections are procedures that form the cornerstone of democracy. Through elections, voters select politicians and political parties that represent their views and interests. If satisfied with the performances of the politicians, voters may reelect them in subsequent elections.

Information such as politicians' manifestos, their accomplishments during their tenure, their ideologies and their personalities influence people's voting behavior. It has repeatedly been emphasized that the development of information and communication technology (ICT) has enhanced individuals' ability to gather and disseminate information, thereby contributing to achieving democracy.

However, what is currently drawing attention is the risk posed to democratic society by distorted voting behavior.

Who distorts elections?

In the mid-2010s when the concept of emerging technologies began to come under the spotlight, concerns arose regarding the unclear outlook of technological development and the uncertainty surrounding its social impact. Under such circumstances, significant discussions began to emerge regarding the actual risks associated with rapidly developing and spreading technologies. This led to rapid progressions in debates over how to regulate them. The risks posed by information and communication-related emerging technologies on democracy can be broadly classified into two patterns.

One is the issue of foreign governments exerting influence. Russia's interference in the 2016 U.S. presidential election, targeting Democratic Party candidate Hillary Clinton, became a prominent case highlighting how the development of ICT can attract foreign threats.

A threat analysis report released by Microsoft in September 2023 highlighted China's interference in societies and election processes in other countries through cyberspace. It noted that in recent years some Chinese influence operations have begun to utilize generative artificial intelligence (AI) to produce visual content. Such a situation can indeed be considered a national security issue, as it involves the external threat to a political system — essentially, a country's unique value.

The other trend, which has drawn even more attention recently, is the development of emerging technologies leading to election-related risks within a country. Distorted information or discourses based on misunderstanding are not solely spread by



foreign entities, but can also originate within a country and can be propagated easily through cyberspace.

Furthermore, there are concerns that elections could be deliberately manipulated not only through information distortion, but also through digital gerrymandering — utilizing ICT and digital data to intentionally redraw electoral districts and generate biased voting behavior. Discussions over how to utilize and regulate such technologies also highlight the issue of how governments should handle their countries' political systems and deal with the social risks created within them.

Generative AI in elections

The technology that has caused the most concern regarding its adverse effect on democracy in the past year is generative AI. Generative AI involves the risks arising from a user's intentions and behaviors, alongside the frequently discussed risk of AI autonomy potentially leading to unintended consequences beyond human control. At the current stage, there are cases in which election candidates and campaigns disseminate information using generative AI.

In April 2023, following U.S. President Joe Biden's announcement of his reelection campaign, the Republican National Committee released a video on YouTube featuring images suggesting Biden's reelection would result in a series of crises relating to international affairs and financial markets.

The caption underneath the YouTube video read, "An AI-generated look into the country's possible future if Joe Biden is re-elected in 2024," and the video was still available at the time of writing. While the video presents an imagined future scenario rather than distorting facts, it serves as an example of attempts to manipulate public opinion using generative AI. Still, we can argue that the use of generative AI in this manner represents an extension of negative campaigning tactics conducted through existing media channels.

In the context of impact on elections, a more significant concern is the dissemination of uncertain information originating from anonymous sources. For instance, prior to last year's Turkish presidential election, in which President Recep Tayyip Erdogan was reelected, a video of his main challenger, Kemal Kilicdaroglu, which was later found to have been manipulated using deepfake technology, stirred controversy.

In Slovakia, days before parliamentary elections in September, a fake recording seemingly created using generative AI, in which one of the candidates boasted about how he'd rigged the election, spread widely online. In January, investigations commenced in the United States following reports that an apparent robocall utilized AI to mimic Biden's voice, discouraging supporters of the Democratic Party from going to the polls for the primary ballot of the U.S. presidential election. Trust in elections will be eroded if voters are to make decisions under the influence of such information distortion.



Pushing for co-regulation

Although the risk of many people being swayed by anonymous, sensational information of unknown origin has been widely recognized, the option of not using generative AI is no longer discussed due to the usefulness of the technology. This is why today's challenge is focused on how to guarantee the credibility of information sent out in cyberspace.

It is noteworthy that private companies are embarking on self-regulation to manage risks, particularly with 2024 being a global election year. This development represents a significant milestone in considering future regulations regarding this issue. In early 2023, companies such as OpenAI and Meta established restrictions on the use of their generative AI tools in political contexts.

Later, in July, the Biden administration obtained voluntary commitments from major AI companies to mitigate the risks posed by AI, and subsequently, based on this agreement, in October the administration issued an executive order on safe, secure and trustworthy AI. The executive order represents a typical example of a co-regulation model as it is founded on consensus reached with private enterprises that implement the regulations.

From a global perspective, it is significant that discussions regarding regulations are advancing, including in China. At the global AI Safety Summit held in the United Kingdom in November, leaders shared their awareness of the risks posed by generative AI affecting upcoming elections through disinformation. This indicates that there is a broad consensus regarding the

necessity for regulations not only among allies, but also China. The global response to the risks is also made on the private-sector level.

In February, 20 major IT firms signed a voluntary accord to help stop deceptive AI-generated content from interfering with global elections. They pledged to collaborate on measures such as developing technology to detect and watermark realistic content created with AI. The group includes not only U.S. firms, but also TikTok, a Chinese company whose ties with the Chinese Communist Party have often raised concerns.

At the same time, the U.S. government announced the establishment of the AI Safety Institute Consortium, through which more than 200 leading AI stakeholders agreed to cooperate in developing guidelines for risk management, safety and security. Governments and the private sector are working together beyond national borders and differing political systems to establish regulations on generative AI.

Varying risks

However, are democratic and authoritarian regimes facing the same risks? If the use of AI distorts elections, it would doubtlessly present a major risk, particularly for democratic political systems. On the other hand, even China is concerned that technologies like generative AI could be used as a tool to criticize authorities, which suggests there is an incentive for implementing certain regulations. This indicates that the same technology is perceived as having different risks depending on the kind of political systems adopted.



If both democratic and authoritarian states perceive technologies like AI as posing risks, albeit in different forms, they may cooperate in creating regulations. However, we must note that due to differing political systems, benefits from such cooperation could be asymmetrical. Technological regulations implemented with the aim of protecting freedom in democratic states could potentially become rules to excessively restrict freedom of expression and media unfavorable for authorities under authoritarian states.

Yet, recognition regarding AI regulation may vary even within democratic states. While they share a common understanding that risks posed to democracy by cyberspace and generative AI must be properly managed, their perspectives on individual rights and democracy may differ. If there is a gap between their interpretations of what should be protected, the discrepancy — along with differences in the technological trends and industrial structure of each country — could lead to friction among countries in forming specific rules.

Japan's challenges

What is the situation like in Japan? It is true that Tokyo is taking a proactive approach to AI regulation, leading the launch of the Hiroshima AI Process following the Group of Seven summit in Hiroshima in May. This initiative aims to promote international rule-making for advanced AI systems, as well as supporting consensus-building at the AI Safety Summit. At the same time, however, while the U.S. and Europe are taking the lead in strengthening rules

within their country or the bloc, Japan has been relatively slow in formulating domestic regulations in the field of AI, despite growing concerns.

In light of this situation, it is significant that Japan is discussing the drafting of legislation to oversee generative AI technologies, with the aim of enacting a new law within this year. This move will be essential for Japan to participate in the global efforts to create regulations while taking into account its own perspective of democracy and technological background, and make its domestic regulatory framework match global-level discussions on regulations.

Regarding the impact of AI technologies on elections, fortunately, or unfortunately, there have not been reports of specific cases directly affecting election results in Japan. However, there was one case of a fake video featuring Prime Minister Fumio Kishida that went viral.

From a technological standpoint, public-private joint efforts to develop a domestically produced Large Language Model (LLM) — a specialized type of AI that has been trained with vast amounts of text data to understand existing content and generate original content — could have a significant impact. In Japan today, the use of generative AI dependent on LLMs developed in English-speaking countries has been the mainstream. If Japanese-based LLMs become widespread, the use of AI will accelerate in Japanese society, alongside an increase in the amount of content with risks.

Moreover, content seen by Japanese speakers as unnatural can spread in a more natural form, indicating risks of disinformation becoming



harder to detect. As in many other countries, the use of emerging technologies, including generative AI, is accelerating in Japan, but as these become more widespread, voters in Japan will face an increasing number of risks.

Working to establish regulations domestically and internationally, and creating a healthy information environment, involves not only determining how to use technologies, but also addressing the issue of clarifying how our democracy should be.



Profile



Visiting Senior Research Fellow Associate Professor, Faculty of Global Studies, Sophia University

Expertise

Kousuke Saito

International Relations / Security Studies / Technology Management / Innovation and Politics

https://ihj.global/en/experts/experts-4426/

Disclaimer: The views expressed in this API Geoeconomic Briefing do not necessarily reflect those of the API, the Institute of Geoeconomics (IOG) or any other organizations to which the author belongs.