Bill to combat deepfakes during election timely despite challenges: Analysts

Chin Soo Fang
The Straits Times, 09 September 2024

SINGAPORE - Proposed measures to combat deepfakes during elections are timely given the proliferation of such content worldwide, say analysts. But the effectiveness of such laws will depend on factors such as enforcement and public awareness, they added.

The Elections (Integrity of Online Advertising) (Amendment) Bill, tabled in Parliament on Sept 9, will prohibit the publication of digitally-manipulated content during elections. This refers to content that realistically depicts an election candidate saying or doing something that he or she did not, and includes misinformation generated using artificial intelligence (AI) - commonly known as deepfakes.

These measures will be from the issuance of the Writ of Election to the close of polling on Polling Day, with the Returning Officer empowered to issue corrective directions to those who publish such content.

Professor Mohan Kankanhalli, director of the National University of Singapore's AI Institute, said the problem of misinformation and disinformation requires a combination of technical solutions, regulation and legislation, and public education.

"These laws not only serve as deterrents, they also provide legal recourse post-publication. Such legislation is therefore necessary," he said.

He added that while such laws signal a proactive stance, enforcement in other countries has been challenging.

"Detecting and proving malicious intent behind deepfakes can be difficult," he said. "However, these capabilities are constantly improving."

Prof Kankanhalli cited the example of the 2020 US presidential election where deepfakes were a concern, though their direct use was limited.

One notable case involved a manipulated video of House Speaker Nancy Pelosi, which was slowed down to make her appear intoxicated or cognitively impaired. It showed how video manipulation could mislead the public, and demonstrated the potential for deepfakes to be used as a political weapon, he said.

He also cited the example of the 2019 Indian general election, when deepfakes were used by the Bharatiya Janata Party (BJP) to create manipulated videos for campaign purposes. On one occasion, the party produced videos of Delhi BJP President Manoj Tiwari, in which he appeared to speak in different dialects of Hindi and Haryanvi. The videos were designed to reach specific regional audiences more effectively, without requiring him to physically record the same speech multiple times.

"Though this use of deepfake technology wasn't meant to deceive in a malicious sense, it raised ethical concerns about the potential for such technology to mislead voters if misused,"

Prof Kankanhalli said, adding that this incident also marked one of the first high-profile cases where deepfake technology was used in a political campaign.

Assistant Professor Roy Lee, from the Singapore University of Technology and Design's Information Systems Technology and Design pillar, noted that concerns have also been raised about deepfakes for the upcoming 2024 US presidential election. Manipulated videos targeting Indonesian politicians also emerged during Indonesia's recent election, he said.

In response to this growing problem, laws aimed at curbing deepfakes have been introduced in several countries.

For example, the US state of California passed a law in 2019 to criminalise the distribution of manipulated media such as deepfakes intended to mislead voters. Specifically, it prohibited individuals or entities from distributing such media with malice within 60 days of an election.

The European Union also enacted the Digital Services Act in 2022 which imposes stricter regulations on digital platforms, including measures to prevent the spread of manipulated content.

Prof Lee said: "These laws have been part of broader efforts to prevent election interference, although their effectiveness largely depends on timely detection and public awareness."

Mr Benjamin Ang, head of the Centre of Excellence for National Security at Nanyang Technological University, noted that the US has also banned the use of AI-generated voices in robocalls, including those used in election campaigns to spread misinformation and mislead voters.

The decision comes after AI-generated robocalls impersonating President Joe Biden sought to discourage voting in the New Hampshire primary election in January. Some experts noted that enforcing this law against foreign actors seeking to interfere in US elections may still be challenging, though it sends a clear message that exploiting AI to mislead voters will not be tolerated.

"The law is only one part of the battle to combat deepfakes and protect electoral fairness and integrity, because this also requires vigilance and cooperation from tech platforms where the deepfakes are circulating, public education about the dangers of spreading deepfakes, and our own personal choice to stop and think very seriously before we share any videos or other content," said Mr Ang.

He added: "The impact of this Bill, like all other laws, should be to set standards of behaviour by which our society can maintain order, resolve disputes, and protect rights."

Dr Carol Soon, principal research fellow at Institute of Policy Studies and adjunct principal scientist at the Centre for Advanced Technologies in Online Safety (CATOS) which studies deepfakes, said deepfakes also make it easier for political candidates to falsely claim genuine content to be manipulated or generated by AI, allowing them to benefit from the "liar's dividend" on a polluted information ecosystem.

For example, during the recent Turkish election, a video that showed compromising images of an electoral candidate was said to be a deepfake when it was in fact real.

“This proposed Bill is surgical as it is focused both in terms of the defined offense and time frame. The Bill thus seeks to strike the fine balance between upholding election integrity and allowing for non-harmful use of generative AI such as entertainment, education and creative usage,” she said.

To be protected under the proposed Bill, prospective candidates will first have to pay their election deposits and consent to their names being published on a list that will be put up on the Elections Department’s website, some time before Nomination Day. If they choose do so, it will be the first time that the identities of prospective candidates are made public before Nomination Day.

The proposed law will also cover successfully-nominated candidates from the end of Nomination Day to Polling Day.

On the early disclosure of candidates’ names, Prof Lee said this primarily enhances transparency in the electoral process.

“This transparency can help mitigate the risk of misinformation and deepfake-related content as voters will have more time to scrutinise information about candidates and ensure its accuracy,” he said. “It also provides more time for online platforms and regulatory bodies to monitor and take corrective actions against manipulated content targeting these candidates.”