Deepfakes in India: Regulation and Privacy

While the use of deepfake videos are relatively rare in Indian politics, ***Simran Jain and Piyush Jha (Independent Researchers, India)*** *argue that the potential of their misuse in other domains, and subsequent infringement of individual privacy, cannot be underestimated. Only rapid governmental intervention in the form of new legislative and regulatory frameworks can help the country deal with this rapidly evolving technology.*

In February 2020, during the Delhi Assembly polls, a video of Delhi's BJP President criticising his opponent surfaced on the internet. Interestingly, this video was a result of morphing an older video of his with another in which he was talking about a completely different issue. This event marked one of the first usages of deepfake technology in an Indian election.

A deepfake is an advanced Machine Learning algorithm that uses Generative Adversarial Networks. Videos of individuals are used to create strikingly similar, but forged versions, by mimicking their blinking patterns, head movements, vocal patterns, and facial expressions. The creator can put words into the mouth of the concerned individual to deceive the viewer. A prominent use of deepfakes includes a video of Facebook CEO Mark Zuckerberg claiming to control stolen data of billions of Facebook users.

'Seeing is believing' is an old saying, but with deepfakes, one can no longer believe what they are viewing. This is why deepfakes pose a threat to individual privacy as well as to society. They are cheap to create and, upon misuse, have the potential to influence voters, manipulate masses to result in communal unrest and cause invasions of privacy, to name just a few issues with them.

Deepfakes have also challenged legal systems across the world that are trying to keep themselves abreast of this rapidly evolving technology. In the USA, the Deepfakes Accountability Act (passed in 2019), mandated deepfakes to be watermarked for the purpose of identification. Virginia has also amended its law banning nonconsensual pornography from including deepfakes.

In India however there is no explicit law banning deepfakes. Amidst the current laws in force, sections 67 and 67A of The Information Technology Act 2000 ("IT Act") provide punishment for publishing sexually explicit material in electronic form. Section 500 of the Indian Penal Code 1860 provides punishment for defamation, but these provisions are insufficient to tackle various forms in which deepfakes exist.

The right to privacy has been recognized as a fundamental right in India in the Supreme Court judgment of *Justice KS Puttaswamy (Retd.) v Union of India*, and it is not long before rampant use of this technology may infringe the privacy of individuals. The Personal Data Protection Bill 2019 ("Bill") provides for the protection of personal data of individuals, which includes data relating to a natural person who is directly or indirectly identifiable. The bill places restrictions on the processing of data except for a lawful purpose. The state, company or individual in charge of processing personal data is under an obligation to make sure that the processed data is not misleading. It also lays down penalties in the case of contravention of its provisions; and S.20 provides for the right to be forgotten, so that circulation of personal data of an individual could be stopped. This bill also has extraterritorial applicability, in case the creator of such videos is situated outside India. Therefore, it can be concluded that once this bill has been passed, it shall impliedly prohibit the usage and circulation of deepfake videos.

However, it does not contain any provisions relating to the protection of data of deceased persons. These provisions are essential in the context of politicians, spiritual leaders, whose deepfakes in the form of speeches, can be circulated after their death with an intent to manipulate the beliefs of masses. Therefore, certain provisions to this effect can be added to the bill, which include seeking the consent of the heirs of such deceased persons before making use of their data. Additionally, such heirs or other persons interested in the protection of the deceased person's data should be given rights for filing a suit, in case provisions of the Bill are violated. Such similar provisions exist under S.25 of The Privacy Act of Hungary. Further, the Spanish Data Protection Act (Organic Law 3/2018) gives rights to heirs of the deceased to erase or rectify data unless the deceased person would have prohibited it.

Date originally posted: 2020-05-21

Permalink: https://blogs.lse.ac.uk/southasia/2020/05/21/deepfakes-in-india-regulation-and-privacy/

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

Apart from making legislation adept towards limiting the misuse of this technology, another major concern is to be able to detect whether a video is fake in the first place. To date, for every flaw exposed in deepfakes to help with its detection, a better version of its algorithm has been released that eliminates the previous imperfections. Therefore, it is imperative that the government and other regulatory bodies take steps to ensure the authenticity of videos circulated in the public domain. For instance, the Election Commission can make it mandatory for all political parties to make use of Digital Signature, as under S.3 of the IT Act, on any video circulated by them for the purpose of campaigning. In a scenario where the origin of the video cannot be controlled, the government should set up a body that can monitor deepfakes using blockchain technology. Blockchains store blocks of data on a decentralized network where anyone can verify the originality of the information by matching with the distinct non-invertible key. Even the slightest manipulation of the data will result in a mismatch.

Recently in his response to deepfake technology, India's IT minister had assumed the use of deepfakes to be limited for the circulation of fake news. However, deepfakes can be used solely for entertainment and yet infringe on someone's privacy. Therefore, along with spreading awareness about this novel technology to the masses, adequate attention should be given by the government towards the challenges posed by deepfakes, before they become a menace in India.

This article gives the views of the author, and not the position of the South Asia @ LSE blog, nor of the London School of Economics. Featured photo: Camera at live event. Credit: Donald Tong, Pexels.

Date originally posted: 2020-05-21

Permalink: https://blogs.lse.ac.uk/southasia/2020/05/21/deepfakes-in-india-regulation-and-privacy/

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