Navigating the Ethical Labyrinth: A Comprehensive Examination of Deepfake Regulation in India

Shaantam Saini

Introduction

The insidious rise of deepfakes, exemplified by the recent scandal involving Indian actress Rashmika Mandanna, has thrust this sophisticated form of digital manipulation into the public spotlight in India. The manipulated video, decried for its misogynistic undertones and invasion of privacy, serves as a stark reminder of the ethical and regulatory challenges posed by deepfakes and AI-based fake news. As technology advances at an unprecedented pace, the potential harm to an individual's reputation, privacy, and the broader societal fabric looms larger. This academic discourse critically examines the policy implications, international case studies, and comparative analyses, identifies gaps in the existing regulatory framework and outlines a comprehensive roadmap for navigating the intricate ethical labyrinth of deep fakes in the Indian context.

As the boundaries between reality and manipulated digital content blur, the need for a nuanced and adaptive regulatory framework becomes evident. This discourse seeks to unravel the complex layers of deepfake regulation, emphasizing the importance of aligning technological advancements with ethical considerations in India's ongoing quest for a secure and trustworthy digital landscape.

Policy Implications of Deepfakes and AI-Based Fake News

Challenges of Regulating Deepfakes and AI-Based Fake News

Crafting effective regulatory frameworks for deepfakes and AI-based fake news is a daunting task, given the rapid evolution of technology. The lack of universally accepted definitions for these terms adds complexity to the regulatory landscape. The dynamic nature of the internet, with its global reach, makes it difficult to enforce regulations across borders. However, the absence of federal laws specifically addressing deepfakes in India is not a legislative oversight but a reflection of the evolving nature of these technologies.

India's existing legal framework, notably the Information Technology (IT) Act of 2000 and relevant sections of the Indian Penal Code, does provide a foundational basis for addressing certain aspects of deepfake misuse. Sections 67 and 67A of the IT Act criminalize the transmission of obscene material and sexually explicit content in electronic form, respectively. Additionally, Section 500 of the IPC deals with defamation. The Personal Data Protection Bill, pending in the Indian Parliament, holds the potential to offer a more comprehensive legal framework for addressing privacy concerns related to deepfakes.

As the boundaries between reality and manipulated digital content blur, the need for a nuanced and adaptive regulatory framework becomes evident. This discourse seeks to unravel the complex layers of deepfake regulation, emphasizing the importance of aligning technological advancements with ethical considerations in India's ongoing quest for a secure and trustworthy digital landscape.

Case Studies of Deepfakes and AI-Based Fake News

Examining international case studies reinforces the need for a robust regulatory framework. The Pelosi

deepfake incident in the United States demonstrated how a manipulated video could be used to discredit a political figure. Similarly, during the Myanmar genocide, Facebook's role in spreading fake news had severe consequences, contributing to violence against the Rohingya minority. These incidents underscore the broader societal implications of unchecked dissemination of deepfakes and AI-based fake news.

In the Indian context, the 2020 Delhi assembly polls witnessed the emergence of a deepfake video featuring the Bhartiya Janta Party's Delhi President criticizing his opponent. This video, a result of morphing an older video related to the Citizenship Amendment Act 2019, exemplifies how deepfakes can infiltrate political discourse, influencing public opinions during critical electoral events.

Comparative Analysis of Deepfakes and AI-Based Fake News Policies

A comparative analysis of regulatory approaches globally reveals valuable insights. France has adopted a comprehensive strategy with the establishment of the Online Harms Regulator, emphasizing the need for a centralized authority. Singapore takes a more targeted approach, criminalizing specific content harmful to an individual's reputation or privacy. The United Kingdom, while lacking specific legislation, proposes measures to enhance transparency and user control.

France's Law No. 2020-766 of June 24, 2020, on Confronting Respect for the Principles of the Republic introduces a broad definition of "online harms," encompassing deepfakes and AI-based fake news. The establishment of the Online Harms Regulator, with the authority to impose significant fines on non-compliant platforms, demonstrates a proactive approach to enforcement.

Singapore's Protection from Online Harms Act (POHA) criminalises the creation and dissemination of deepfakes and AI-based fake news intending to harm a person's reputation or privacy. This targeted approach empowers the Singapore Police Force to investigate and prosecute offences under the POHA, accompanied by provisions for victim compensation and support.

While the United Kingdom has not enacted specific legislation for deepfakes and AI-based fake news, the "Online Harms White Paper" outlines proposed measures. These include increasing transparency around social media companies' algorithmic use, empowering users to control data and privacy settings, and supporting fact-checking and verification tools.

Gaps in the Existing Policy Framework AND the Way Forward

Lack of Clear and Consistent Definitions

The absence of clear and consistent definitions for deepfakes and AI-based fake news poses a significant challenge. To address this, the Indian government can take a proactive stance by establishing a working group or committee comprising experts from academia, industry, government, and civil society. This group can work towards developing precise and widely accepted definitions.

Insufficient Scope of Regulation

While the current focus is on protecting individuals, the potential societal harms of these technologies necessitate an expanded regulatory scope. The Indian government could consider broadening the scope to include the protection of privacy, democratic processes, and national security. This broader approach aligns with global concerns about the potential misuse of deepfakes.

Singapore's Protection from Online Harms Act (POHA) criminalises the creation and dissemination of deepfakes and AI-based fake news intending to harm a person's reputation or privacy. This targeted approach empowers the Singapore Police Force to investigate and prosecute offences under the POHA, accompanied by provisions for victim compensation and support.

Inadequate Enforcement Mechanisms

Enhancing enforcement mechanisms is crucial for effective regulation. Measures such as increased fines for non-compliant platforms, improved global cooperation, and investment in advanced content detection technologies

can strengthen enforcement. Cooperation with law enforcement agencies globally is particularly vital, considering the decentralised nature of deepfake technology.

Lack of Specific Legislation

The absence of specific legislation tailored to address the challenges of deepfakes and AI-based fake news creates uncertainty. The Information Technology Act, 2000, does not account for the nuances of deepfake creation, distribution, and misuse. The Indian government could consider drafting and enacting legislation explicitly targeting these technologies, providing legal clarity and a foundation for effective regulation.

Vulnerability of Non-Existent Human Faces

The unique vulnerability of synthetic faces, not existing in the real world, presents a distinct challenge. Platforms must take preventative measures to combat the misuse of these synthetic faces in deepfakes. Addressing this concern requires specific regulations or guidelines from the government, ensuring that synthetic faces are not employed to create deceptive content.

Limited Protection for Deceased Persons' Data

The current legal framework lacks provisions for protecting the personal data of deceased persons. Amending the pending Personal Data Protection Bill, 2019, to explicitly include deceased persons as data subjects can fill this gap. Such an amendment would grant legal rights to heirs, allowing them control over the usage of their deceased loved ones' data.

Absence of Clear Guidelines for Intermediaries

Clear guidelines for intermediaries, especially social media platforms, are essential to curb the spread of deepfakes and AI-based fake news. Collaboration with law enforcement agencies and prompt identification, removal, and reporting of such content by intermediaries can mitigate the rapid dissemination of deceptive content.

Lack of Public Awareness

Public awareness about deepfakes and AI-based fake news remains relatively low in India. Launching public awareness campaigns can bridge this gap, educating people about the dangers of these technologies. Such campaigns can provide information on identifying fake content, reporting it to platform operators, and seeking help from law enforcement agencies.

Concluding Remarks

India stands at a critical juncture in its efforts to grapple with the multifaceted challenges posed by deepfakes and AI-based fake news. The evolving nature of this threat demands a dynamic and comprehensive regulatory approach, one that aligns with the principles of individual privacy, ethical use of technology, and the safeguarding of democratic processes. While the Indian government has taken initial steps through advisories and existing legal frameworks, there remains a pressing need to fortify the nation's defences against the malicious potential of deepfakes.

The proposed amendments to the Personal Data Protection Bill, 2019, exemplify India's commitment to adapt legal frameworks to contemporary challenges. However, a concerted effort is required to bridge the awareness gap among the public, fortify enforcement mechanisms, and bolster international collaboration in tackling cross-border implications. As India charts its course in the digital era, a proactive and adaptive stance in shaping policies will be indispensable to foster a resilient, secure, and ethical technological landscape. The journey towards combating deepfakes is not only a legal imperative but a societal responsibility, necessitating collective vigilance and collaborative action. ❑

India stands at a critical juncture in its efforts to grapple with the multifaceted challenges posed by deepfakes and AI-based fake news. The evolving nature of this threat demands a dynamic and comprehensive regulatory approach, one that aligns with the principles of individual privacy, ethical use of technology, and the safeguarding of democratic processes.