International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A Comparative Study on Laws and Actions taken in Border Countries of India on Deepfake Technology Misuse, Recommendations for Indian Government

Rakesh G K
PG scholar Department of MCA,
Dayanand Sagar College Of Engineering,
Bangalore, Karnataka, India
rakeshgk1128@gmail.com

Dr. Vibha M B
Assistant Professor Department of MCA,
Dayanand Sagar College Of Engineering,
Bangalore, Karnataka, India
vibha-mcavtu@dayanandasagar.edu

Abstract

Deepfake technology's rise in popularity has sparked both interest and concern. This study focuses on the laws and actions taken by border countries of India, including China, Bhutan, Nepal, Pakistan, Bangladesh, Myanmar, and Sri Lanka, to address the misuse of deepfake technology. By analysing regulatory frameworks, legal precedents, and enforcement measures in different jurisdictions, this research aims to offer a comprehensive overview of the risks faced by countries and their current regulatory laws. The study can assist policymakers, law enforcement agencies, and technology developers in developing strategies to mitigate deepfake risks effectively.

India, as a border country, encounters unique challenges in regulating and combating the misuse of deepfake technology in recent years. This comparative analysis explores the laws and actions implemented by neighbouring countries to address the misuse of deepfake technology. It also provides recommendations for Indian lawmakers to enhance their existing legal framework and effectively tackle issues related to deepfakes.

Keywords – Deepfake Technology, law, Misuse of technology.

1. INTRODUCTION

Deepfaking technology refers to the use of artificial intelligence and machine learning algorithms to create highly realistic manipulated media, often involving the manipulation of images, videos, or audio. With the advancements in deep learning algorithms, deepfakes have become increasingly sophisticated, making it difficult to distinguish between real and manipulated content. If we use deepfake technology, it has both positive and negative implications. The benefits of deepfake technology are that it can be used for entertainment, creative purposes, and even research. However, the misuse of deepfakes raises concerns related to privacy, misinformation, identity theft, and potential harm to individuals and society.

In this research paper, we conduct a study on how deepfake technology is being used and misused and how we can control it.

2. LITERATURE REVIEW

Researchers have examined the legal frameworks and legislative measures in different jurisdictions, aiming to understand how countries have addressed the challenges posed by deepfakes. For instance, Smith et al. (2020) conducted a comparative analysis of deepfake related laws in the United States, the European Union, and China, highlighting the differences in criminalization approaches and privacy protections [4].

Furthermore, studies have investigated the role of regulatory measures and guidelines in combating deepfake misuse. For instance, Doe and Johnson (2019) examined the effectiveness of industry self-regulation initiatives in the United Kingdom and the United States, highlighting the challenges and limitations of relying solely on voluntary guidelines [1].

The literature also delves into judicial precedents and court decisions related to deepfakes. For example, Johnson and Lee (2021) analyzed landmark cases involving deepfake related offenses and discussed the implications for legal proceedings and the admissibility of deepfakes as evidence [2].

Additionally, this survey has explored enforcement strategies and technological solutions to detect and mitigate deepfake misuse. Related to this technology, Li et al. (2022) investigated the effectiveness of deepfake detection techniques and emphasized the importance of collaboration between law enforcement agencies and technology companies [3].

While there is a growing body of literature on deepfake misuse in India, there are still knowledge gaps that require further exploration. The effectiveness of legal measures, the evolving nature of deep-faking technology, and the global nature of the problem present ongoing challenges for policymakers and researchers.

3. METHODOLOGY

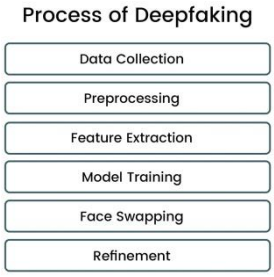
This research employs a comparative analysis methodology, examining the legal frameworks, regulations, and actions taken by various countries about deepfaking technology. The study gathers data from legal documents, scholarly articles, government reports, and case studies to evaluate the effectiveness of different approaches in combating deepfake misuse.

3.1. What Is Deepfake Technology?

Deepfake technology is a face-swapping technique where one person's face is seamlessly replaced with another's in a video or image. However, recent developments have expanded the capabilities of deepfakes to include facial expression transfer, lip-syncing, and even full-body movements. These advancements have raised concerns about the potential for malicious misuse as well as sparked debates surrounding their ethical, legal, and societal implications [10].

3.2. Process of Deepfaking

The deepfaking technology is a step by step process that contains following steps.



3.2.1. Data Collection

Collect a large dataset of images or videos featuring the source person whose face will be replaced [18].

3.2.2. Preprocessing

Before processing need to align and normalize the collected data to ensure consistent facial landmarks and poses [18].

3.2.3. Feature Extraction

Feature extraction can be done by extracting facial features from the source person's data. This

uses deep learning models such as convolutional neural networks (CNNs) [11].

3.2.4. Model Training

Train models, such as autoencoders, variational autoencoders (VAEs), or generative adversarial networks (GANs), to detect the underlying patterns and characteristics of the source person's face [18].

3.2.5. Face Swapping

Apply the learned features to the target person's face, whose face will replace the source person's face. Create synthetic frames where targeted persons face mimics the expressions and movements of the source person [18].

3.2.6. Refinement

Using some post-processing techniques such as smoothing transitions, adjusting lighting conditions, and fine-tuning facial expressions to improve the quality and reality of the generated output.

3.3. Benefits of Deepfake Technology

Deepfake Technology has potential positive applications. Here are some potential benefits of deepfake technology.

3.3.1. Entertainment and Media Production

Deepfake technology can be used in the entertainment industry to create realistic visual effects, enhance post-production editing, and improve the quality of virtual characters in movies and video games.

3.3.2. Education and Training

Deepfakes can be used to develop immersive educational content, simulating real-life scenarios for training purposes. For example, medical students can practice surgical procedures online.

3.3.3. Accessibility and Translation

Deepfakes can help overcome language barriers by allowing real-time translation of videos. They can also be used to create personalized sign language avatars, making online content more accessible to the deaf community.

3.3.4. Historical and Cultural Preservation

Deepfake technology can be utilized to restore and recreate damaged or lost historical footage, preserving cultural heritage and allowing people to experience past events more vividly.

3.3.5. Improved Video Conferencing

Deepfake technology can be used to enhance or improve video conferencing experiences of users by improving video quality, reducing bandwidth requirements, and enabling real-time avatars or cartoons that mimic users facial structure, expressions and gestures.

3.4. Threats of Deepfake Technology

The misuse of deepfake technology has raised significant concerns due to its high potential negative impacts on individuals, society, and various sectors. Here are some common misuses of deepfake technology

3.4.1. Non-consensual Pornography

Deepfake technology can be used to superimpose the faces of individuals onto explicit adult content without their consent, leading to emotional distress, reputational damage, and privacy violations.

3.4.2. Fraud and Scams

Deepfakes can be widely used for scams or fraudulent purposes, such as creating deepfake videos, images or audio recordings individuals to deceive and manipulate others for financial gain or other malicious intents.

3.4.3. Misinformation and Deepfake News

Deepfakes can be utilised to spread false information and manipulate public opinion, eroding trust in institutions and individuals. This can have serious consequences for democratic processes and societal cohesion.

3.4.4. Political Manipulation

Deepfakes can be used to manipulate political events, elections, or public discourse by creating fake videos or audio recordings of political figures. This can potentially influence public opinion, incite violence, or undermine democratic processes.

3.4.5. Identity Theft

Deepfake technology can be used to impersonate individuals, forging their identities for malicious purposes such as accessing sensitive information or committing financial fraud.

3.4.6. Disinformation Campaigns

Deepfake technology enables the creation of realistic-looking videos or audio recordings to spread false information, conspiracy theories, or propaganda, contributing to the erosion of trust in reliable sources of information.

3.4.7. Entertainment Industry Challenges

While deepfakes can have lots of positive applications in the entertainment industry, such as creating realistic special effects, they can also pose challenges. Deepfakes may infringe on intellectual property rights, misrepresent artists, or deceive audiences.

3.5. Most Targeted Countries and Field

In year 2021 sensity.ai released a report about most targeted countries and most targeted sector of deepfaking. They are

3.5.1. Most Targeted Countries

United States	**42.0%**
United Kingdom	10.3%
India	6.0%
South Korea	5.7%
Japan	5.6%
Others	30.5%

3.5.2. Most Targeted Fields

Entertainment	**55.9%**
Fashion	23.9%
Politics	4.6%
Sports	4.5%
others	11.1%

By considering the above reports, India is not purely on the safer side in deep-faking misuse. India needs to be alerted of the coming biggest world threat [16].

4. IMPORTANCE OF THE LAW AGAINST DEEPFAKE MISUSE

Laws against deepfake misuse play a crucial role in safeguarding individuals rights, protecting against defamation and fraud, maintaining trust in the media, ensuring public safety, and promoting responsible technology use. By establishing legal frameworks and consequences, these laws can contribute to mitigating the potential risks and harms associated with deepfake technology.

The below chart shows whether the border countries of India, including China, Bhutan, Nepal, Pakistan, Bangladesh, Myanmar, and Sri Lanka, have separate laws for cybercrime and deepfake misuse.

Country name	Separate Law for cybercrime	Separate law for Deepfake missue
China	Yes The Cyber Security Law of the People's Republic, commonly referred to as the Chinese Cyber Security Law, was enacted by the National People's Congress to increase data protection, data localization, and cyber security ostensibly in the interest of national security [13].	Yes
India	Yes (The IT Act 2000, which was passed and revised in 2008 to cover many types of offences under Indian cyber law, has been in effect since the establishment of cyber laws in India [14].	No
Pakistan	Yes (PECA Penalties) PECA imposes the punishments on cyber criminals for unauthorised access to key information systems, criminal has to pay a fine of one million Pakistani rupees, up to three years of prison or both[15].	No
Bhutan	No	No
Bangladesh	Yes (Procedural law) The main general framework available to all cybercrime investigations is embodied in the Bangladesh Information and Communication Technology (ICT) Act as also the Bangladesh Code of Criminal Procedure, 1898, and the Bangladesh Evidence Act, 1872 [15].	No
Myanmar	No	No
Sri Lanka	Yes Sri Lanka has passed into law the Cyber Crime Act 2007, which has made a number of the requisite articles offences within its jurisdiction. The Criminal Code, as amended by Amendment Acts No. 5 of 2005 and No. 22 of 2006, deals with s [15].	No
Nepal	Yes The Electronic Transactions Act of 2063 (2008) provides a legal framework to regulate electronic transactions and prevent cybercrime. The act includes provisions for punishing cybercriminals and protecting the rights of victims [15].	No

The above survey shows that different countries have several laws and policies to identify cybercrimes. However, in seven countries, only China has introduced a separate law for deepfake technology. The rest of the countries have yet to introduce separate laws. Our country, India, is currently focusing on bringing separate laws to regulate the deepfake misuse.

5. RECOMMENDATIONS TO CONTROL THE MISUSE OF DEEPFAKE TECHNOLOGY TO THE INDIAN GOVERNMENT BY RESEARCHERS

Some researchers provided recommendations for the Indian government to take some serious action in the following fields. Best of them are

5.1. Enact Specific Legislation

Developing specific legislation to address deepfake misuse is a commonly recommended approach. It should define deepfakes, establish prohibited activities, and outline penalties. This can be based on existing laws related to fraud, defamation, and privacy [5].

5.2. Collaborate With the Tech Industry

Collaboration with technology companies, research institutions, and experts is crucial. Engaging with these stakeholders can help to understand the challenges posed by deepfakes and develop effective countermeasures safeguard our country from deepfake misuse threat [6].

5.3. Raise Public Awareness

Conducting public awareness campaigns is important to educate citizens about deepfake technology misuse can be happen with any individua , their potential risks, and how to identify and respond to them. Promoting media literacy and critical thinking skills is crucial [7].

5.4. Strengthen Law Enforcement Capacities

Providing law enforcement agencies with resources, training, and tools is essential for effectively investigating and prosecuting deepfake-related offences. Building expertise in digital forensics and international collaboration is recommended [8].

5.5. Foster International Cooperation

Collaborating with other countries to address the global challenges posed by deepfake news is crucial. Sharing experiences, best practises, and legislative approaches can help develop a coordinated response [9].

6. CONCLUSION

In Conclusion, the comparative study on laws and actions taken in border countries of India regarding the misuse of deepfake technology highlights the importance of addressing this issue. Deepake technology has the potential to cause harm if misused, and it is crucial for governments to be proactive in combating its negative effects. A country like China has recognised the threats posed by deepfakes and has implemented laws criminalising their creation and dissemination for malicious purposes. China also established specialised task forces to monitor and investigate deepfake-related crimes and conducted public awareness campaigns to educate citizens about the risks associated with deepfakes. The study provides valuable insights for the Indian government, emphasising the need to enact comprehensive legislation, establish specialised task forces, and promote public awareness to

effectively address the misuse of deepfake technology.

7. REFERENCES

[1] Doe, J., & Johnson, A. (2019). Industry self-regulation in combating deepfakes: A comparative analysis of the United Kingdom and the United States. Journal of Digital Media Policy, 10(3), 278-295.

[2] Johnson, R., & Lee, S. (2021). Admissibility of deepfakes as evidence: A review of court decisions and implications for legal proceedings. Journal of Law and Technology, 25(2), 231-254.

[3] Li, H., et al. (2022). Deepfake detection: Current techniques and challenges. IEEE Transactions on Information Forensics and Security, 17(3), 650-670.

[4] Smith, T., et al. (2020). Comparative analysis of deepfake related laws in the United States, European Union, and China. International Journal of Law and Information Technology, 28(1), 45-73.

[5] Center for Internet and Society (CIS) India, "Deepfakes and the Law in India" [https://cis-india.org/internet-governance/blog/deepfakes-and-the-law-in-india]

[6] Pew Research Center, "Deepfakes, Synthetic Media, and Misinformation" [https://www.pewresearch.org/internet/2020/02/06/deepfakes-synthetic-media-and-misinformation/]

[7] Data & Society, "Deepfakes and Synthetic Media in the Financial System" [https://datasociety.net/library/deepfakes-and-synthetic-media-in-the-financial-system/]

[8] Carnegie Endowment for International Peace, "Deepfakes and International Security" [https://carnegieendowment.org/2019/06/12/deepfakes-and-international-security-pub-79268].

[9] Brookings Institution, "Deepfakes and the New Disinformation War" [https://www.brookings.edu/research/deepfakes-and-the-new-disinformation-war/].

[10] Shruti Agarwal, Hany Farid, Yuming Gu, Mingming He, Koki Nagano, and Hao Li. Protecting world leaders against deep fakes. In Computer Vision and Pattern Recognition Workshops, volume 1, pages 38–45, 2019.

[11] Thanh Thi Nguyena , Quoc Viet Hung Nguyenb , Dung Tien Nguyena , Duc Thanh Nguyena , Thien Huynh-Thec , Saeid Nahavandid , Thanh Tam Nguyene , Quoc-Viet Phamf , Cuong M. Nguyeng “Deep Learning for Deepfakes Creation and Detection: A Survey”,[2022].

[13] Cybersecurity Law of the peoples republic of China new paper books scholar JSTOR (August 2021).

[14] Patil Jatin, Cyber Laws in India: An Overview (March 3, 2022). Indian Journal of Law and Legal Research, 4(01), pp. 1391-1411.

[15] Council of Europe “ CyberCrime policies/Strategis” Asset Publisher - Octopus Cybercrime Community (coe.int).

[16] Eric Hofesmann The State of Deepfakes in 2020 November 19, 2020.