DEEPFAKES IN INDIA: LEGAL GAPS UNDER BNS AND THE IT ACT 2000

Anushka Adhikari*

ABSTRACT

The rapid development of deepfake technology has emerged as a serious challenge to privacy, electoral integrity, financial security, and public trust. Deepfakes, which use artificial intelligence to create highly realistic but manipulated images, videos, and audio, can be misused for fraud, misinformation, impersonation, blackmail, and reputational harm. Despite the growing risks associated with such technology, India presently does not have a dedicated legislative framework specifically regulating artificial intelligence and deepfakes. The existing legal framework, primarily comprising the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, relies largely on provisions designed to address conventional forms of cheating, forgery, identity theft, and online misconduct and does not comprehensively address the distinctive challenges posed by AI-generated content.

This paper critically examines the adequacy of India's existing legal framework in addressing deepfake-related harms and identifies the principal regulatory and enforcement gaps. It further analyses the emerging regulatory framework, including the Information Technology Rules, 2026, with a focus on their ability to address the creation, dissemination, and misuse of synthetic media. To provide a comparative perspective, the paper examines approaches adopted in the United Kingdom and the United States towards AI-generated content and deepfake-related harms. The comparative analysis highlights the strengths and limitations of India's present approach and the need for greater clarity regarding liability, platform responsibility, consent, content authentication, and effective remedies for victims. The paper argues that India's existing laws, while capable of addressing certain instances of deepfake misuse, remain fragmented and insufficient to comprehensively regulate the evolving risks associated with synthetic media. It therefore proposes the enactment of a dedicated AI and

*LLB, FIRST YEAR, ASIAN LAW COLLEGE, CCS UNIVERSITY, UTTAR PRADESH.

Deepfake Regulation Act establishing a clear, technology-neutral, rights-based, and enforceable framework for prevention, accountability, detection, and redressal of deepfake-related harms in India.

Keywords: Deepfakes, BNS, IT Act, Cybercrime, Fake Videos, AI Law, Privacy.

INTRODUCTION

In 2023, a fake video involving actress Rashmika Mandanna showed how dangerous deepfakes can be. In that video, her face was put on someone else's body using AI. The video looked so real that most people believed it was true. After this, the government had to send strict warnings to Instagram, YouTube and other apps. The government said that if they did not remove such fake videos quickly, they would lose legal protection.

After that, in 2024, during elections, fake videos of politicians also came. One fake video involving actor Ranveer Singh was also shared. These cases showed that AI is not a future problem. It is a problem today. Now India has replaced the old IPC, 1860, with the Bharatiya Nyaya Sanhita, 2023. But the big question is: Can BNS and the old IT Act, 2000 stop AI crimes? Or are we trying to solve a new digital problem with old rules? This paper explains what deepfakes are, what laws we have now, what problems are there, and what India can learn from other countries.

WHAT ARE DEEPFAKES AND HOW DO THEY WORK?

Most deepfakes are made using something called GAN. GAN means two computer programs work against each other. One program makes the fake video. The other program checks if it looks real. After doing this millions of times, the fake video becomes so real that normal people cannot tell the difference.

Main Types of Bad Use of Deepfakes –

Voice Cloning and Money Scams: With just 3 seconds of someone's voice, AI can copy it. Scammers call people and act like their son or daughter is in trouble. They ask for money on UPI urgently. Many old people have lost money like this.

Fake Political Videos: During elections, people make fake videos of leaders saying bad things. One video can spread in 10 minutes and change how people vote. This can create fights and confusion.

Fake Porn and Private Videos: This is the worst use. Someone takes a girl's photo from Instagram and puts her face on a porn video. 90% of deepfakes on the internet are like this, and most victims are women. Victims go through a lot of mental trauma, and their reputation also gets damaged.

WHAT LAWS DO WE HAVE IN INDIA RIGHT NOW?

India does not have one law for AI. So, Police use different sections from the BNS and the IT Act together.

Bharatiya Nyaya Sanhita, 2023 (BNS): BNS replaced IPC. It has some new words about "electronic records", but it does not mention "AI" or "deepfake" anywhere. So, police have to use old sections in new ways.

Offense	IPC/BNS	How it is used for Deepfakes?
Cheating by Personation	419 / 319	When someone uses AI voice or fake video to act like another person and cheat
Cheating	420 / 318	When fake video is used to make someone transfer money
Forgery	463/464 / 336/340	Deepfake is treated as "false electronic record"
Criminal Defamation	499/500 / 356	When fake video is made to spoil someone's name

Also, Section 228 BNS can be used if a fake video is shown in court as proof. Section 77 BNS can be used for fake private videos of women.

Information Technology Act, 2000 (IT Act) –

Section 66C - Identity Theft: Punishes using someone else's password, signature or biometric. Lawyers now argue that face and voice are also "identity features".

Section 66D - Cheating by Computer: Punishes using a computer or phone to cheat by acting like someone else. Jail up to 3 years and fine up to 1 lakh. This is used a lot for AI scam calls.

Section 66E - Privacy Breach: Punishes sharing private photos without permission. Now courts also use it for fake nude videos made by AI.

Section 67 and 67A - Obscene Content: Used against deepfake porn. Section 67A gives jail up to 5 years.

Rules for Social Media Companies –

Under Section 79 of the IT Act, companies like Meta, X, and YouTube get "safe harbour". It means they are not responsible for what users post, unless the government tells them to remove it. But after the Rashmika case, rules became strict. The Supreme Court in K.S. Puttaswamy (2017) said privacy is a fundamental right. Now we have IT Intermediary Guidelines Amendment Rules, 2026. These new rules say companies must remove deepfake content very fast. If they don't, they can lose protection.

WHAT ARE THE BIG PROBLEMS IN CURRENT LAW?

Even with BNS, the IT Act and 2026 Rules, there are 4 big gaps.

No Definition of "Deepfake" or "AI" in Law: BNS does not have the words "AI" or "deepfake". Police have to force old words like "forgery" to fit new technology. Under Section 336 of BNS, forgery means making a "false document" to cheat. But what if someone makes a funny political parody video with no plan to cheat? Then forgery is hard to prove. The law only works after damage is done. It cannot stop the crime before it happens.

Problem of Proof in Court: Now we have Bharatiya Sakshya Adhiniyam 2023 instead of the Evidence Act. Section 63 BSA talks about electronic proof. To prove a video is fake, police

must show it in court. For that, they need forensic labs to check things like: does the person blink normally? Are shadows correct? But Indian FSL labs have too much work and not enough AI tools. So, proving "this video is AI-made" becomes very hard. Cases get stuck for years.

Who is Guilty: Creator, Platform or Person Sharing? On WhatsApp, one fake video can reach 1 million people in 1 hour. Under BNS, to punish someone, we must prove "mens rea" = guilty mind. But if a normal person forwards a fake video thinking it is real, he did not plan to cheat. Still, he helped spread it. Law does not clearly say: who is more guilty - the person who made it, the app that hosted it, or the person who forwarded it?

Problem of Other Countries: AI tools are free on the internet. A person sitting in the USA or Russia can make a deepfake of an Indian and upload it from another country. Section 75 of the IT Act says Indian law applies if a computer in India is used. But to catch the foreign person, police need MLAT - a long government process between countries. By the time that happens, the damage is already done.

IMPACT OF DEEPFAKES ON COMMON PEOPLE AND STUDENT LIFE

Deepfakes do not only affect celebrities and politicians. Common people and students are also getting trapped.

Problem for Students: Today, most students use Instagram, Snapchat and YouTube. Anyone can take a student's photo and make a fake video. In schools and colleges, some students are making fake videos of teachers or classmates to take revenge or for fun. Once such a video goes viral, the student's name gets spoiled. Even if police later prove it was fake, the shame and bullying do not stop. Many students feel depressed and stop coming to college.

Problem for Families: Scammers are using AI voice to call parents. They copy the voice of the child and say, "Mummy, I am in the police station; send 50,000 on UPI fast". Because the voice sounds real, many parents get scared and send money. After that the number gets switched off. This is happening a lot in small towns.

Problem of Trust: The biggest damage is that now people do not believe real videos also. If a girl posts proof of harassment, people say "maybe it is deepfake". If a news channel shows a leader's speech, people say "maybe it is AI". This means truth and lies look the same.

So, deepfakes are not just a tech problem. They are breaking trust between people. That is why we need laws + awareness together. Schools should teach students about digital safety and how to check if a video is real or fake. Digital evidence to prove crime is important.

ROLE OF SOCIAL MEDIA COMPANIES IN STOPPING DEEPFAKES

Social media apps like Instagram, YouTube, Facebook and X are where most deepfakes spread first. So, these companies also have a big duty.

Fast Removal of Fake Videos: Right now, by the time a company removes a fake video, it already gets 10 lakh views. The 2026 IT Rules say companies must take down deepfakes within 36 hours of complaint. But this is still slow. Companies should use AI tools to detect fake videos on their own and remove them in 2-3 hours.

Label and Watermark System: Every AI-generated video should have a clear tag like "AI Generated". Some apps like Instagram have started this, but most Indian apps don't do it. If people see a label, they will be careful before believing or sharing it.

Reporting and Help for Victims: Today, if a girl's fake video is posted, it is very hard to get it removed. She has to fill out 5-6 forms and wait for days. Companies should make one simple "Report Deepfake" button. They should also give free legal and counselling help to victims, because many people get depressed.

Ban Repeat Offenders: People who keep making and posting deepfakes should be permanently banned. Also, companies should share data with police when a serious crime happens.

Social media companies make crores from ads, so they must also spend money to keep users safe. Safe harbour protection should only be given if they do their job properly. Otherwise, they are also responsible.

SUGGESTIONS: WHAT INDIA SHOULD DO?

The problem of deepfakes is new, so our solutions also have to be new. Just using old BNS and IT Act sections is not enough.

Clear Definition First: The first step is to define "Deepfake" and "AI Content" in law. Right now, police are confused about which section to use. If BNS has a clear definition, then filing cases will become easy and fast.

Special Cyber Police Cells: Every district should have a small cyber cell with 2-3 people trained in AI. When someone complains about a fake video, this cell should immediately check it and send it to FSL. Right now, common police stations don't even know how to save WhatsApp proof.

Liability for AI App Companies: Companies that make free AI apps should be forced to add safety checks. Like asking for ID before making a person's face, or blocking nude generation. If they don't do this, they should also be fined.

Public Awareness Campaign: Government should run ads on TV and YouTube: "Don't believe everything you see". Banks, schools and RWAs should do workshops. Most parents and old people don't know that AI voice calls are fake. I think awareness is a way to stop deepfakes. The government should make strict rules for this.

Fast Takedown + Compensation: Social media platforms should remove deepfakes in 24 hours. If they fail, they should pay compensation to the victim. Also, courts should give quick interim orders to delete content, as they do in defamation cases.

If we mix strict law + technology + awareness, we can control deepfakes without stopping real innovation.

CONCLUSION

Deepfakes are a big danger to privacy and democracy in India. The Rashmika and election cases showed how fast one fake video can spread. Right now, we use BNS and the IT Act to fight AI crimes, but these laws are old and not made for AI. The 2026 IT Rules are good but not enough. India needs a separate AI law like the UK has. We must define deepfake, fix proof problems, and train police. Only then can we protect people's dignity and also keep the internet free. Law must be fast, clear and ready for the AI age.

REFERENCES

1. Rashmika Mandanna Deepfake Incident, Government Advisory (2023)

2. Bharatiya Nyaya Sanhita 2023, section 77
3. Bharatiya Nyaya Sanhita 2023, Section 318
4. Bharatiya Nyaya Sanhita 2023, section 319
5. Bharatiya Nyaya Sanhita 2023, section 336
6. Bharatiya Nyaya Sanhita 2023, section 356
7. Information Technology Act 2000, section 66C
8. Information Technology Act 2000, section 66D
9. Information Technology Act 2000, Section 66E
10. Information Technology Act 2000, section 67A
11. Information Technology Act 2000, Section 79
12. Information Technology Intermediary Guidelines Amendment Rules 2026
13. K.S. Puttaswamy v Union of India (2017) 10 SCC 1