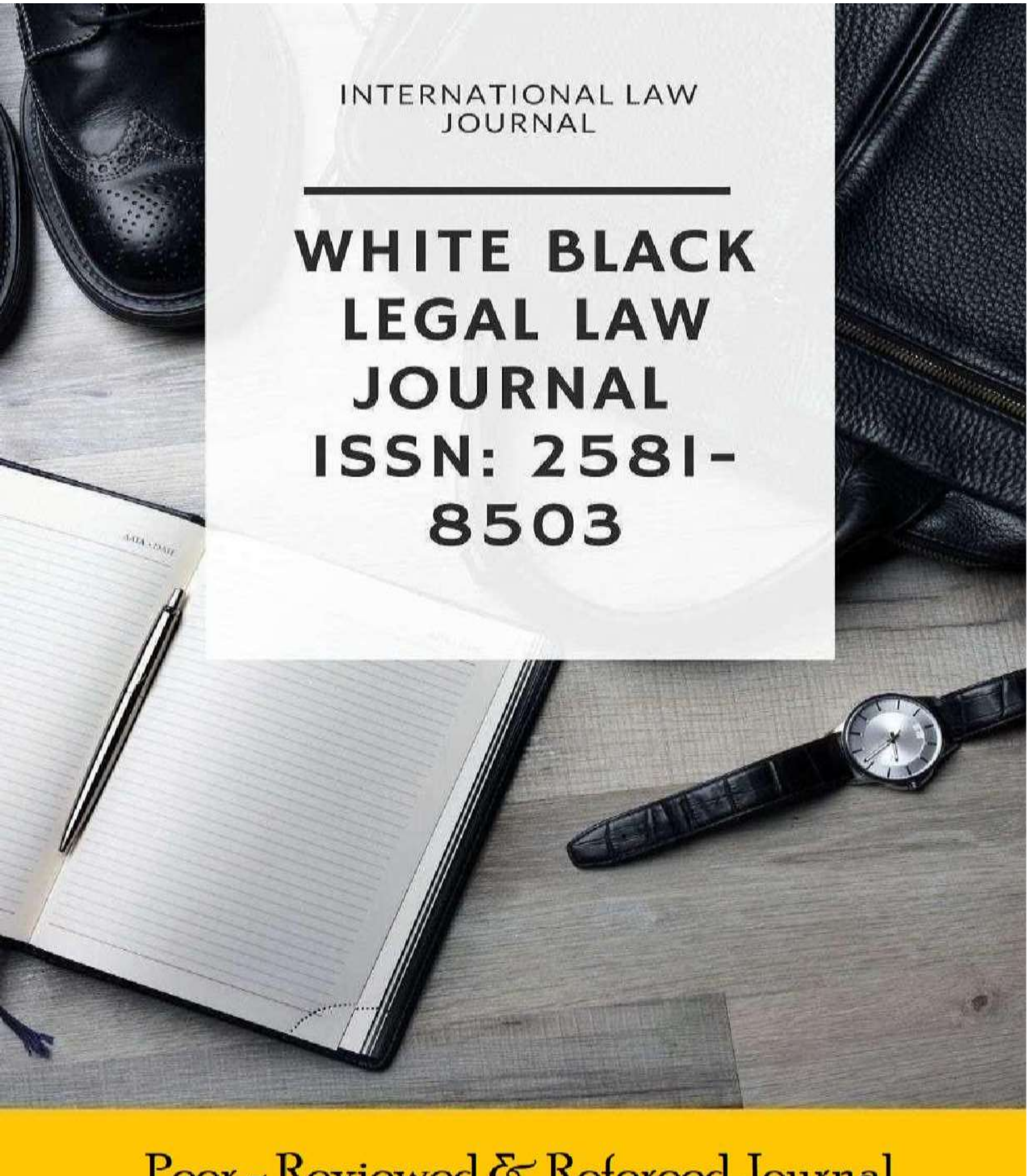

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

TRUTH ON TRIALS: DEEPFAKES AND THE LAW

AUTHORED BY - KIRTI NAGAR & CHESHTHA AGRAWAL

Abstract

AI: An Existential Risk to Humanity

Artificial intelligence has come up as one of the most changing technologies around. It also seems pretty dangerous in ways we did not expect. Elon Musk keeps warning people that AI could really threaten human civilization in a big way. The thing is, by the time we get regulations in place, it might already be too late to stop the problems.

Geoffrey Hinton, who people call the godfather of AI, is a computer scientist and Nobel winner. He has shared similar worries too. He figures there is a 10 to 20 percent chance that AI might wipe out humans in the next thirty years or so[1]. What stands out as scary here is that even the experts who built this stuff feel regret now. They understand how it works inside out, yet they fear what they let loose.

Musk and Hinton along with other top scientists keep saying AI could bring deep risks to society and people in general. Machines that think and learn like us do that, but they do it quicker and more precise without any feelings getting in the way. Over time, they might beat us at everything we do. The real trouble is not just that AI takes over. It is more about how we depend on it so much that we lose grip. As it gets stronger, our control slips away. That could lead to society falling apart, not because AI plans it, but because we hand over the reins without much fight.

One of the worst parts from all this progress is how deepfakes are rising up. They are fake media made by AI that can twist the truth right at its core.

Keyword: AI, Threat to human civilization, Deepfakes, Fake media, Misinformation, Ethics, Humanity, Future.

[1] Cade Metz, *Geoffrey Hinton Quits Google and Warns of AI Dangers*, N.Y. Times (May 1, 2023).

Deepfakes and Digital Deception: The Need for Legislative Safeguards

Introduction: What Are Deepfakes

The Existential Risk of Artificial Intelligence and the Rise of Deepfakes

"The biggest risk we face as a civilization is artificial intelligence.[2]" – Elon Musk

Deepfakes come from AI that uses deep learning and machine learning to make synthetic media. This lets people change audio, pictures, and videos so folks look like they say or do stuff they never really did. The tech looks at faces, voices, and how bodies move to swap heads or tweak words. It can even build whole made-up scenes that feel totally real.

Sure, this sounds like a cool invention. Still, it brings up big issues with privacy getting broken, wrong info spreading, and crimes online. In India, we lean on things like the IT Act, Cybercrime Guidelines, and the Bharatiya Nyaya Sanhita to handle these problems. The catch is, without a clear law just for deepfakes, it gets hard to catch and punish the bad actors.

We see real examples that show just how bad this can get.

Back in the 2020 U.S. Presidential Election[3], fake videos of leaders popped up. One had Barack Obama in a deepfake that tricked voters with lies.

Then there was that viral deepfake of Tom Cruise on social media. It made it tough to tell what was real from what was not.[4]

Types of Deepfakes:

1. **Face swapped videos**: The face of one subject is superimposed over the moving body of another in the most well-known kind of face-swapped video. Neural nets can detect facial expressions and match them frame by frame to create realistic illusions. Some of these deepfake movies are funny memes, but others are dangerous lies that can ruin reputations. Even the most astute observers without advanced detection methods may find high-fidelity detail confusing.

2. **Lip-synchronized audio overlays:** Lip-sync fakes, also referred to as puppeteering, use mouth movements to simulate altered or synthetic audio. The result? The words

[2] Elon Musk, Interview with MIT Aeronautics & Astronautics (Oct. 24, 2014).

[3] https://r.search.yahoo.com/_ylt=AwrKANmazPRo9wEAx4i7HAx.;_ylu=Y29sbwNzZzMEcG9zAzEEdnRpZAMEc2VjA3Ny/RV=2/RE=1762083227/RO=10/RU=https%3a%2f%2fwww.techtarget.com%2fsearchenterpriseai%2ffeature%2fThe-deepfake-2020-election-threat-is-real-but-containable/RK=2/RS=leds4bEodXpmFVUptaKjpm.nQ5g-

[4] Chris Stokel-Walker, *Tom Cruise Deepfakes Are the Beginning of a New Internet Era*, Wired (Mar. 2021).

seem to be addressed to a speaker, but they are never. When paired with voice cloning, the face in the clip can effectively perform entire screenplays.

3. **Voice-Only Cloning:** The only foundation of audio deepfakes is the imitation of the AI voice in the absence of images. Fraudsters use them in phone scams, such as posing as executives to control urgent wire transfers. For marketing purposes, some will produce voiceovers for celebrity cameos. Because it lacks visual cues and necessitates sophisticated spectral analysis or dubious context triggers, identifying this kind of deepfake is challenging.

4. **Complete Body Reenactment:** Generative models are able to map an actor's entire body language, gestures, and posture onto another person. As a result, the subject appears to be dancing, participating in sports, or carrying out activities they have never done. Full-body illusions are required for AR or film experiences. However, the potential for creating alibi videos or staged evidence is what deepfake cybersecurity is most concerned about.

5. **Conversational Clones Based on Text:** Generative text systems mimic a person's writing or conversational style, though they are not as frequently called deepfakes. Cybercriminals copy the language and writing style of the user to create new message threads. A multi-level fake or even a complete deepfake character can be produced by adding the voice or image to the illusion. It is predictable that as text-based generative AI becomes more sophisticated, it will be employed in social engineering schemes via messaging platforms rather than just image forgeries.

Risks Arising from Deepfake Technologies

Deepfake as a Threat

Deepfake technology presents serious risks in a number of fields. Deepfakes can propagate false information and affect political outcomes by producing realistic-looking but phony audio and video content. By facilitating complex social engineering, deepfakes have the potential to jeopardize private data kept in Critical Information Systems (CIS). The sections that follow go over a few areas where deepfakes can be extremely problematic.

Threat to Political Stability

One of the biggest risks posed by deepfakes in India is political stability. The political climate in Bharat is marked by extreme polarization and fierce election rivalry. Deepfakes can be used as a weapon in such a setting to discredit political rivals, disseminate false information, and sway public opinion. Fake films of political figures making divisive remarks, for instance, have the potential to provoke violence, sabotage elections, or erode public confidence in democratic institutions.

These videos can be quickly shared on social media, which increases the danger because misleading information can spread to millions of people before it can be refuted. To target particular voter groups, a political party was observed employing deepfake technology to produce recordings of a leader giving speeches in various languages during the 2020 Delhi elections[5]. Despite their lack of malevolent intent, these videos raised worries about the possible misuse of deepfakes by highlighting how they could be used for political ends.

Threat to Social Cohesion and Communal Harmony

Bharat is a multi-religious, multi-lingual, and multi-cultural country. The task of preserving communal peace and social cohesion never goes away. By producing phony videos that seem to depict members of one community attacking another, deepfakes can be used to inflame tensions across communities. As demonstrated by less sophisticated misinformation, particularly that pertaining to the Citizenship Amendment Act (CAA) and its associated aspects, which led to a law-and-order issue in Delhi in February 2020, such content can spread rapidly and spark violence and rioting[6]. The psychological impact of seeing false evidence of attacks or any impactful information can be reflective, making it difficult to quell unrest once it has started.

Threat to National Security and Defence

A deepfake video purporting to show Ukrainian President Volodymyr Zelensky telling Ukrainians that their army had surrendered surfaced on February 18, 2022[7]. President Zelensky's deepfake exposed how deepfake technology can be used to spread false information during a military war and compromise media outlets. Deepfakes can also be used in psychological operations to transmit misleading orders, demoralize soldiers, or cause confusion

[5] Prabhash K. Dutta, *How Deepfakes Entered Indian Elections*, India Today (Feb. 2020).
[6] Ministry of Home Affairs, Govt. of India, *Delhi Riots Status Report* (2020).
[7] BBC News, *Deepfake Video of Zelenskyy Surrender Circulates Online* (Mar. 17, 2022).

among the ranks. A deepfake film depicting a senior military officer giving up or giving a fraudulent order, for example, might have disastrous effects on military morale and operational efficacy. Deepfakes could be used to fabricate stories or sway diplomatic interactions, which could affect a nation's ties with other countries.

Other Damages

1. Democratic Damage

Fake videos can push people one way or another in their views. They spread stories that are not true and stir up fights, mostly around election time. This stuff plays on feelings about culture and politics, which hurts how democracy works overall.

The Indian Constitution in Article 19(2) lets limits on free speech for reasons like keeping the country safe or public calm or morals. Deepfakes slip past those rules though. They turn into new ways to push propaganda.

In 2020, during campaigns with big Indian leaders, AI deepfakes showed up. They twisted talks and made folks doubt what they saw online.

2. Gendered Abuse

Deepfakes turn into weapons for hurting people sexually and through gender attacks. Women get hit the hardest most times. Bad guys grab photos and clips from social sites to make porn without anyone agreeing. They use it to get money or force victims into things.

The National Cyber Crime Reporting Portal saw complaints jump in 2025[8]. Over 90 percent of deepfakes worldwide are porn like this, and India sees the same pattern[9]. It does not stop at breaking privacy. Victims deal with mind damage, lost reputation, and sometimes thoughts of ending it all.

3. Erosion of Trust in Media

Deepfakes mix up what is real and what is made up so much that trust in news drops off. Both old school media and online stuff suffer. When fake clips of leaders or stars go everywhere, people start questioning even the true ones. This doubt spreads wrong info further. It hurts reporters and makes it hard to hold power accountable in democracy.

[8] National Cyber Crime Reporting Portal, Govt. of India, Annual Report (2024–25).

[9] Sensity AI, *State of Deepfakes Report* (2023).

4. Financial Risks

Deepfakes open doors to money scams too. Crooks clone voices with AI to sound like family in trouble. They ask for quick cash help. These tricks lead to lost money for sure. They also break faith in calls and messages online. It shows how tech can hit right at our soft spots like worry for loved ones.

5. Legal Challenges in India

India faces this growing problem without a law aimed right at deepfakes. The rules we have help some, but they fall short in key spots.

6. No Clear Legal Definition

Indian laws do not clearly define what counts as a deepfake. While acts like the IT Act, 2000[10], and the Bharatiya Nyaya Sanhita touch on cybercrime and identity misuse, none directly address AI-generated fake media. This leaves a grey area when deciding whether a manipulated video or image is defamation, forgery, or just satire.

Without a legal definition, enforcement becomes patchy. Victims find it hard to prove harm, and platforms struggle to decide what content to remove. A clear legal meaning would help set boundaries between creative use of AI and harmful manipulation, giving courts and police a stronger base to act quickly and fairly.

7. Authentication Challenges

Section 65B of the Indian Evidence Act[11] deals with proving digital evidence in court. Deepfakes make that much harder. Since AI-generated media can look almost identical to real footage, it becomes tough to show what's authentic and what's fake.

Even digital forensics experts can't always catch subtle edits. This weakens confidence in online proof from videos of crimes to political speeches. To tackle this, India needs better forensic tools, digital watermarking systems, and clearer rules for verifying electronic evidence in the age of AI.

8. Lack of Precedents

Deepfake-related cases are still new in India, so there are few legal precedents to guide judges. Each case ends up being treated differently, as courts must first understand how

[10] Information Technology Act, 2000, India Code.
[11] Indian Evidence Act, 1872, § 65B.

the technology works before applying existing laws. This slows down justice and leaves victims uncertain about where they stand.

Judgments like *Chaitanya Rohilla vs. Union of India* and *Khairati Lal vs. State*[12] have started shaping direction, but a consistent body of rulings is still missing. Building more precedents will help create clearer standards and faster decisions in the future.

9. **Cross-Border Barriers**

Most deepfakes originate or circulate through servers outside India. Tracking and punishing offenders becomes difficult since Indian law stops at its borders. Even when culprits are identified abroad, the process of cooperation through international treaties is long and complex.

This shows the need for stronger global coordination on cyber laws and AI misuse. India should work with other nations to share data, standardize rules, and speed up responses to cross-border digital crimes.

Key Case Laws on Deepfakes[13]

- **May 2025:** The Supreme Court looked at a viral deepfake of a military officer and said lawmakers need to step up with rules.
- **Abhishek Bachchan and Aishwarya Rai v. Google & YouTube:** They sued for four crore rupees over deepfake content used without permission.
- **Chaitanya Rohilla v. Union of India:** The Delhi High Court pushed for government rules on AI and deepfakes to stop privacy breaks.
- **Anil Kapoor and Amitabh Bachchan:** Got court orders to block misuse of their images, stressing protection of names and faces.
- **Justice K.S. Puttaswamy v. Union of India (2017):** Set privacy as a basic right, meaning deepfakes without consent go against the Constitution.
- **Shreya Singhal v. Union of India (2015):** Backed free speech limits for impersonation or public harm, fitting deepfake lies well.
- **Khairati Lal v. State (2023):** The Delhi High Court faced a deepfake porn case, showing how missing laws delay justice.

[12] Chaitanya Rohilla v. Union of India, W.P. (C) No. 8918/2020 (Del. HC).

[13] https://r.search.yahoo.com/_ylt=AwrKAzs3z_RoAgIAqbe7HAx.;_ylu=Y29sbwNzZzMEcG9zAzMEdnRpZAMEc2VjA3Ny/RV=2/RE=1762083896/RO=10/RU=https%3a%2f%2flawfullegal.in%2fthe-legal-framework-of-deepfake-technology-in-india-challenges-implications-and-the-need-for-regulation%2f/RK=2/RS=JHCVRsbMd.vTUfY5kqgsLicqiOQ-

- Celebrities like **Rashmika Mandanna and Alia Bhatt** were victims of non-consensual deepfake pornographic content, prompting public outrage and legal debate.

Comparative Legal Perspective[14]

Though the situation shows alarming trends throughout the world, we have countries such as US, UK who have taken progressive steps in order to eradicate the issue.

In the **United States**, places like California and Texas passed rules against deepfake porn without consent and lies in politics.

The **European Union** has the **GDPR**, **Digital Services Act**, and a coming **AI Act**. These push for clear labels on fake media and openness.

The **United Kingdom** relies on laws like the **Malicious Communications Act** and the **2023 Online Safety Act** to fight deepfakes.

India can learn from these spots around the world. Our **IT Rules** and **Bharatiya Nyaya Sanhita** show some steps forward. Still, we need laws made just for us, thinking about our mix of people, politics, and how lies spread here.

Suggestions and Conclusion

Although there are no laws or regulations that specifically address the problem of deepfake content, the Information Technology Act of 2000's Sections 66D (Punishment for cheating by personation by using computer resources) and 66E[15] (Punishment for violation of privacy) stipulate that anyone who impersonates another person and publishes or transmits images of private body parts in an electronic format without that person's consent faces imprisonment and a fine. To detect and stop the spread of deepfake information online, these IT Act measures are insufficient. Ashwini Vaishnav, the Minister of Electronics and IT, met with representatives from industry, academia, and social media companies on November 23, 2023, to talk about the necessity of a successful response.[16]

[14] https://lawarticle.in/deepfakes-in-india-a-legal-analysis-of-emerging-challenges-and-regulatory-framework/#6_Comparative_Legal_Perspectives

[15] Information Technology Act, No. 21 of 2000, §§ 66D, 66E, India Code.

[16] https://www.vifindia.org/article/2024/july/11/Deepfakes-A-Threat-to-National-Security-in-the-Digital-Era

With the potential to upend political stability, erode social cohesiveness, affect national defense, and destabilize the economy, deepfakes pose a serious and constantly changing threat to Bharat's national security, demanding an aggressive and all-encompassing response. Given the rapid advancement of deepfake technology, it is easy to forecast that it will become increasingly difficult to believe political leaders' videos in the future. Two years after the 2018 Parkland tragedy, a deepfake video of Joaquin Oliver, one of the kids killed, was created. One of the most notable instances is when a deceased individual was able to be brought back to life using deepfake technology, and he addressed lawmakers about the issue of gun violence in the United States.

India should tackle deepfake dangers with layers of fixes, mixing rules, tech, and teaching folks.

- Update the IT Act to cover deepfake crimes straight on.
- Make platforms take real blame for spotting and pulling fake content fast.
- Start drives to teach people about online smarts and spotting lies.
- Set up a group just to watch if rules get followed.
- Work with other countries to handle cases that cross borders.

On a personal side, everyone needs to watch what they take in and put out online. Check wild videos twice, look at sources from different places, and keep your own stuff from easy grabs. Deepfakes can help in fun like movies or making things easier for some. Without controls though, they hit hard at private lives, fair votes, and what we know as true. Tech keeps changing, so our sense of right, smarts, and laws have to keep up too.

The path for AI, if it helps us rise or brings us down, rests on how we guide it with care.