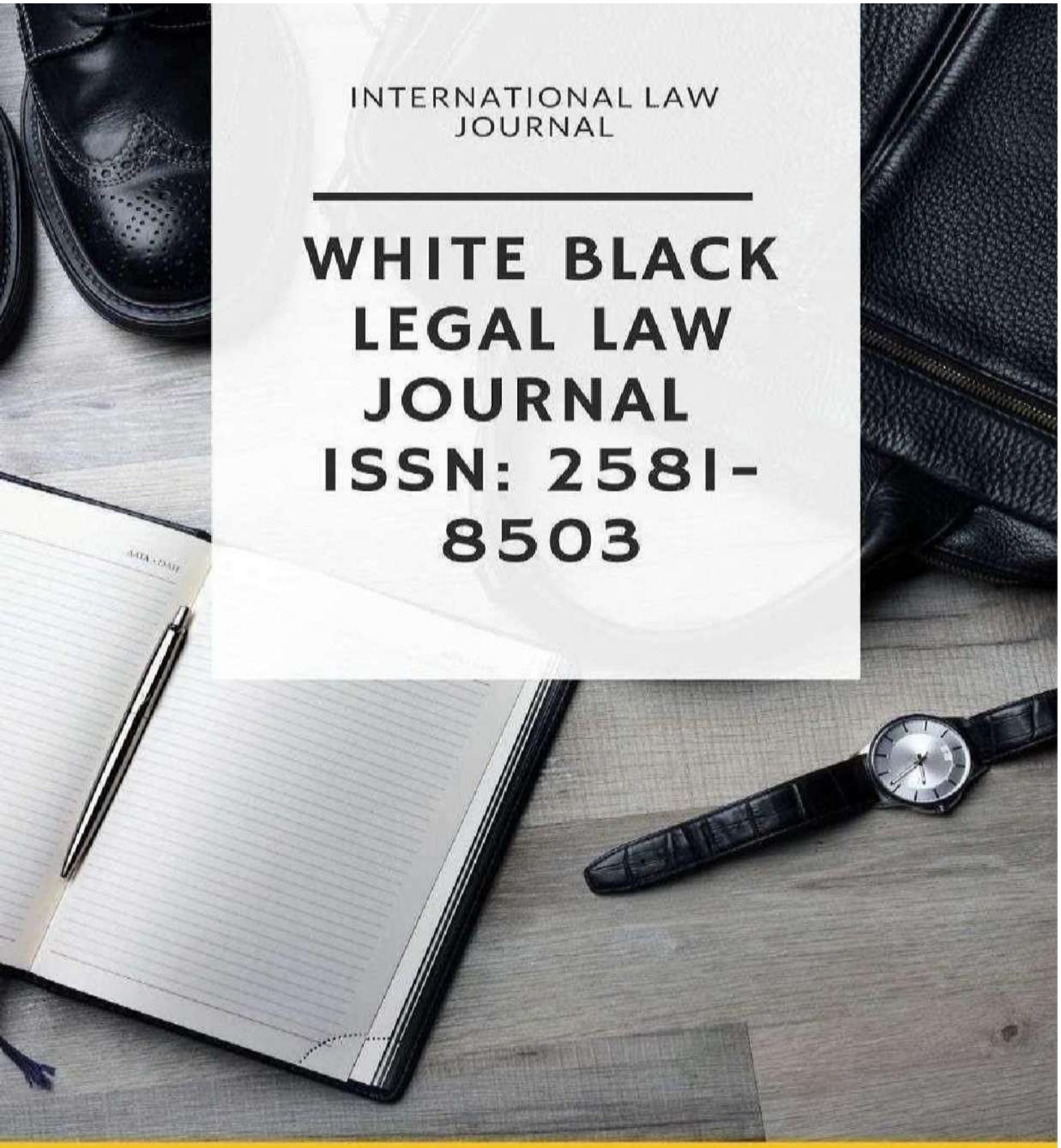

INTERNATIONAL LAW JOURNAL

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

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

AI-GENERATED DEEPFAKE FRAUD: A GROWING THREAT TO DIGITAL TRUST IN INDIA

AUTHORED BY- AKHITHA TAJY
LLM SCHOLAR,
CSI College For Legal Studies, Kanakkary, Kottayam.
Affiliated Under Mahatma Gandhi University, Kerala.

Abstract

Artificial intelligence (AI) has transformed digital communication, governance, commerce, and social interaction in India. However, this technological progress has introduced a new threat: AI-generated deepfake fraud. Deepfakes synthetic audio, video, or images created using advanced machine learning are increasingly used for financial fraud, corporate deception, political manipulation, and gender-based cybercrime. The rise of generative AI tools, combined with India's massive digital population, extensive mobile payments adoption, and low digital literacy, has made the country highly susceptible. This article examines the technological foundations of deepfakes, the various types of deepfake fraud prevalent in India, the vulnerabilities in India's digital ecosystem, the social, economic, and political impacts, and the legal challenges in regulating such crimes. It also explores international frameworks and offers a comprehensive policy roadmap to safeguard digital trust in India.

1. INTRODUCTION

India has witnessed an unprecedented digital revolution over the past decade, encompassing online banking, e-governance, social media, and digital commerce. While this transformation has brought numerous benefits, it has also exposed Indian citizens and institutions to sophisticated forms of cybercrime. Among these, AI-generated deepfakes represent a particularly alarming threat because they blur the line between reality and fabrication. Unlike traditional fraud, which relies on stolen information, deepfakes allow criminals to fabricate identities convincingly, manipulate speech and video, and exploit human trust at scale.[1]

In recent years, Indian law enforcement agencies and CERT-In (Computer Emergency

[1] Pankaj Mishra, AI Scams Surge: Voice Cloning and Deepfake Threats Sweep India, NDTV (Oct. 10, 2024).

Response Team) have reported a surge in deepfake-enabled scams. Individuals have been targeted by phone calls replicating the voices of relatives or employers, compelling them to transfer funds immediately. Corporate executives have been impersonated through AI-generated video calls, directing employees to reveal confidential information or execute financial transactions. Political deepfakes have been circulated to influence elections and stoke communal tensions, while women and minors have been targeted with synthetic sexual content for blackmail and harassment.[2]

These incidents underscore the urgent need to address the threat posed by deepfakes. The erosion of digital trust the foundation of India's online ecosystem poses systemic risks to the financial sector, public governance, democratic processes, and societal cohesion. Without timely legal, technological, and institutional interventions, deepfakes could fundamentally undermine the credibility of information in India.

2. UNDERSTANDING DEEPFAKE TECHNOLOGY

Deepfakes are primarily generated through Generative Adversarial Networks (GANs) and diffusion models, which allow AI systems to learn patterns from large datasets of images, audio, or video. Once trained, these systems can synthesize highly realistic replicas of individuals, enabling a variety of manipulations.

Deepfakes can:

- Clone voices using less than 30 seconds of audio.
- Synchronize lip movements with arbitrary speech.
- Generate real-time synthetic video calls.
- Replicate facial expressions and body language.
- Circumvent biometric authentication in some cases.

Although deepfakes have legitimate applications in film, accessibility, education, and research, their misuse introduces profound risks. The core problem lies not in the technology itself, but in its ability to deceive individuals and institutions with content that appears authentic.[3]

[2] Cyber Con Held, Rs 2L Seized, Times of India (Dec. 2025).
[3] Indian Computer Emergency Response Team (CERT-In), Advisory on Deepfake Threats (2024).

3. FORMS OF DEEPFAKE FRAUD IN INDIA

Deepfake-enabled crimes in India manifest in multiple ways, each exploiting specific vulnerabilities in society and institutions.

3.1 VOICE-CLONING FINANCIAL SCAMS

Voice-cloning scams have become the most prevalent form of deepfake fraud in India. Criminals replicate the voices of family members, employers, or government officials to manipulate victims into transferring money for purported emergencies.[4] Victims often respond without verification due to the urgency conveyed by the AI-generated voice.

3.2 Impersonation of Public Officials

Fraudsters have created deepfake videos and audios impersonating IAS officers, police commissioners, and ministers. Such synthetic communications can:

- Demand money for fabricated legal actions.
- Direct citizens to submit sensitive documents.
- Issue fake government notifications.

The societal impact is severe, undermining public trust in institutions and creating confusion about authentic government directives.[5]

3.3 CORPORATE DEEPFAKE FRAUD

Corporate sectors are increasingly targeted by deepfake-enabled "CEO fraud." Fraudsters use AI-generated voices or videos of executives to instruct employees to transfer funds or share confidential data. INTERPOL has identified deepfake-based corporate fraud as one of the fastest-growing cybercrime categories globally.[6]

3.4 DEEPFAKE SEXTORTION

Deepfake sexual content, or synthetic pornography, is often used to extort victims. Criminals generate videos using ordinary images or social media content of women, minors, and public figures, threatening to release them unless ransom is paid.[7] This not only damages reputations but also inflicts severe psychological trauma on the victims.

[4] INTERPOL, Beyond Illusions: Synthetic Media and Crime (2024).
[5] DeepStrike, Deepfake Statistics 2025: AI Fraud Data & Trends (Sept. 2025).
[6] Digital Fraud: Cybercriminals Stole Rs 23,000 Crore from Indians in 2024, NDTV (Aug. 2, 2025).
[7] Ruchi Gupta, Synthetic Pornography and Sextortion in India, Indian Cyber Law Review (2024).

3.5 POLITICAL DEEPFAKES AND ELECTION MANIPULATION

India's electoral system is particularly vulnerable to deepfake misinformation. Fabricated videos of political leaders, manipulated speeches, and synthetic interviews have been used to sway public opinion and inflame communal tensions. The Election Commission has issued advisories, but controlling the rapid spread of deepfakes remains a challenge.[8]

4. FACTORS MAKING INDIA VULNERABLE

Several factors amplify India's vulnerability to deepfake fraud.

4.1 MASSIVE DIGITAL POPULATION

India is home to one of the world's largest social media and messaging platforms, including WhatsApp, Instagram, and YouTube. This creates a vast target ecosystem for cybercriminals.

4.2 HIGH DIGITAL PAYMENTS ADOPTION

With platforms like UPI enabling billions of monthly transactions, fraudsters exploit the immediacy of digital payments to execute scams efficiently.[9]

4.3 LOW DIGITAL LITERACY

Many users cannot distinguish between authentic and manipulated media. This widespread lack of awareness increases susceptibility to deepfake scams.

4.4 WEAK CYBER HYGIENE

Extensive sharing of personal photographs, voice notes, and videos online provides the raw material for training deepfake AI models.

4.5 PROLIFERATION OF EASY-TO-USE AI TOOLS

Free or inexpensive mobile apps now allow anyone to generate realistic deepfakes in minutes, lowering the barrier to cybercrime.[10]

[8] Election Commission of India, Guidelines on Digital Media and Deepfakes (2023).
[9] National Payments Corporation of India (NPCI), UPI Transaction Report (2025).
[10] Rahul Sinha, The Democratization of Deepfake Tools in India, Journal of Cybersecurity (2024).

5. IMPACT OF DEEPFAKE FRAUD ON SOCIETY

Deepfake fraud has profound social, economic, and political ramifications.

5.1 EROSION OF PUBLIC TRUST

Widespread deepfakes may lead citizens to question the authenticity of digital communication, reducing trust in media, government, and corporate institutions.[11]

5.2 FINANCIAL LOSSES

India reported over ₹23,000 crore in digital fraud losses in 2024, a significant portion involving AI-enabled scams.[12] Financial institutions, fintech companies, and individual victims are all affected.

5.3 GENDER-BASED CYBER VIOLENCE

Women are disproportionately affected by deepfake sextortion. Beyond financial extortion, victims suffer reputational damage, professional setbacks, and mental health challenges.[13]

5.4 THREATS TO NATIONAL SECURITY

Deepfake impersonation of officials can disrupt governance and be weaponized for political or extremist agendas, threatening national security.[14]

5.5 CHALLENGES FOR THE JUSTICE SYSTEM

Courts rely increasingly on digital evidence. Deepfakes complicate authentication, requiring advanced forensic techniques and new legal standards to determine admissibility.[15]

6. LEGAL AND REGULATORY CHALLENGES IN INDIA

India lacks a dedicated deepfake law, relying on fragmented existing statutes.

6.1 INFORMATION TECHNOLOGY ACT, 2000

Sections 66D (impersonation), 66E (privacy violation), and 67 (obscene content) address some aspects of deepfake misuse but do not explicitly cover AI-generated synthetic media.

[11] Neha Verma, Erosion of Public Trust Through Deepfakes, Indian Journal of Law & Technology (2024).
[12] Ibid.
[13] Ruchi Gupta, supra note 7.
[14] CERT-In, supra note 3.
[15] DeepStrike, supra note 5.

6.2 BHARATIYA NYAYA SANHITA (BNS), 2023

The BNS criminalizes cheating and fraud, but provides no definition or guidance regarding AI-generated impersonation.

6.3 DIGITAL FORENSICS GAP

India lacks standardized protocols for authenticating deepfake evidence in court. Police and forensic labs require advanced AI detection tools.

6.4 JURISDICTIONAL ISSUES

Many deepfake crimes originate abroad, complicating enforcement and legal proceedings.

6.5 PLATFORM LIABILITY

Social media and messaging platforms are not legally obligated to detect or remove deepfakes promptly. Mandatory obligations for platforms remain unimplemented.[16]

7. INTERNATIONAL APPROACHES

India can learn from global efforts to regulate deepfakes.

7.1 EUROPEAN UNION

The EU AI Act mandates transparency and labels for AI-generated media, classifying deepfakes as "high-risk" content.

7.2 UNITED STATES

Several U.S. states criminalize malicious deepfakes, particularly in elections or non-consensual pornography.

7.3 CHINA

China requires AI-generated content to be watermarked and imposes licensing for content creators.

[16] Pankaj Mishra, supra note 1.

8. POLICY RECOMMENDATIONS

A multi-layered strategy is required to combat deepfake fraud in India.

8.1 ENACT A DEDICATED DEEPFAKE LAW

Define "synthetic media" and "AI impersonation."

Criminalize malicious deepfakes, especially for financial, sexual, and political harm.

Mandate transparency, watermarking, and platform accountability.

8.2 NATIONAL DEEPFAKE FORENSIC LABORATORY

- Centralize AI forensic resources.
- Assist law enforcement, courts, and intelligence agencies.
- Collaborate internationally for cross-border investigations.

8.3 STRENGTHEN CERT-IN AND STATE CYBER CELLS

- Provide training in AI forensic analysis.
- Equip officers with detection tools and threat intelligence.

8.4 DIGITAL LITERACY AND PUBLIC AWARENESS CAMPAIGNS

- Teach citizens to identify deepfakes.
- Promote safe online practices and verification mechanisms.

8.5 COLLABORATION WITH INDUSTRY AND ACADEMIA

- Partner with AI labs, universities, and tech companies to improve detection algorithms.
- Develop AI ethics guidelines and public-private monitoring systems.

9. CONCLUSION

AI-generated deepfake fraud represents one of the most pressing cyber challenges for India. By eroding trust, facilitating financial scams, targeting women, and threatening political stability, deepfakes compromise the integrity of the digital ecosystem. India's unique vulnerabilities massive digital population, extensive online financial activity, and low digital literacy make it a prime target for cybercriminals.

To safeguard digital trust, India must implement a comprehensive strategy combining legislation, technological safeguards, forensic capabilities, public education, and international cooperation. Deepfake fraud is not merely a technical problem; it is a societal, legal, and ethical challenge that demands immediate, coordinated action.