INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions ofthe authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in theJournal.

EDITORIALTEAM

EDITORS

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

DEEPFAKES, DIGITAL ARRESTS, AND CYBERBULLYING: MAPPING THE LEGAL REGIME FOR ONLINE SAFETY IN INDIA

AUTHORED BY - PROF. DR. RICHA RANJAN[1] & JYOTI[2]

Abstract

The exponential growth of digital technologies has transformed the landscape of human interaction but it has also introduced unprecedented threats to individual rights and public safety. Among the most concerning developments are deepfakes, synthetic media generated using artificial intelligence, cyberbullying, and the rising phenomenon of digital arrests where individuals are identified, tracked, or apprehended through technological surveillance. In India, the legal system faces significant challenges in addressing these threats due to outdated statutory frameworks, limited judicial precedent, and the absence of specific legislation. This research paper critically examines the Indian legal regime's response to these evolving issues, highlighting the inadequacies in current laws such as the Information Technology Act, the Indian Penal Code (and its revised version, the Bharatiya Nyaya Sanhita), and the recently enacted Digital Personal Data Protection Act 2023. The paper further discusses the implications of these digital harms on fundamental rights including privacy, freedom of expression, and due process. Through comparative legal analysis with jurisdictions such as the United States, European Union, and China, the paper identifies best practices and legislative innovations that could guide Indian reforms. The study concludes by proposing specific legal, judicial, and policy recommendations to build a robust and future-ready framework that safeguards online safety while preserving constitutional values. Addressing the legal vacuum around deepfakes, clarifying the scope of digital arrests, and ensuring accountability in cyber-policing are crucial steps toward achieving digital justice in the world's largest democracy.

Keywords: *deepfakes, cyberbullying, digital arrest, online safety, Indian law, surveillance rights*

[1] Principal, Swami Devi Dyal College Of Law, Panchkula

[2] Assistant Professor, Swami Devi Dyal College Of Law**,** Panchkula

1. INTRODUCTION

The advancement of digital technologies has significantly impacted India's social, economic, and political landscape.[3] While these technologies have enabled numerous benefits, they have also introduced new challenges, particularly with the rise of cyber threats. Among the most concerning threats are deepfakes, digital arrests, and cyberbullying. Each of these issues presents unique challenges to the legal system and raises questions about the protection of privacy, the integrity of communication, and the accountability of online platforms. Deepfakes, which are synthetic media created using artificial intelligence to manipulate existing videos or images, have emerged as one of the most alarming technological developments in the realm of cybercrime.[4] The ability to create highly realistic videos or audio recordings of individuals saying or doing things they never did poses a serious threat to personal reputation, security, and even national integrity. In India, deepfake videos have already been used to defame celebrities and political figures, highlighting the need for a legal framework that can address the rapidly evolving threat.[5] The Indian legal system, which is based on the Information Technology Act, 2000 and various sections of the Indian Penal Code, has not yet fully adapted to address the nuances of deepfake-related crimes. As a result, victims often struggle to find legal recourse, and cybercriminals remain difficult to prosecute.

Alongside deepfakes, the rise of cyberbullying has become another major issue in India. Cyberbullying encompasses a range of online behaviors, including harassment, stalking, defamation, and identity theft, all of which can cause significant harm to individuals, particularly vulnerable groups such as children, women, and marginalized communities. While India has made strides in addressing online harassment through existing laws, many victims still face significant barriers to accessing justice. This is partly due to the lack of specific legal provisions targeting online harassment, and partly due to societal reluctance to report such incidents due to the stigma attached to being a victim of cyberbullying. Moreover, the anonymity provided by the internet allows perpetrators to hide behind fake profiles, making it difficult for law enforcement agencies to track and prosecute offenders. Despite attempts to

[3] Kaur, Sumanpreet, and Sajad Ahmad Mir. "Digital India: An Analysis of its Impact on Economic, Social, and Environmental Sectors." *Neuroquantology* 20.22 (2022): 2551-2561.

[4] Barnes, Curtis, and Tom Barraclough. "Deepfakes and synthetic media." *Emerging technologies and international security*. Routledge, 2020. 206-220.

[5] Verma, Karishma. "Digital Deception: The Impact of Deepfakes on Privacy Rights." *Lex Scientia Law Review* 8.2 (2024): 859-896.

address these issues, such as through the Digital Personal Data Protection Act, 2023, more targeted legal reforms are required to tackle cyberbullying effectively.

The concept of digital arrests, an emerging form of cybercrime, further complicates the landscape of online safety. In digital arrest scams, cybercriminals impersonate law enforcement officials, using video calls, fake documents, and other deceptive tactics to convince individuals that they are under investigation for serious crimes.[6] These criminals exploit the trust people place in authority figures, coercing victims into transferring money or providing sensitive personal information under the threat of legal action. Recent incidents in India have brought this issue to light. For example, a school headmaster in Hyderabad was defrauded of ₹65 lakh by scammers posing as CBI and ED officers. Similarly, a family in Delhi was held hostage through continuous video calls by individuals claiming to be from the Telecom Department, CBI, and ED, resulting in an extortion of ₹8 lakh. In both cases, the criminals used sophisticated digital tools to impersonate authority figures, thereby exploiting the trust of the victims. These scams highlight a significant gap in India’s legal framework, which has not yet fully addressed the complexities of such frauds, leaving citizens vulnerable to exploitation by cybercriminals.

In response to these threats, the Indian government has begun to take steps to improve online safety. Advisories have been issued, warning citizens about unsolicited video calls from individuals claiming to be judges, law enforcement officers, or other government officials. These advisories urge people to verify the identities of callers before taking any action, and to report suspicious activity to cybercrime helplines. Additionally, the government has launched initiatives aimed at improving public awareness about cybercrimes, including campaigns that educate citizens on how to protect their personal data and recognize fraudulent online activity. The law enforcement agencies have also started to implement more robust digital forensics tools to detect and investigate cybercrimes, although the capacity to address all forms of cybercrime remains limited.

Despite these efforts, the legal framework in India remains insufficient to deal with the rapidly evolving nature of cyber threats. While existing laws like the Information Technology Act, 2000 provide a foundation for addressing some aspects of cybercrime, they do not fully address the complexities of deepfakes, digital arrests, or cyberbullying. Additionally, there is a lack of

[6] Turvey, Brent E., John O. Savino, and Aurelio Coronado Mares. *False allegations: Investigative and forensic issues in fraudulent reports of crime*. Elsevier, 2017.

specific legal provisions that tackle these issues comprehensively, leaving many victims without legal recourse. The current legal regime also fails to adequately address the international nature of many cybercrimes, as criminals can operate from outside India, making enforcement difficult.[7]

To effectively address these emerging threats, India needs to reform its legal framework and create new laws that specifically target deepfakes, digital arrests, and cyberbullying. There is also a need for more comprehensive training for law enforcement agencies in digital forensics and cybercrime investigation. Public awareness campaigns must be expanded, and the role of social media platforms in preventing and addressing cybercrimes must be more clearly defined. International cooperation is also essential to address the cross-border nature of many cybercrimes. As technology continues to evolve, so too must the legal frameworks designed to protect individuals from cyber threats. Only with a coordinated effort from the government, law enforcement, and the public can India ensure a safer digital environment for all.

2. UNDERSTANDING THE THREATS

The rise of technology has brought with it a new breed of cyber threats that are increasingly targeting individuals, institutions, and national security. These threats are not only difficult to detect but also sophisticated in nature, making them a significant challenge for governments, law enforcement agencies, and individuals. The three major threats discussed in this paper deepfakes, digital arrests, and cyberbullying are particularly problematic as they exploit technological advancements to deceive, manipulate, and harm individuals. Understanding these threats is crucial to developing effective countermeasures.

2.1 Deepfakes

Deepfakes refer to the use of artificial intelligence (AI) and machine learning algorithms to create hyper-realistic media that manipulate video, audio, or images. By using AI, deepfakes can digitally alter or replace a person's face or voice, making it appear as if they are saying or doing something they never did. The technology behind deepfakes has evolved rapidly, making it increasingly difficult to distinguish between authentic and fabricated content.[8] While

[7] Buçaj, Enver, and Kenan Idrizaj. "The need for cybercrime regulation on a global scale by the international law and cyber convention." *Multidisciplinary Reviews* 8.1 (2025): 2025024-2025024.

[8] Ghiurău, David, and Daniela Elena Popescu. "Distinguishing Reality from AI: Approaches for Detecting Synthetic Content." *Computers* 14.1 (2024): 1.

deepfake technology has legitimate uses in entertainment and creative industries, its misuse has raised significant ethical and legal concerns.

In India, deepfakes have been used for various malicious purposes, including defamation, identity theft, and the spreading of misinformation. Celebrities and politicians have been prime targets, with deepfake videos being created to misrepresent their actions or statements. For example, a 2023 incident involved a deepfake video of a famous Bollywood actress that was circulated online, portraying her in a compromising situation. This video led to a temporary social media uproar, causing harm to her reputation. While India has some legal provisions for defamation, deepfakes present a unique challenge as they are often distributed through social media platforms, which complicates enforcement.

The key issue with deepfakes is the difficulty in detecting them and proving their falseness. While AI-driven tools are being developed to detect deepfakes, they are often not sophisticated enough to keep up with the rapid pace of technological advancements. Furthermore, there are currently no specific laws in India that address the creation, distribution, and malicious use of deepfakes.[9] The lack of a clear legal framework means that individuals whose reputations are damaged by deepfakes often have limited legal recourse, and perpetrators of such crimes are difficult to apprehend.

2.2 Digital Arrests

Digital arrests are a relatively new form of cybercrime where criminals impersonate law enforcement officers[10], often through video calls, emails, or phone calls. These criminals pose as officials from government agencies such as the CBI, ED, or even the judiciary, and inform their victims that they are under investigation for serious crimes. The perpetrators use fake documents, official-looking logos, and other deceitful tactics to create the illusion of an authentic legal process. In many cases, victims are pressured into paying large sums of money or providing sensitive personal information in exchange for the promise of avoiding arrest or legal trouble.

In India, the rise of digital arrest scams has been alarming. In 2024, a well-known case in Delhi

[9] Vig, Shinu. "Regulating Deepfakes." *Journal of Strategic Security* 17.3 (2024): 70-93.

[10] Chauhan, Jyoti. "Digital Arrest: An Emerging Cybercrime in India." *Issue 6 Int'l JL Mgmt. & Human.* 7 (2024): 1632.

involved a family being held hostage through a series of video calls by scammers posing as officials from the Telecom Department and the CBI. The criminals threatened to arrest the family members if they did not transfer ₹8 lakh, which was eventually extorted. Another incident in Hyderabad saw a school headmaster losing ₹65 lakh after being convinced by scammers posing as CBI officers. These incidents highlight how the perpetrators exploit the trust people have in authority figures and the fear of legal consequences to extort money.

What makes digital arrests particularly challenging is that the fraudsters are not bound by geographic location, meaning they can operate from anywhere in the world, making enforcement more complicated. Additionally, as these scams rely on digital communication channels like video calls, phone calls, and emails, they fall into legal gray areas where traditional law enforcement practices may not be effective. As a result, the victims often suffer from financial and emotional harm, and the perpetrators remain difficult to apprehend.

2.3 Cyberbullying

Cyberbullying refers to the use of digital platforms, such as social media, messaging apps, and gaming websites, to harass, intimidate, or harm others. Unlike traditional bullying[11], cyberbullying allows perpetrators to remain anonymous and reach their victims from anywhere, making it particularly insidious. The effects of cyberbullying can be severe, leading to psychological distress, anxiety, depression, and even suicide in extreme cases. In India, cyberbullying has emerged as a major concern, particularly among teenagers and young adults. The anonymity provided by the internet enables bullies to target individuals without facing immediate repercussions, making it a prevalent issue across various social media platforms.[12]

Recent statistics show a rise in incidents of cyberbullying in India, with many cases linked to school students, women, and activists. For example, a 2024 incident in Mumbai involved a young woman who was relentlessly bullied online after a personal photo was shared without her consent. The bullying escalated to threats of physical violence, which led the victim to seek help from law enforcement.[13] In many such cases, victims find it difficult to navigate the legal

[11] Hinduja, Sameer, and Justin W. Patchin. "Cyberbullying." *Cyberbullying Research Center. Retrieved September* 7 (2014): 2015.

[12] Ghosh, Ria, Meetu Malhotra, and Naresh Kumar. "Cyber Bullying in the Digital Age: Challenges, Impact, and Strategies for Prevention." *Combating Cyberbullying With Generative AI*. IGI Global Scientific Publishing, 2025. 151-180.

[13] Rahmadani, Celsy, Hartiwiningsih Hartiwiningsih, and Sulistyanta Sulistyanta. "The law enforcement against teenagers as perpetrators of bullying from the perspective of victim justice." *International conference on law, economic & good governance (IC-LAW 2023)*. Atlantis Press, 2024.

system due to the complexity of online harassment and the lack of specific provisions addressing cyberbullying in Indian law. Additionally, social media platforms often do not take swift action to remove harmful content or block abusive accounts, further complicating the issue.

One of the primary challenges in combating cyberbullying is that the perpetrators are often anonymous, using fake profiles or accounts to target victims.[14] Even when law enforcement is alerted, the lack of proper digital forensics tools and the failure to track down anonymous accounts make it difficult to identify and prosecute the offenders. Furthermore, societal stigma around online harassment often discourages victims from reporting such incidents, leaving many cases unreported. While there have been some legal efforts to address cyberbullying, such as through provisions in the Information Technology Act, 2000, these efforts are still insufficient to deal with the scale and complexity of the problem.

3. LEGAL FRAMEWORK IN INDIA

3.1 Constitutional Framework

The Constitution of Bharat guarantees the fundamental right to freedom of speech and expression under Article 19(1)(a). However, this right is not absolute. Article 19(2) allows the State to impose reasonable restrictions in the interest of sovereignty, public order, morality, security of the State, friendly relations with foreign states, contempt of court, defamation, or incitement to an offence.

Further reinforcing the individual's right to privacy, the landmark judgment in *K.S. Puttaswamy v. Union of India*[15] held that the right to privacy is intrinsic to Article 21, which guarantees the right to life and personal liberty. The Court emphasized the growing dangers to privacy in the digital age, especially from both State and non-State actors. It urged the Government to establish a robust data protection framework to strike a balance between individual privacy and State interests such as national security and innovation.

This constitutional scheme thus not only empowers the State to restrict harmful expression but also imposes a duty to safeguard citizens against the malicious misuse of personal data,

[14] Shafik, Wasswa. "Cyber Attacker Profiling and Cyberbullying Overview." *Cyber Space and Outer Space Security*. River Publishers, 2024. 125-149.
[15] (2017) 10 SCC 1

including through synthetic or manipulated content like deepfakes.

3.2 Information Technology Act, 2000

The Information Technology Act, 2000, forms the backbone of cyber law in Bharat. Though it does not explicitly mention "deepfakes," several of its provisions apply to the creation, transmission, and misuse of synthetic or manipulated digital content. The following sections are particularly relevant:

- **Section 66C – Punishment for Identity Theft**

  This section penalises any person who, fraudulently or dishonestly, makes use of the electronic signature, password, or any other unique identification feature of another person.

  Punishment: Imprisonment of up to **three years** and/or a **fine up to one lakh rupees**.
- **Section 66D – Cheating by Personation Using Computer Resource**

  This section criminalises cheating by personation through any communication device or computer resource. It is applicable to cases where deepfakes are used to impersonate someone and extract benefits or cause harm.

  Punishment: Imprisonment of up to **three years** and a **fine up to one lakh rupees**.
- **Section 66E – Violation of Privacy**

  This provision deals with capturing, publishing, or transmitting the image of a private area of any person without consent, under circumstances violating their privacy.

  Punishment: Imprisonment up to **three years** or a **fine not exceeding two lakh rupees**, or both.
- **Section 67 – Publishing or Transmitting Obscene Material in Electronic Form**

  This section punishes any person who publishes or transmits obscene material in electronic form. This provision is frequently invoked in cases where deepfake pornographic content is circulated.

  Punishment: First conviction: Imprisonment up to **three years** and a **fine up to five lakh rupees**, second or subsequent conviction: Imprisonment up to **five years** and a **fine up to ten lakh rupees**.
- **Section 67A – Publishing or Transmitting Material Containing Sexually Explicit Act**

  This section applies when the transmitted material involves actual or simulated sexually explicit content.

Punishment: First conviction: Imprisonment up to **five years** and a **fine up to ten lakh rupees**, second or subsequent conviction: Imprisonment up to **seven years** and a **fine up to ten lakh rupees**.

- **Section 67B – Publishing or Transmitting Child Pornography**

  This section criminalises material that depicts children in sexually explicit acts, including fabricated or deepfaked images.

  Punishment:First conviction: Imprisonment up to **five years** and a **fine up to ten lakh rupees**, Second or subsequent conviction: Imprisonment up to **seven years** and a **fine up to ten lakh rupees**.

  Application to Deepfakes: While the Act does not mention "deepfakes" specifically, these sections are regularly invoked when synthetic media is used to:

  - Impersonate someone online (Sections 66C and 66D),
  - Capture or publish non-consensual intimate images (Section 66E),
  - Circulate manipulated obscene or pornographic content (Sections 67, 67A, 67B).

3.3 Bharatiya Nyaya Sanhita, 2023

With the introduction of the Bharatiya Nyaya Sanhita (BNS), Bharat has modernized its criminal law to address new-age digital harms.

- Section 77 criminalizes the non-consensual capture or dissemination of a woman's image engaged in private acts.
- Section 351 penalizes threatening a person with injury or coercing them to act under duress.
- Section 356 defines and punishes defamation, including reputational harm caused by digital impersonation or false AI-generated content.

These provisions provide legal recourse in situations where deepfakes are used to harass, defame, or intimidate individuals, especially women.

3.4 Digital Personal Data Protection Act, 2023

The DPDP Act introduces a rights-based framework for data privacy and protection. It identifies individuals as data principals and places obligations on data fiduciaries who collect and process personal data.[16] The Act mandates that personal data must be processed only for lawful purposes with consent and outlines rights such as data access, correction, and erasure.

[16] Bisht, Ajay Kumar, and Neeruganti Shanmuka Sreenivasulu. "Information Privacy Rights in India: A Study of the Digital Personal Data Protection Act, 2023." *Data Privacy-Techniques, Applications, and Standards*. IntechOpen, 2024.

In the context of deepfakes, the unauthorized use of an individual's likeness or biometric data can be challenged under this Act. The DPDP's emphasis on consent and accountability is critical for tackling AI-driven misuse of personal identities.

3.5 Proposed Digital India Act

The proposed Digital India Act aims to overhaul the IT Act and address challenges posed by emerging technologies such as AI, deepfakes, and augmented reality. While the full draft is awaited, it is expected to address platform liability, content moderation, and algorithmic transparency. This legislation will be instrumental in plugging existing legal gaps related to digital manipulation and ensuring platform accountability.

3.6 International Perspectives

United States: Recent legislative efforts include the Preventing Deepfakes of Intimate Images Act, which criminalizes the unauthorized creation and dissemination of sexually explicit synthetic media. Other significant Bills include the No AI Fraud Act, the No Fakes Act,[17] and the Deepfakes Accountability Act. These measures recognize the voice and likeness of individuals as intellectual property and mandate transparency in AI-generated content.

European Union: The EU's General Data Protection Regulation (GDPR) offers robust protections against the misuse of personal data. Under the EU Artificial Intelligence Act, Article 50 mandates that AI-generated content, including deepfakes, must be clearly labeled.[18] This disclosure requirement helps users distinguish between real and manipulated media, thus enhancing transparency and accountability.

Saudi Arabia: Saudi Arabia has released comprehensive guidelines on the ethical use of deepfakes.[19] These cover regulatory compliance, data protection, consumer rights, and penalties for misuse, providing a structured framework for stakeholders ranging from developers to content platforms.

Australia and the United Kingdom: Australia's Criminal Code Amendment Act includes AI-generated sexual imagery within the scope of non-consensual image offences.[20] The UK's

[17] Graham, Claire. "Fake Images, Real Harm: A Case for Criminalising Non-consensual Intimate Deepfakes." (2024).

[18] Voigt, Paul, and Axel Von dem Bussche. "The eu general data protection regulation (gdpr)." *A practical guide, 1st ed., Cham: Springer International Publishing* 10.3152676 (2017): 10-5555.

[19] Khimi, Weeam, et al. "A Systematic Review on Deep Fake Image Generation Detection Techniques Ethical Implications and Overcoming Challenges." *International Journal of Computers and Informatics.* (2024).

[20] Graham, Claire. "Fake Images, Real Harm: A Case for Criminalising Non-consensual Intimate Deepfakes." (2024).

Online Safety Act, 2023, expands legal definitions to include computer-generated images as part of harmful content, thereby strengthening safeguards against deepfake abuse.

4. CASE STUDIES

To understand the real-world implications of deepfakes, digital arrests, and cyberbullying, examining actual case studies is essential. These cases highlight how these threats manifest in India and provide insights into the challenges of combating them through the existing legal and technological frameworks. The following case studies offer a glimpse into how the threats are taking shape and impacting victims across the country.

4.1 Rashmika Mandanna Deepfake (2023): In one of the first high-profile deepfake incidents in India, a fabricated video surfaced online in 2023 showing popular actress Rashmika Mandanna in a compromising situation. Created using AI tools to mimic her face and voice, the video went viral on WhatsApp and Telegram, causing immense reputational damage. Rashmika publicly condemned the video, leading to widespread debate over the misuse of AI and the lack of robust digital protection laws.

4.2 Kerala Schoolboy Impersonation Case (2023): In a small town in Kerala, a 14-year-old school student used free deepfake apps to create morphed images of his classmates and circulated them in school WhatsApp groups. Some images were indecent, causing distress among the students and their families. School authorities intervened, and a cyber complaint was registered. Though the child was dealt with under juvenile guidelines, the incident raised questions about early exposure to AI tools and lack of awareness.

4.3 Chennai College Sextortion Ring (2023): Late in 2023, Chennai police busted a sextortion racket that was targeting college girls. The gang used deepfake tools to superimpose faces of real students onto explicit videos and threatened to release them online unless money was paid. The operation led to multiple arrests and revealed the growing use of synthetic media in extortion crimes.

4.4 AI-Generated Minister Speech Incident (2023): In November 2023, a video began circulating on social media showing a Union Minister allegedly making controversial foreign policy remarks. Later investigations confirmed it was a deepfake, combining authentic visuals with AI-generated voice to mimic the minister. Though debunked by official agencies, the incident demonstrated how deepfakes could be weaponized for disinformation and political manipulation.

4.5 Delhi Deepfake Scam (2024): A gang in Delhi carried out an elaborate scam in 2024 by impersonating senior bureaucrats and business leaders via AI-generated video calls. Victims were tricked into transferring funds to fake accounts under the belief they were interacting with real officials. The police cyber unit eventually tracked down the culprits, but not before several people had lost substantial sums.

4.6 Mumbai Cyberbullying Case (2024): In 2024, a 16-year-old girl in Mumbai became the victim of cyberbullying after an intimate image of her was leaked online. Fake profiles began harassing her with threats and lewd messages. The emotional trauma required mental health intervention, and legal proceedings were initiated under the IT Act and POCSO. The case underlined the psychological impact of cyber abuse on minors.

4.7 Bengaluru Tech Employee Scam (2024): A Bengaluru software professional was conned out of ₹9 lakhs in late 2024 through a deepfake Zoom call. Believing he was speaking to his company's HR head, the employee transferred funds for a fake emergency. It was only after internal verification that the fraud came to light, sparking a warning notice from the company and legal action.

4.8 Hyderabad Influencer Defamation (2025): In early 2025, a Hyderabad-based influencer became the target of deepfake defamation. Fake videos showing her making offensive remarks were uploaded by anonymous users, resulting in public backlash and brand loss. Forensic analysis confirmed manipulation, and she lodged complaints under the IT Act and defamation laws.

5. RECOMMENDATIONS AND CONCLUSION

The rise of deepfakes, digital arrest scams, and cyberbullying highlights the urgent need for India to modernise its cyber regulatory ecosystem. These issues, while technologically diverse, share a common thread: they exploit gaps in the existing legal framework and target victims through impersonation, manipulation, and psychological coercion. As online threats grow in sophistication and accessibility, India must adopt a proactive, multi-stakeholder approach to ensure digital safety, build deterrence, and restore user trust in the digital ecosystem.

5.1. Recommendations:

1. Enact Specific Legislation on Deepfakes and Synthetic Media: India must introduce clear legal definitions and penal provisions for the creation, distribution, and malicious use of deepfakes. The proposed Digital India Act should include specific clauses that criminalise synthetic media when used for impersonation, defamation, political manipulation, or non-consensual pornography. It should also prescribe standards for watermarking AI-generated content and mandate transparency obligations for platforms hosting such content.

2. Criminalise Digital Arrest Scams: There must be a dedicated provision in the BNS or cybercrime law that recognises impersonation of law enforcement officers and courts in virtual spaces. This includes penalising the unauthorised use of official insignias, forged arrest warrants, or fake video calls claiming judicial authority. The law should treat such acts as aggravated offences, given their potential to incite fear, cause reputational damage, and extract money or data.

3. Introduce a Dedicated Anti-Cyberbullying Statute: India should pass a comprehensive anti-cyberbullying law with special protections for children, women, and vulnerable communities. This law must include time-bound redressal mechanisms, school and workplace reporting frameworks, and mandatory takedown protocols for abusive content. The law should empower victims to file complaints without the fear of reprisal, and ensure platform accountability through fines and compliance audits.

4. Strengthen Digital Forensics and Capacity-Building: Law enforcement agencies must be equipped with AI-based tools for deepfake detection, metadata analysis, and real-time content tracking. Cyber forensics labs should be expanded to all states and integrated with district-level police units. Capacity-building workshops must be institutionalised through collaborations with academia, think tanks, and private tech firms.

5. Establish a Centralised Cyber Safety Authority: A nodal agency akin to the Financial Intelligence Unit or the National Investigation Agency must be created to oversee cyber safety. This authority should be tasked with policy formulation, inter-agency coordination, standard-setting, and international collaboration. It must also operate a 24x7 emergency helpline and victim support portal.

6. Encourage Public-Private Partnerships (PPPs): Given the dominance of private platforms in digital communication, the government must institutionalise partnerships with companies like Meta, Google, and X (formerly Twitter) for expedited response protocols, AI moderation, and training. Voluntary codes of conduct can be negotiated, focusing on transparency, human rights, and victim empowerment.

7. Launch National Awareness Campaigns: The government must run regular campaigns warning citizens about digital arrest scams, deepfake risks, and online abuse. These should be conducted in multiple regional languages and disseminated via television, social media, and community outreach. Advisories — such as the one recently issued by the Ministry of Home Affairs about video calls from fake judges or CBI officers — must be made more accessible and frequent.

8. Build International Cooperation Frameworks: India must negotiate mutual legal assistance treaties (MLATs) and sign cross-border enforcement treaties to enable quicker takedowns, evidence sharing, and prosecution of perpetrators in foreign jurisdictions. The G20 Digital Economy Working Group and UN cybercrime treaty negotiations offer such platforms.

5.2. Conclusion:

The digital revolution in India, while transformative, has introduced complex threats that demand equally nuanced legal and policy responses. Deepfakes can destroy reputations and distort truth. Digital arrests terrorise citizens and erode trust in state institutions. Cyberbullying can push victims to depression or even suicide. These harms are not abstract — they are daily realities reported across the country, as seen in the Delhi deepfake scam of 2024, the impersonation of judges in video calls, and cyber harassment of celebrities and common citizens alike.

A fragmented legal approach, inadequate enforcement, and low digital literacy only exacerbate the problem. However, the solution does not lie solely in harsher laws or surveillance. It lies in creating an inclusive, transparent, and rights-respecting digital environment — one where technology serves the people and not the other way around.

A robust legal regime for online safety in India must therefore be forward-looking, tech-aware, victim-sensitive, and democratically accountable. With the right reforms and institutional will, India can set a global example for balancing digital innovation with user protection in the 21st century.

BIBLIOGRAPGHY

Books

1. Barnes, Curtis, and Tom Barraclough, *Deepfakes and Synthetic Media*, Routledge, 2020.
2. Bisht, Ajay Kumar, and Neeruganti Shanmuka Sreenivasulu, *Data Privacy—Techniques, Applications, and Standards*, IntechOpen, 2024.

3. Buçaj, Enver, and Kenan Idrizaj, *Multidisciplinary Reviews*, 2025.
4. Chauhan, Jyoti, *Int'l J.L. Mgmt. & Human.*, 2024.
5. Ghiurău, David, and Daniela Elena Popescu, *Computers*, MDPI, 2024.
6. Ghosh, Ria, Meetu Malhotra, and Naresh Kumar, *Combating Cyberbullying with Generative AI*, IGI Global, 2025.
7. Graham, Claire, *Fake Images, Real Harm*, 2024.
8. Hinduja, Sameer, and Justin W. Patchin, *Cyberbullying Research Center*, 2014.
9. Kapadia, Priya, *NUJS Law Review*, 2024.
10. Khimi, Weeam, et al., *International Journal of Computers and Informatics*, 2024.
11. Kumar, Arvind, *Cyber Law Review*, 2023.
12. Ministry of Law and Justice, *The Digital Personal Data Protection Act*, 2023.
13. Rahmadani, Celsy, Hartiwiningsih, and Sulistyanta, *IC-LAW 2023*, Atlantis Press, 2024.
14. Sharma, Ritu, *National Law School Journal*, 2023.
15. Shafik, Wasswa, *Cyber Attacker Profiling and Cyberbullying Overview*, River Publishers, 2024.
16. Singh, Abhishek, *Indian Journal of Law and Technology*, 2024.
17. Turvey, Brent E., John O. Savino, and Aurelio Coronado Mares, *False Allegations: Investigative and Forensic Issues in Fraudulent Reports of Crime*, Elsevier, 2017.
18. Verma, Karishma, *Lex Scientia Law Review*, 2024.
19. Vig, Shinu, *Journal of Strategic Security*, 2024.
20. Voigt, Paul, and Axel Von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer, 2017.

Research Papers

1. Barnes, Curtis, and Tom Barraclough, "Deepfakes and Synthetic Media." *Emerging Technologies and International Security*, Routledge, 2020.
2. Bisht, Ajay Kumar, and Sreenivasulu, "Information Privacy Rights in India." *Data Privacy*, 2024.
3. Chauhan, Jyoti, "Digital Arrest: An Emerging Cybercrime in India." *Int'l J.L. Mgmt. & Human*, 2024.
4. Ghiurău, David, and Daniela Elena Popescu, "Distinguishing Reality from AI." *Computers*, 2024.

5. Ghosh, Ria, et al., “Cyber Bullying in the Digital Age.” *Combating Cyberbullying with Generative AI*, 2025.
6. Graham, Claire, “Fake Images, Real Harm.” 2024.
7. Hinduja, Sameer, and Justin W. Patchin, “Cyberbullying.” *Cyberbullying Research Center*, 2014.
8. Kaur, Sumanpreet, and Sajad Ahmad Mir, “Digital India: An Analysis.” *Neuroquantology*, 2022.
9. Kapadia, Priya, “Social Media and Misuse of Deepfakes.” *NUJS Law Review*, 2024.
10. Khimi, Weeam, et al., “Deep Fake Detection Techniques.” *International Journal of Computers and Informatics*, 2024.
11. Rahmadani, Celsy, et al., “Law Enforcement Against Teen Bullying.” *IC-LAW 2023*, 2024.
12. Sharma, Ritu, “Online Harassment and Women’s Safety.” *National Law School Journal*, 2023.
13. Shafik, Wasswa, “Cyber Attacker Profiling and Cyberbullying.” *Cyber Space and Outer Space Security*, 2024.
14. Singh, Abhishek, “Privacy and Technology in Indian Law.” *Indian Journal of Law and Technology*, 2024.
15. Vig, Shinu, “Regulating Deepfakes.” *Journal of Strategic Security*, 2024.

Case Laws

1. Association for Democratic Reforms v. Union of India
2. Internet Freedom Foundation v. Ministry of Electronics and IT
3. JSW Steel Ltd. v. Bhushan Power & Steel Ltd.
4. Kamlesh Vaswani v. Union of India
5. K.S. Puttaswamy v. Union of India
6. State of Madhya Pradesh v. Balveer Singh
7. State of Tamil Nadu v. Governor of Tamil Nadu
8. Supriyo v. Union of India
9. Wikimedia Foundation v. ANI
10. X v. Union of India