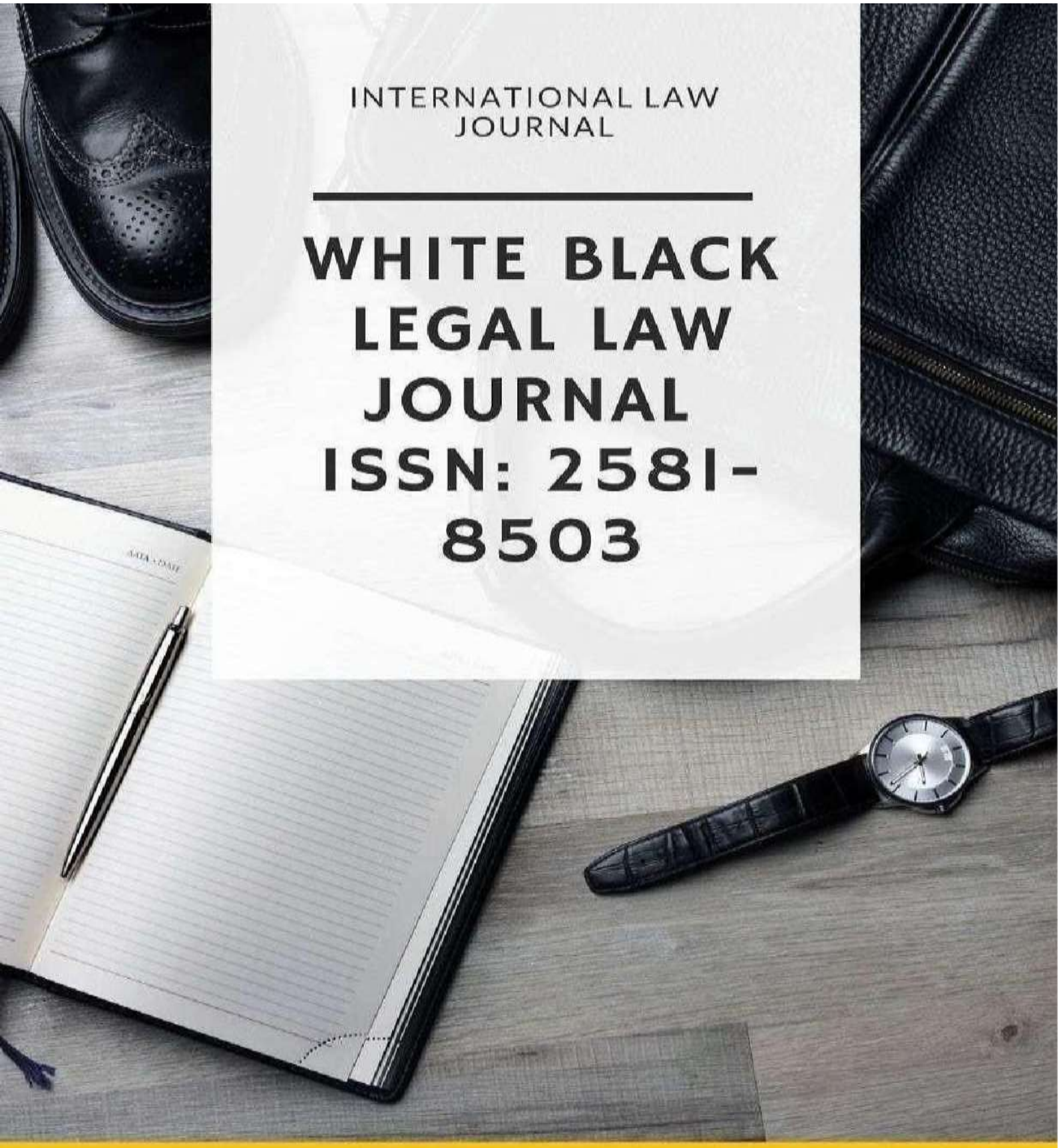

INTERNATIONAL LAW JOURNAL

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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | July 2025 ISSN: 2581-8503

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 providededicated 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

www.whiteblacklegal.co.in
Volume 3 Issue 1 | July 2025 ISSN: 2581-8503

REVENGE PORN AND DEEPFAKES: THE NEED FOR A ROBUST LEGAL FRAMEWORK IN INDIA

AUTHORED BY - LAKSHAY KUMAR

ABSTRACT

The widespread use of social media and the quick development of digital technology have led to the emergence of new types of cyber exploitation, most notably deepfake and revenge pornography. Whereas deepfakes use artificial intelligence to create hyper-realistic but fake content, usually for defamatory, coercive, or harassing purposes, revenge porn is the unconsented distribution of sexually explicit images or videos, usually with the intention of embarrassing or retaliating against the victim. These phenomena, which primarily affect women and marginalized communities, constitute a serious violation of people's rights to privacy, physical autonomy, and dignity.

In India, there is no comprehensive legal framework created especially to address the complexities and changing nature of image-based sexual abuse in the digital age, even though certain provisions under the Indian Penal Code (BNS), 2023, the Information Technology Act, 2000, and the Indecent Representation of Women (Prohibition) Act, 1986 may be invoked to address elements of these crimes. Victims are left with few options and insufficient protection in the absence of a clear definition, transparent procedures, and robust enforcement measures.

This paper highlights important legal gaps and procedural difficulties in the current statutory and judicial responses to deepfakes and revenge porn in India. Additionally, it compares itself to international legal norms, such those in the US, UK, and Australia, in order to find possible reform models. In order to ensure compliance with international human rights commitments and constitutional norms, the paper makes the case for the urgent necessity to pass tailored legislation that identifies, criminalizes, and offers appropriate remedies for such digital sexual violence.

This study aims to add to the conversation on updating India's cybercrime jurisprudence to better protect victims and discourage offenders in the digital era by placing these offenses within larger problems of gender justice, cybersecurity, and technological accountability.

INTRODUCTION

The way people express themselves, communicate, and create connections has changed as a result of the digital revolution. But this change has also made room for new kinds of sexual exploitation made possible by the internet, such as deepfake technology and revenge pornography. The term "revenge porn" describes the unconsented dissemination of sexually explicit pictures or movies, frequently by a resentful ex-partner, with the goal of controlling, humiliating, or harassing the victim. Conversely, deepfakes are produced by using artificial intelligence and machine learning to produce synthetic audio-visual content that superimposes a person's voice or face onto another person's body without that person's knowledge or consent, usually in sexually explicit or libelous circumstances.

A person's rights to privacy, dignity, and bodily autonomy—all guaranteed by the Indian Constitution and acknowledged by case law like Justice K.S. Puttaswamy v. Union of India—are seriously threatened by both types of abuse. The victims, who are primarily women and members of gender minorities, suffer irreversible harm to their reputation, jobs, and mental health in addition to emotional distress and social exclusion. The current judicial systems in India are still insufficient to handle the complexities of image-based sexual abuse and synthetic media manipulation, even if the frequency of such occurrences is rising.

Although the Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023) and the Information Technology Act of 2000 attempt to offer some legal recourse, they were not intended to address technologically complex and consent-based offenses like revenge porn or deepfakes. A significant portion of impacted people are left vulnerable and without proper protection or justice due to the absence of clear definitions, transparent procedures, and victim-centered redressal methods.

This article aims to critically analyze the legal gaps in India's cybercrime jurisprudence in light of the growing abuse of digital means to commit sexual violence and harassment. In order to successfully handle and prevent the growing threat of revenge porn and deepfakes in the digital age, it also makes the case for the urgent creation of a comprehensive, gender-neutral, and technology-oriented legislative framework.

II. Understanding the Offenses

Understanding the unique characteristics and mechanisms of revenge porn and deepfakes is crucial for assessing the appropriate legal response to these crimes. Despite the fact that they both entail the production or non-consensual distribution of sexual content, their goals, methods, and technological sophistication vary greatly.

A. Revenge Porn

Often referred to as non-consensual pornography, revenge porn is the practice of publishing or disseminating sexually explicit photos or videos of someone without that person's consent. Usually, this is done by someone who had access to the material during a private or personal relationship. This act's main motivation is frequently coercion, humiliation, or retaliation. These documents are frequently used by the offender, who is frequently a previous love or sexual relationship, to extort the victim, inflict emotional distress, or exercise authority.

There are serious repercussions for this type of image-based sexual abuse. In severe situations, victims are motivated to self-harm or commit suicide. They also experience severe psychological distress, social estrangement, and job difficulties. In contrast to more conventional types of sexual violence, the trauma is repeated and prolonged due to the permanent nature of content posted online, particularly when it becomes viral or shows up on pornographic websites.

B. Deepfakes

A more modern and technologically sophisticated type of misuse is represented by deepfakes. They entail creating hyper-realistic audio-visual content using generative adversarial networks (GANs) and deep learning techniques. When it comes to sexual exploitation, deepfakes typically entail altering pornographic content by substituting the face of an unwitting person—typically celebrities, prominent personalities, or former partners—for the original subject's without getting their permission.

Deepfakes create imaginary but convincing content, in contrast to revenge porn, which may contain genuine photographs or videos that are published without consent. This presents a special legal problem because, despite the fact that the content is fictional, the harm it causes—such as emotional distress, defamation, blackmail, and reputational damages—is real and

serious. Prosecution is made even more difficult by the challenge of identifying and demonstrating that such content is fake.

Furthermore, the threat has increased due to the availability of free and easy-to-use AI tools like face-swapping applications and synthetic speech generators, which have made it easier for anybody to produce deepfakes. The situation is further complicated by the gendered character of this abuse, which disproportionately affects women.

III. Legal Landscape in India

Even while deepfake abuse and revenge porn are becoming more common, the Indian legal system does not have a thorough and focused framework to deal with these particular offenses. The Indian Penal Code (now Bharatiya Nyaya Sanhita, 2023), the Information Technology Act, 2000, and other sectoral laws may provide some partial remedies, but they are insufficient to address the technological subtleties, consent-based violations, and gendered nature of these digital crimes.

A. Information Technology Act, 2000

India's main law regulating cyber activity is the Information Technology Act (IT Act). When it comes to deepfakes and revenge porn, a few clauses are pertinent:

- **According to Section 66E**, it is illegal to purposefully take, publish, or send pictures of someone else's private areas without that person's agreement. The punishment can be up to three years in prison, a fine of up to ₹2 lakh, or both.
- **Section 67:** Makes it illegal to produce or distribute pornographic content online. Publishing or sending content that contains sexually explicit conduct is covered by Section 67A.
- Child sexual abuse material (CSAM) is covered under **Section 67B.**

Limitations:

- The idea of "consent" as being essential to image sharing is not specifically acknowledged by these clauses.
- Deepfakes and other artificial intelligence-generated or fake content are not mentioned.
- Enforcement authorities are left to interpret the terminology, which is still outdated and ambiguous.

- The Act is more concerned with the pornographic or obscenity of the content than with its unconsented distribution or alteration.

B. Indian Penal Code (Now Bharatiya Nyaya Sanhita, 2023)

Various sections of the Indian Penal Code (now subsumed under BNS, 2023) have been invoked in cases of online sexual exploitation:

- **Section 354C (Voyeurism)**: punishes observing or taking pictures of a lady doing an intimate act without getting her permission.
- **Section 292 & 293**: Address the distribution and sale of pornographic content.
- **Section 509**: punishes actions that use words, gestures, or invasions to disparage a woman's modesty.
- **Section 499 (Defamation)** and **Section 500 :**Reputational harm may be subject to (punishment for slander).

Limitations:

- These portions are frequently restricted to victims who are women and are largely gendered.
- Since Deepfakes are fictional, they might not be considered "obscenity" or "voyeurism."
- When creating synthetic content, it might be challenging to prove that the goal was to harass or slander.
- Despite being a significant change, the Bharatiya Nyaya Sanhita, 2023, does not contain any provisions specifically addressing deepfake technology or exploitation based on artificial intelligence.

C. Other Relevant Laws

- **The Indecent Representation of Women (Prohibition) Act, 1986**: prohibits the derogatory portrayal of women in writings, publications, ads, and other media, including electronic media. It is important but mostly out of date in revenge porn.
- **The Protection of Children from Sexual Offences (POCSO) Act, 2012**:imposes severe penalties for disseminating or publishing sexually explicit content involving children, even online.
- **The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 (POSH Act)**: Online distribution of pornographic material about a coworker may occasionally be considered workplace harassment.

Gaps:

- Deepfakes are not specifically covered by these regulations, nor do they define "image-based sexual abuse."
- Neither a special cybercrime court nor tribunal exists, nor is there a fast-track redressal process.
- Victim initiative plays a major role in prosecution, which is challenging considering the trauma and stigma involved.

D. Judicial Approach and Challenges

In response to these cases, the Indian judiciary has issued temporary remedies like FIR registrations, content deletion orders, and limited compensation. The Supreme Court strengthened the constitutional basis for judicial redress in such cases by recognizing the right to privacy as a basic right under Article 21 in Justice K.S. Puttaswamy v. Union of India (2017).

However:

- Deepfake pornography is not particularly covered by any significant court ruling.
- The jurisprudence of the courts on consent in digital sexual offenses has not developed.
- Trial delays and a shortage of qualified judges continue to be significant obstacles.

Sectional Conclusion

Although India has a patchwork of laws to deal with some aspects of deepfakes and revenge porn, there are still a lot of gaps in protection, enforcement, and restitution because there isn't a single, comprehensive, and enforceable law. Because of the speed, scope, and complexity of these crimes, the criminal justice system is now ill-prepared to handle them, leaving victims at risk and offenders generally unpunished.

IV. Challenges in Legal Enforcement

India confronts several systemic, administrative, and technological challenges in enforcing laws against deepfake abuse and revenge porn. Even in cases when laws are in place, they are not always well implemented, which frequently leads to poor conviction rates, underreporting, and a lack of investigation. Victims now face a justice gap as a result of the intricacy of these crimes, institutional indifference, and social stigma.

A. Jurisdictional and Technological Barriers

The jurisdictional ambiguity brought on by the worldwide nature of internet infrastructure is one of the biggest obstacles to prosecuting cases of digital sexual abuse. Because the servers that house the offensive content are frequently located outside of India, cross-border data access and collaboration are unpredictable and time-consuming processes. India currently lacks robust bilateral cybercrime agreements with numerous nations, and the Mutual Legal Assistance Treaty (MLAT) process is sluggish.

Furthermore, because of the anonymity provided by the internet, criminals can hide their identities by using encrypted platforms, VPNs, and phony accounts. Investigating officers frequently lack the technological know-how and resources required to track digital footprints, especially when dealing with anonymous file-sharing websites or AI-generated content.

B. Absence of Digital Forensic Infrastructure

Investigation is significantly hampered by the lack of trained staff and digital forensic labs in various regions of the nation. Procedures for retrieving and maintaining electronic evidence are either unclear or improperly implemented, and cybercrime cells are understaffed even in urban regions. This frequently results in evidence manipulation, errors in procedure, and the accused's eventual acquittal.

C. Delayed FIRs and Low Conviction Rates

First Information Reports (FIRs) are frequently delayed by victims' extreme psychological strain, fear of social stigma, and lack of trust in law enforcement. When dealing with situations featuring sexual content, police officers are typically inexperienced or insensitive, which encourages victim-blaming and discourages legal action. Instead of pursuing criminal prosecution, law enforcement officials frequently try to mediate.

The lengthy trial procedure and absence of confidentiality protections, even in cases when FIRs are registered, discourage victims from seeking justice. Consequently, conviction rates for sexual offenses aided by cyberspace continue to be appallingly low.

D. Victim Re-traumatization and Social Ostracization

Because the content may be reposted or reshared numerous times, victims of deepfakes and revenge porn experience recurring anguish. Digital content's longevity guarantees that it may

reappear on other platforms even after being removed. In addition, survivors frequently suffer from mental health problems, professional harm, and social exclusion.

E. Lack of Institutional Coordination

Poor cooperation between police, social media companies, and judicial authorities results from the lack of a centralized structure for reporting, tracking, and addressing digital sexual offenses. Platforms may oppose removal unless ordered by a court, and requests to remove content are delayed.

Conclusion of Section

Therefore, the actual enforcement of rights against digital sexual abuse is still weak and dispersed, even in cases where there are legal remedies in theory. The promise of justice in these situations is mainly unrealized without a huge investment in victim support networks, digital infrastructure, and training.

V. Comparative International Legal Frameworks

The problems caused by deepfakes and revenge porn are not exclusive to India; a number of countries have recognized and addressed these new types of online abuse with specific laws. Many nations have shifted from traditional obscenity laws to victim-centric, tech-aware rules, according to a comparative review. India may learn a lot from these various legal systems about creating a comprehensive legal system.

A. United Kingdom

One of the first countries to enact legislation specifically prohibiting revenge pornography was the United Kingdom. Section 33 of the Criminal Justice and Courts Act of 2015 made it illegal to reveal private sexual images and videos without permission or with the intention of upsetting someone. Regardless of the parties' connection, the offense carries a maximum sentence of two years in jail.

The UK passed the Online Safety Act in 2023, giving people legal protection from deepfake pornography that is not consenting. Platforms are required by this law to assist authorities and delete damaging deepfake content. Additionally, the law requires digital businesses to evaluate and reduce the dangers of sexual exploitation caused by AI on their platforms.

B. United States

In the United States, a patchwork of state laws has developed despite the lack of a single federal legislation that particularly addresses revenge porn. The non-consensual distribution of intimate photos is now illegal in more than 46 states and the District of Columbia. For instance, purposeful dissemination of private information without consent is punishable under California's Penal Code Section 647(j)(4), particularly when done with the intention of causing distress.

The planned DEEPFAKES Accountability Act is one piece of current federal legislation that aims to control the production and distribution of synthetic media, including labeling specifications and sanctions for malevolent use.

C. Australia

In order to address image-based abuse, Australia has implemented a unified legislative framework across the country. According to the Criminal Code Amendment (distributing of personal Images) Act of 2018, possessing, distributing, or threatening to share personal images without consent is illegal and carries a maximum sentence of seven years in jail. It stands out for being consent-focused and gender-neutral.

Furthermore, the eSafety Commissioner, an independent regulatory body formed in Australia, has the authority to receive complaints, order takedowns, and even impose civil fines on violators or platforms that do not comply.

Key Takeaways for India

- precise definitions and legislative terminology based on consent.
- platform liabilities and responsibilities for content control.
- specialized authorities for regulation or reparation.
- mechanisms for time-bound takedown and inquiry.

In comparison, India's current legal system is still disjointed, antiquated, and unprepared to deal with the complex nature of online sexual assault. India might modify the clear legislative models and innovative policies from the worldwide examples to fit its own situation.

VI. Need for a Comprehensive Law

The disjointed way that Indian law handles deepfakes and revenge porn highlights how urgently a focused, all-encompassing, and future-proof legal framework is needed. The Bharatiya Nyaya Sanhita (BNS), the Information Technology Act, and other general criminal statutes now have provisions that are out-of-date, insufficient, and unsuitable for dealing with the psychological effects and technological complexity of these offences.

The clear legal recognition of deepfakes and revenge porn as separate criminal offenses must be the first step toward a strong framework. This involves providing precise definitions for concepts like:

- “Pornography that is not consenting”
- "Deepfake material"
- "Sexual abuse based on images"
- "Synthetic manipulation of media"

The importance of permission must be ingrained in the legal system, moving the emphasis from morality or obscenity to the infringement of individual liberty and dignity. A contemporary statute should acknowledge that, in contrast to traditional obscenity laws, even non-sexually explicit deepfakes can be considered a type of digital sexual assault and psychological abuse when they are produced with the intent to harass, extort, or slander.

Furthermore, in order to shield everyone from this kind of abuse, regardless of sexual orientation or gender identity, the law must be gender-neutral. LGBTQIA+ men and women are among the many victims of digital sexual abuse who experience severe institutional neglect and social stigma. A non-discriminatory and inclusive statute is therefore essential.

The law must provide the following provisions in addition to making the production and distribution of such content illegal:

- Removal of such content from digital sites with a time limit
- Mandatory reporting requirements for service providers and intermediaries
- Injunctions and compensation are examples of civil remedies.
- Techniques for maintaining confidentiality to safeguard victim identity
- Punitive measures for careless platforms as well as individual offenders

The creation of a specialized tribunal or authority (such a "Cyber Crime Redressal Commission") may also be necessary given the scope of the issue and the difficulty of gathering digital evidence in order to manage complaints, oversee takedowns, and guarantee prompt adjudication.

In conclusion, any legal reaction to deepfakes and revenge porn needs to be survivor-centric, rights-based, forward-thinking, and technologically advanced. This will guarantee that the law not only punishes the offender but also protects the victim's privacy and dignity in a timely and significant way.

VII. Recommendations and Way Forward

Given the growing prevalence of deepfake and revenge porn abuse in India, as well as the shortcomings of the current judicial system, a multifaceted approach is necessary to counteract this online threat. To guarantee a fair, effective, and survivor-centered framework, the following institutional, legal, and legislative changes are suggested:

1. Enact a Specific Law on Image-Based Sexual Abuse and Synthetic Media Crimes

- India needs to enact a specific law that covers all aspects of image-based sexual abuse, including offenses involving deepfakes and non-consensual pornography. The law ought to:
- Important concepts such as "consent," "intimate image," and "synthetic sexual content" should be defined precisely.
- Make it illegal to create, possess, or threaten to disclose such material in addition to distributing it.
- Include harsher penalties for serial offenders, those who target kids, or those who exploit others for profit.

2. Consent-Centric and Gender-Neutral Framework

Consent-based protection of bodily autonomy and dignity must replace obscenity-based morality in the legal system. In order to eradicate discrimination in legal protection, the law should also apply to everyone, including men and LGBTQIA+ people.

3. Fast-Track Reporting and Takedown Mechanisms

- Create a 24-hour cyber grievance site with streamlined reporting processes for material.

- legally require platforms and intermediaries to respond to takedown requests within 24 to 48 hours (as stipulated in Rule 3 of the IT Rules, 2021).
- Platforms should be penalized for delays or noncompliance.

4. Judicial and Law Enforcement Training

- Provide specialist training courses on how to handle technology-enabled sexual violence for judges, prosecutors, and detectives.
- Make sure victim-sensitive protocols are followed throughout the gathering of evidence, recording of statements, and trial.

5. Public Awareness and Digital Literacy

- Start national efforts to inform users about the value of consent, cyber safety, and legal recourse options.
- Include instruction on digital ethics and privacy in the curricula of universities and schools.

6. Establish a Dedicated Cyber Crime Redressal Authority

Like Australia's eSafety Commissioner, a quasi-judicial or regulatory body ought to be established to:

- Respond to grievances,
- Give instructions for an immediate takedown,
- Work together with social media sites, and
- When necessary, recommend prosecution.

7. International Collaboration

To guarantee prompt action against transnational crimes, India needs to fortify its data-sharing agreements and Mutual Legal Assistance Treaties (MLATs) with international IT firms and governments.

To successfully protect digital dignity and stop the weaponization of privacy in the cyber age, a concerted institutional and legal reaction based on constitutional principles and technological knowledge is essential.

VIII. Conclusion

In a culture that is digitizing as quickly as India, the growth of deepfakes and revenge porn poses a severe danger to people's autonomy, privacy, and dignity in the digital age. These crimes disproportionately affect women, LGBTQIA+ people, and vulnerable communities, and despite their technological sophistication, they are essentially predicated on gender-based abuse, domination, and humiliation.

India's legal system is nevertheless disjointed, antiquated, and reactive, despite the country's significant progress in acknowledging the right to privacy as a basic right guaranteed by Article 21 of the Constitution. Existing legislation is either too limited to adequately address the entire spectrum of new digital hazards or too broad to be properly implemented. Furthermore, victims are frequently discouraged from pursuing justice due to social stigma, poor enforcement, procedural difficulties, and a lack of technical readiness.

Many other jurisdictions, on the other hand, have passed clear, consent-focused, survivor-centric legislation that is backed by institutional safeguards to guarantee both prevention and redress. These international models provide unambiguous reform routes.

Thus, comprehensive laws that specifically punish deepfakes and revenge porn, offer expedited redress, require platform accountability, and acknowledge the psychological and technological complexity of these crimes are desperately needed in India. A strong law must be accompanied by international collaboration, public awareness campaigns, and law enforcement training.

The law must change to keep up with technology in the digital age. India must give priority to anticipatory, inclusive, and unwavering legislative change that upholds human dignity and cyber justice if it is to effectively safeguard citizens' fundamental rights.