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.
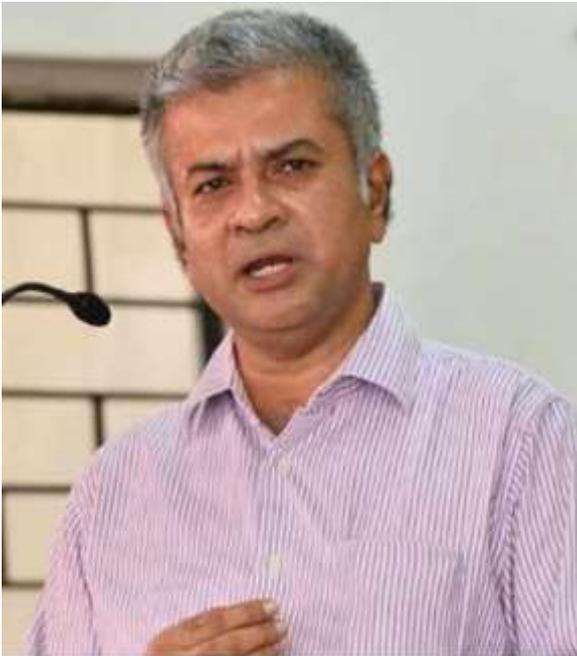
DISCLAIMER

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.
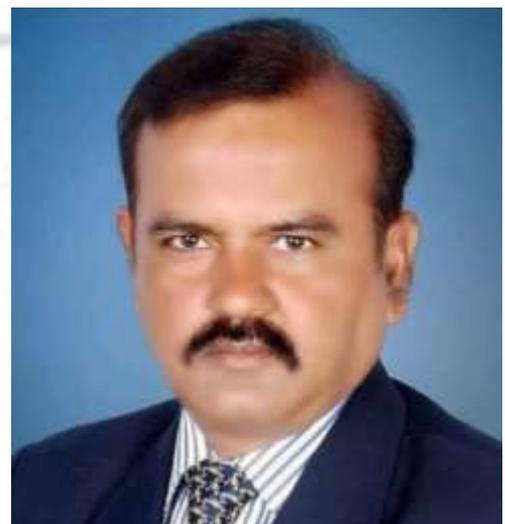
Senior Editor

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

INTERSECTION OF REVENGE PORN, DEEPFAKE TECHNOLOGY AND WOMEN'S PRIVACY

AUTHORED BY - DR. OMPRABHA

Associate Professor, MDU-CPAS, Gurugram

ABSTRACT

In the digital age, technological advances have rendered it possible for new forms of violence to emerge that disproportionately affect women, particularly through deepfake and revenge pornography. The release of intimate and sensitive photographs without consent is known as revenge porn, whereas deepfakes apply artificial intelligence to produce fake yet hyper-realistic sexual content, frequently without the subject's consent. Women's autonomy and privacy are violated by both types of abuse, which use their online personas as a means of control and humiliation.

The objectification and commoditization of women's bodies are reinforced by these behaviors, which go beyond individual betrayal and are a reflection of larger structural injustices. While the institutional and legal remedies available are still often ineffective and fragmented, victims frequently experience economic loss, social isolation, emotional suffering, and reputational harm. This chapter examines how deepfakes and revenge porn upend conventional ideas of identity, consent, and privacy in digital contexts. It also highlights the necessity of survivor-centered support networks, platform accountability, and extensive legal protections.

Cross-sector collaboration between legislators, tech developers, educators, and activists is desperately required as technology advances in order to establish safer online spaces. In the era of artificial intelligence and widespread internet access, addressing these challenges is crucial for maintaining human dignity, promoting gender equality, and ensuring individual justice.

KEYWORDS: Revenge Porn, Deepfakes, Digital Privacy, Women's privacy and rights, Artificial Intelligence, pornography, illicit crimes, consent.

REVENGE PORN

MEANING: refers to the non-consensual publishing of intimate photos or videos, generally by a former partner, with the intention of hurting, ridiculing embarrassing, or humiliating the subject. It involves posting nude images and videos of the subject without their consent altogether impacting the victim psychologically, socially and economically. Revenge porn is also known as Image Based Sexual Abuse (IBSA).

ETYMOLOGY: The term "revenge porn" is a combination of two words – "revenge" which means retaliation or punishment for a perceived wrong act or conduct and "porn" is a short for pornography, referring to sexually explicit material

MOTIVE/PURPOSE: The motive behind posting such sexually explicit content may include:

1. **Acts of revenge** – Sharing such explicit content to punish, humiliate or emotionally hurt someone, often after a breakup or personal conflict.

2. **Entertainment** – Uploading explicit material purely for amusement, shock value or for

    attracting attention without regard to the victim's consent.

3. **Political reasons** – disseminating such content to blackmail, tarnish or discredit the reputation of political opponents, leaders or public figures.

4. **Financial Gains** – Blackmailing, extortion or selling the content for financial gains.

5. **Humiliation –** In order to shame or publically embarrass the subject.

HISTORY:

1. PRINT ERA (Pre Internet – Early 1990s)

    Distribution in print era was physical in form of photos, magazines, letters etc. There was non- explicit sharing and distribution of content like private Polaroid or film developing staff making unauthorized copies. However, such incidents were rare and localized and they were viewed with the lens of breach of privacy or reputational harm, since, the term "revenge porn: didn't exist back then. "Though the advent of photography likely marks the first opportunity for

> **DID YOU KNOW??**
> Before digital threats, people engaged in postal blackmail threatening to pose compromising printed photos to families, employers or spouses unless paid off.

revenge porn, one of the oldest known incidents dates to the 1950's when Marilyn Monroe agreed to be photographed nude, only to have the photos surface years later on the cover of Playboy magazine without her consent in 1953."[1]

During the print era, film cameras such as Polaroid were used to capture private images. However, the spread was easy to contain at that time because the content couldn't be widely spread due to expensive reproduction of copies and narrow distribution channels. Because there was no photography or digital media throughout the ancient and mediaeval periods, the idea of "revenge porn" as we know it now did not exist. Nonetheless, retaliation via disclosing personal or sensitive information continued to happen. Women's honour and virginity were closely linked to family reputation in patriarchal countries. After a breakup or rejection, men would occasionally spread letters, poems, or rumours that implied a woman's sexual behaviour or infidelity. These behaviours had comparable functions to contemporary revenge porn: punishment, control, or humiliation. Even accusations, whether written or spoken, had the power to destroy a woman's life because virginity and chastity were highly valued.

There were no specific laws regarding the invasion of privacy, hence recourse was taken under the general law for defamation, voyeurism, harassment but very few victims pursued it due to the fear of society. For instance, ex partners share intimate pictures in physical format to extract revenge from their partners. Further, in tabloid culture intimate photos of celebrities that have been stolen or leaked are occasionally published by magazines.

2. **Digital ERA (Mid 1990s-2020)**

When photography was developed in the nineteenth century, individuals started making intimate, personal portraits. It was feasible to create sexual or nude photos by the late 19th century. Intimate photos were occasionally shared between partners, despite the scarcity of cameras and restricted access. When relationships ended, abandoned lovers, usually men, could threaten to sell these images to underground collectors, brothels, or newspapers. Although technology constraints prevented extensive distribution, the threat was immensely harmful because of the fear of

---

[1] Fallik Seth Wyatt, Stone Erika, Victory Danielle, Markevitch Taylor, Salvo Ronaldo, Mallalieu Lexis, "A Critical Content Analysis of the Nation's Laws and Reflection upon Social Science Researc", November 30, 2021, *Available at:* https://scholasticahq.com/criminology-criminal-justice-law-society/

scandal in a time when social conservatism was prevalent.

Intimate image retaliation grew increasingly widespread as mass media and photography developed. Polaroids and film cameras made it possible for couples to take private photos in the middle of the 20th century without hiring a professional photographer. Public figures and celebrities started to be targeted, and private images were occasionally leaked to publications like Playboy or Hustler under the pretence of "exposing secrets." These disclosures had a similar impact—damaging reputations, breaching privacy, and advancing personal or economic agendas—even if they weren't always classified as revenge porn.

The prevalence of digital cameras, emails, and online forums in the 1990s and early 2000s led to a rise in the volume and velocity of non-consensual image sharing. It was now simple for ex-partners to email nude photos to friends, relatives, or employers or post them to websites. Users would publish obscene images along with personal information on early revenge porn websites and online communities. Because the internet provided anonymity and regulations were out of date, victims had little options. The economic, social, and psychological costs were high, and women were disproportionately targeted.

As social media and smartphones proliferated, revenge porn became a worldwide problem. Images and videos could be supplied voluntarily or covertly, then later uploaded online as retaliation. Until more stringent regulations were put in place, websites like Facebook, Twitter, and Reddit became hubs for this kind of content. As public indignation increased, victims started to speak up. As a result of activists' efforts to amend the legislation, revenge porn is now illegal in several nations. Although enforcement remained uneven, high-profile cases— such as those involving celebrities or viral leaks—helped increase awareness

3. 2020S: THE DEVELOPMENT OF IMAGE-BASED ABUSE, DEEPFAKES, AND AI

Tech made revenge porn more complex in the 2020s. AI-generated movies that have someone's face superimposed on another person's body, or "deepfake" technology, have emerged as a new kind of image-based abuse. Now, victims could be taken advantage of without ever exchanging private information. This change signalled a risky progression from leaking authentic content to creating explicit media. Platforms rushed to identify and eliminate such content, while laws found it difficult to keep up.

Consent, digital rights, and the psychological anguish of being exposed or impersonated online became hot topics in public conversation.

4. <u>**CURRENT AND FUTURE: GLOBAL MOVEMENT FOR ETHICAL TECHNOLOGY AND DIGITAL CONSENT**</u>

Retaliation porn is now widely acknowledged as a grave invasion of privacy and consent. Laws that criminalise it have been passed in several nations, though enforcement and penalties differ. Some social media companies utilise artificial intelligence (AI) to identify and filter non- consensual content. Respectful interactions and digital consent are currently the focus of educational initiatives. There are still difficulties, nevertheless, particularly in areas without well-defined legal frameworks or support networks. In order to safeguard people against image-based sexual assault in all of its changing manifestations, ethical norms, legal frameworks, and public awareness must develop together with technology.

<u>REVENGE PORN AND DEEPFAKE IN INDIA</u>

Deepfakes are artificial intelligence (AI)-generated changes that frequently insert a person's image into graphic scenes without the subject's knowledge. When deepfake technology is used to create sexually explicit content with someone's appearance or likeness without their knowledge, usually for the purpose of humiliation or exploitation, this is known as revenge porn. By avoiding proof of validity and making it more difficult to contest or remove the content, this fusion increases the harm. **Babydoll archi case: ai-powered revenge porn:** One of the most alarming deepfake incidents in India involved the viral Instagram persona "Babydoll Archi." "Created by Pratim Bora from Assam, this AI-generated influencer gained over 1.3 million followers by blending one photo of his ex- girlfriend with seductive content using tools like Midjourney, Desire AI, and OpenArt AI. The purpose initially was harassment; soon, it became a lucrative enterprise, earning an estimated ₹10 lakh via subscription links."[2] The real woman suffered deep reputational harm before Bora's arrest prompted discussions on AI ethics, cyber law reform, and digital literacy in India. These incidents demonstrate how deepfakes add anonymity, scalability, and deniability to the conventional revenge porn

---

[2] Jaiswal Nancy, IndiaTimes, Babydoll Archi wasn't real: How a viral AI Instagram star was built on one real woman's photo for fame, revenge and profit. (2025, July), *Available at: https://www.indiatimes.com/trending/babydoll-archi- wasnt-real-how-a-viral-ai-instagram-star-was-built-on-one-real-womans-photo-for-fame-revenge-and-profit- 663942.html?utm_source=chatgpt.com*

paradigm. The absence of deepfake-specific laws presents difficulties for law enforcement, while victims frequently find it difficult to demonstrate the content's untruth.

Deepfake pornography directed against women is becoming more common both internationally and in India, deterring their engagement in public life and strengthening restrictions on their ability to express themselves and exercise digital agency.

The convergence of deepfake technology and revenge porn represents a disturbing evolution in digital abuse, especially in the Indian context where technological advancement often outpaces legal safeguards. Deepfakes involve the use of artificial intelligence to fabricate hyper-realistic videos or images, often placing a person's face onto another's body in sexually explicit or compromising contexts. When these manipulated visuals are created and disseminated without consent— particularly to harass, shame, or retaliate against women— they constitute a form of revenge porn. This intersection significantly amplifies harm by enabling perpetrators to exploit public or social media images to manufacture fake but convincing pornographic content, even without access to private or real intimate materials.

Particularly in India, where technological innovation frequently surpasses legal restrictions, the combination of deepfake technology with revenge porn suggests a troubling evolution in digital abuse. Artificial intelligence is used in deepfakes to create incredibly lifelike films or pictures, frequently superimposing a person's face on another's body in revealing or sexually explicit situations. These altered images are considered revenge porn when they are produced and shared without permission, especially to harass, embarrass, or retaliate against women. By allowing offenders to create false but convincing pornographic content using public or social media images— even in the absence of access to actual or private intimate materials—this junction greatly increases harm.

"As the production of increasingly realistic synthetic images, videos and audio of people saying and doing things they never did becomes possible, new forms of harassment, fraud, political manipulation and non-consensual intimate imagery have been enabled"[3] In addition to causing serious emotional and reputational harm to victims, deepfakes and other synthetic media have the potential to "erode public trust in authentic content" during crucial times like elections.

---

[3] V. Smith, "Deepfake Risks and Ethical Considerations," Journal of AI Security, vol. 5, no. 2, pp. 45-62, 2024

NOTABLE CASES HIGHLIGHTNG THE ISSUE

Baby Doll Archi Case: An impressive illustration of revenge porn possible via deepfake: The Instagram account "Babydoll Archi" was made by an Assamese mechanical engineer based on a single image of his former fiancée. Using programs like Midjourney and OpenArt, he produced suggestive AI material and made up to ₹10 lakh from subscriptions. The victim experienced widespread humiliation, psychological pain, and harm to their reputation. National discussion on AI abuse, cyber defamation, and the need for stricter digital laws was spurred by Bora's imprisonment. **The Deepfake FIR in Lucknow:** When the wife of a government doctor noticed her husband's image in a pornographic film, she filed a formal complaint; he denied any involvement and said the video was a deepfake. This instance highlights the growing abuse of deepfakes for retaliation or personal slander.

State of West Bengal v. Animesh Boxi (2018): "Court treated the victim as a rape survivor and provided her appropriate compensation"[4]. In today's era of technological advancement, even our personal electronic device is not safe anymore. One can easily recollect the 2014 Apple iCloud hack in pornographic materials of various Hollywood celebrities was released online. A person of any age or gender can become a victim of this offense. One can become victims of such heinous crimes because of slightest carelessness, so the only primary prevention is to be attentive always and everywhere because blind trust is a curse.

Subhranshu Rout v. The State of Odisha: this case also tells the tale of the criminal's retaliation, in which an innocent girl is the victim of a revenge porn crime. In this instance, the victim had to fight hard to file the FIR because the police did not take any action in response to the victim's initial written report to the IIC. " By highlighting the significance of the "right to be forgotten"—that is, permanently removing the photo from the server—in the context of the victim's right to privacy, the Hon'ble Court declined to grant bail to the offender, ruling that the offender had infringed upon this right."[5]

Suicide Caused by Threats of Revenge Porn in Kendrapada, Odisha: The disastrous effects of threats of revenge porn are best illustrated by a recent tragic instance from Kendrapada,

---

[4] India Law Offices. (n.d.). Revenge Porn or Non-Consensual Pornography. *Available at* *https://www.indialawoffices.com/legal-articles/revenge-porn-or-non-consensual-pornography*

[5] The Legisprudence. (2021, April 22). "Revenge porn-online abuse and Indian law." *Available at:* https://thelegisprudence.wordpress.com/2021/04/22/revenge-porn-online-abuse-and-indian-law/

Odisha. Following their separation, a 20-year-old college student committed suicide by self-immolation because her ex-boyfriend threatened to share her private images. After the girl's family made a formal complaint, "the accused was detained on charges of abetment, highlighting the way that privacy invasions and cyber-harassment may cause severe psychological pain."[6]

Defamation Case in Surat: Unconsented Instagram Leaks:In a another recent Surat incident, "a 19-year-old lady accused a former acquaintance of defaming her after forcing her to share her naked photos via a video call and then sharing them on a phoney Instagram account."[7] The perpetrator shared the photos with her friends and family after she refused to comply any further. The victim filed formal complaints under the IT Act and the BNS, illustrating how contemporary technology permits unconsented image distribution and damage to one's reputation.

From historic court decisions to horrifying personal tragedies and developing cybercrimes, these incidents highlight the various aspects of revenge porn in India, highlighting the advantages and disadvantages of the country's legal and societal reaction systems.

LEGAL FRAMEWORK IN INDIA

Although there isn't a particular legislation in India called "revenge porn" or "deepfake law," many clauses in the country's current cyber, criminal, and data protection laws address various facets of these offences. The relevant laws are broken out per section below.

Section 66E: Privacy Violation. This occurs when someone takes, sends, or publishes pictures of someone else's intimate areas without that person's permission. Penalty is A fine of up to ₹2 lakh, three years in prison, or both. This is employed when private photos or videos are distributed without permission.

Section 66C: Identity Theft applies when someone exploits another person's password, electronic signature, or distinctive identifying feature dishonestly or fraudulently.Penalties include up to three years in prison and/or a fine of ₹1 lakh. Relevance: Used in impersonation-

---

[6] Times of India. (2025, July 15). "Teen files defamation complaint after nude photos leaked on Instagram. Times of India." *Available at:* https://timesofindia.indiatimes.com/city/surat/teen-files-defamation-complaint-after-nude- photos-leaked-on-instagram/articleshow/122526580.cms

[7] Times of India. (2025, August 14). *Man held for uploading woman's morphed photos online*. *Times of India. Available at:* https://timesofindia.indiatimes.com/city/coimbatore/man-held-for-uploading-womans-morphed-photos- online/articleshow/123289505.cms

based deepfake instances.

Section 66D: Personation Cheating using Computer Resources When Using technology to pose as someone else in order to commit fraud. Penalties include up to three years in prison and/or a fine of ₹1 lakh. Relevance is Vital in deepfake situations, particularly those that result in harassment or defamation

Section 67: Prohibitive Content in Digital Format. When disseminating pornographic material online. Penalty is ₹5 lakh fine and/or up to 3 years in prison for the first conviction; up to 5 years in prison for successive convictions. Relevance is often utilised in deepfake and revenge porn.

Sexually Explicit Content (Section 67A): When it applies: Disseminating sexually explicit content that depicts real or imagined sexual actions. Penalty is of fine of ₹10 lakh or up to five years in prison.Applies even if the act is digitally manufactured, it covers deepfake porn.

Bharatiya Nyaya Sanhita, 2023(BNS)

The BNS, which replaced the IPC, modernises and broadens the scope of several offences to better address cybercrimes.

Section 73: Expressions, Motions, or Behaviour Meant to Disrespect a Woman's Dignity. This section is comparable to IPC 509 includes actions intended to degrade a woman's dignity that are done orally, in writing, or visually.It is helpful in cases of public humiliation including revenge porn and deepfakes.

Section 77: Stalking under this section includes persistent online activity monitoring and digital stalking. It is employed in persistent harassing or information dissemination.

Section 79: Regarding Voyeurism It is illegal to record intimate moments without permission, much like the preceding 354C. Particularly relevant to revenge porn that comes from compromised material.

Section 318 deals with Impersonation. Use of AI/deepfake techniques for digital impersonation is punishable under this section Deals directly with deepfake identity deception.

Digital Personal Data Protection (DPDP) Act, 2023

Consent-Based Data Usage Explicit authorisation is required for any use of personal data, including voice, likeness, and pictures. This legislation is broken by deepfakes that use private images. Redress of Grievances: Data Protection Board may receive reports from victims of data misuse. Relevance: Encourages victims of deepfake or revenge porn to pursue civil remedies

Act of 2023 Amendments to the Indian Evidence Act

Authenticating evidence can be made more difficult by deepfakes. Section 65B remains critical mandating certificates for electronic evidence. Videos and photos must be verified by courts before they may be admitted as admissible evidence.

CONCLUSION

In India, the convergence of women's privacy and deepfake-enabled revenge porn represents a troubling combination of gender bias, legal lag, and AI technology. Synthetic sexual material damages victims' mental health, damages their reputations, and violates their constitutional right to privacy, as demonstrated by cases such as Rashmika Mandana deepfake case or Ranveer Singh's deepfake case. Even while it covers pertinent topics like voyeurism, obscenity, and defamation, India's current legal system is nonetheless ill-equipped to handle this new arena.

In order to restore digital dignity, India has to implement legislations targeting deepfakes, require platform accountability, improve AI detection, increase cyber-forensic capabilities in rural areas, and facilitate victim-centered assistance. Equally important are inclusive legal frameworks and education efforts. India can pave the way for safeguarding women's fundamental right to privacy in the AI era by fusing technology investment, legislative innovation, and societal empathy.