
JUDICIAL APPROACH IN DIGITAL ERASURE: EXPLORING THE OBSTACLES VICTIMS FACE WHEN REMOVING EXPLOITATIVE AI CONTENT ONLINE

Vijayaraghavan K, LLM, School of Criminal Law and Criminal Justice Administration,
Tamil Nadu Dr. Ambedkar Law University, School of Excellence, Taramani, Chennai,
Tamil Nadu, India

ABSTRACT

The rapid proliferation of generative artificial intelligence (AI) has led to a surge in non-consensual AI-generated exploitative content, disproportionately targeting vulnerable individuals. The article exposes the role of judiciary in removing the obstacles that victims encounter when attempting to permanently erase this material from the internet. The systemic barriers to effective digital erasure were investigated based on the technological, legal and institutional frameworks. The technical limitations, rapid automated replication of data across decentralized networks and the inability of standard hashing mechanisms to detect minor AI alterations, render content removal akin to an endless game of whack-a-mole. The legal and regulatory fragmentation creates jurisdictional voids, as existing privacy and copyright laws are ill-equipped to handle synthetic data that does not utilize a victim's actual photograph. Furthermore, it explores the obstacles embedded within platform reporting architectures, where opaque, automated takedown processes often place an exhausting evidentiary burden on the victim. Consequently, victims suffer prolonged psychological, social, and economic trauma. While digital abuse inflicts irreversible psychological and reputational trauma, current judicial and regulatory frameworks remain profoundly ill equipped to facilitate timely digital erasure. This study critically examines the legal, technical, and systemic barriers that victim-survivors encounter when trying to purge malicious, AI-generated material from the internet. These challenges are heavily compounded by jurisdictional impasses and the anonymous, borderless spread of content across decentralized networks.

Keywords: Judicial, digital erasure, right to be forgotten, DPDP Act, IT Act, EU-GDPR.

1. Introduction

The rapid democratization of generative artificial intelligence (AI) has fundamentally altered the landscape of digital harm, transforming synthetic media generation from a specialized technical feat into an accessible, institutionalized weapon of interpersonal violence. At the vanguard of this paradigm shift is the proliferation of non-consensual deepfake pornography (NCDP) and non-consensual altered media (NCAM) finds its way into social networks. These technologies allow bad actors to superimpose real human likenesses onto explicit or defamatory material with terrifying photorealism. While the initial generation of these assets requires mere seconds and nominal technical literacy, the subsequent effort required to eliminate them a process termed "digital erasure" which presents an asymmetrical, often insurmountable challenge for victims. Once exploitative AI content enters the modern hyper-connected digital ecosystem, it becomes functionalized across distributed networks, leaving victims trapped in an adversarial relationship with the very infrastructure of the internet.¹ The digital erasure concept ensure the victim is not subjected to secondary victimization by adopting the process of permanent deletion, de-index, or suppress harmful data, but such erasure faces unprecedented resistance when this concept is applied to AI systems. Unlike traditional digital content hosted on a discrete server, AI-generated content is uniquely challenging to eradicate. Once data is absorbed into an AI model's training dataset, it is encoded across billions of neural weights and parameters. De-indexing a URL from a search engine does not "unlearn" the underlying pattern from a generative model. Victims are caught in a crossfire of legal and technical bottlenecks, including hostile platform reporting structures, jurisdictional enforcement fractures, and inadequate statutory frameworks written before the emergence of hyper-realistic synthetic media.²

This systemic crisis disproportionately targets women, minors, and marginalized communities, establishing new vectors for digital stalking, corporate extortion, financial ruin, and profound psychological trauma. The weaponization of AI content leverages systemic vulnerabilities within existing socio-technical systems, transforming online platforms into vectors of viral amplification. Unlike conventional image-based sexual abuse (IBSA), which historically relied

¹ Citron, D. K. (2022). *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. W. W. Norton & Company.

² Qiwei, L., Kennon, K., Bedera, N., Eaton, A.A., Gilbert, E., and Schoenebeck, S. 2026. Platforms as Crime Scene, Judge, and Jury: How Victim-Survivors of Non-Consensual Intimate Imagery Report Abuse Online. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain. ACM, New York, NY, USA, 19 pages. <https://doi.org/10.1145/3772318.3791115>

on the theft or breach of actual intimate imagery, generative AI enables the infinite fabrication of synthetic intimacy out of entirely public, mundane photographic data. A victim's professional headshot on LinkedIn or a casual selfie on Instagram can be instantly recontextualized into high-definition explicit material. This architectural shift fundamentally alters the nature of digital vulnerability: privacy is no longer compromised by a failure of personal data hygiene, but rather by the mere state of maintaining a visible digital existence.³

While the engineering frameworks behind generative adversarial networks (GANs) and diffusion models advance at an exponential trajectory, the countervailing legal, technological, and bureaucratic mechanisms required to enforce digital erasure remain fragmented, reactive, and chronically underfunded. Victims attempting to purge their likenesses from the internet must navigate an adversarial labyrinth characterized by siloed platform-specific reporting architectures, inconsistent and geographically bounded regulatory frameworks, and non-compliant hosting providers protected by jurisdictional shields. The structural inertia of regulatory bodies, combined with corporate liability exemptions, has effectively shifted the entire economic and operational burden of content moderation onto the aggrieved individual.^{4,5} This paper explores the multi-faceted systemic obstacles that victims confront when pursuing digital erasure of exploitative AI content. Eventually, this analysis underscores how the judiciary balances the socio-technical architecture of the internet that prioritizes corporate infrastructure and technological velocity over individual bodily autonomy and digital safety.

2. Differences in Scope and Execution of Digital Erasure and Right to be Forgotten

- **Scope:** Digital erasure deals directly with data containers (hard drives, solid-state drives, magnetic tapes). It ensures that once a file is marked for deletion, no forensic software can recover the binary code. In contrast, RTBF focuses on the accessibility of data. When someone exercises RTBF (such as against a search engine or news site), the underlying file or web page might still exist on a server, but it is unlinked, de-indexed,

³ Umbach, R., Henry, N., Shelby, R., Stevens, G., and Gonzalez-Pons, K. 2026. AI-generated image-based sexual abuse: Perpetration and consumption across three regions. *Computers in Human Behavior*, 179, 108935. <https://doi.org/10.1016/j.chb.2026.108935>

⁴ Nfissi N. 2025. Protecting human rights in the digital age: Legal frameworks and media literacy as a complementary safeguard, *Digital Law Journal*, 6(3), 1-26. <https://doi.org/10.38044/2686-9136-2025-6-10>

⁵ Nicola, H. Rebecca, U., Renee, S., Gemma, B., and Lisa, M. 2026. It's still abuse: community attitudes and perceptions on AI-generated image-based sexual abuse, *Information, Communication & Society*, DOI: 10.1080/1369118X.2026.2613437

or hidden from public search queries matching the person's name (Table 1).⁶

Table 1. Comparison of digital erasure and right to be forgotten in Indian context

Feature	Digital Erasure (DPDP Act, Sec 12)	Right to be Forgotten (Art. 21 Jurisprudence)
Legal Basis	Statutory Law (DPDP Act, 2023)	Constitutional Law (Article 21 via courts)
Target Entities	Data Fiduciaries (apps, banks, tech companies, e-commerce)	Search engines, online news archives, legal repositories
Typical Scenario	Deleting your account and personal history from a food delivery app.	Asking Google to de-index an old news article about an arrest from which you were acquitted.
Type of Action	Absolute removal of data fields from a corporate database.	De-indexing or masking a name from search engine queries (the data exists, but it's hidden).
Major Hurdle	Subject to compliance rules and structural retention periods mandated by other laws (like RBI rules).	Clashes directly with Article 19(1)(a) (Freedom of Speech / Right to Information of the public).

- **Enforcement and Standards:** RTBF is invoked through formal legal requests or statutory rights (like under European data laws). It is subject to legal exceptions, such as public interest, journalistic freedom, or legal compliance. Digital erasure does not weigh public interest or free speech; it is a mechanical procedure guided by technical benchmarks (like overwriting sectors or cryptographic erasures) to meet confidentiality levels.
- **Intersection:** When an individual successfully claims their Right to be Forgotten under data protection laws, the data controller is legally mandated to perform digital erasure

⁶ Regenscheid, A., Feldman, L., and Witte, G. 2015. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917935 (Accessed September 5, 2026)

or instruct third-party platforms to purge the data from their active and backup systems. However, you can perform digital erasure without invoking RTBF (e.g., when securely wiping an old laptop before selling it), and an RTBF request does not always guarantee absolute physical erasure if legal retention or public archiving exemptions apply.

3. Digital Erasure

The origin of digital erasure spans two distinctly different contexts: legal privacy jurisprudence (the right to delete online traces) and technological data sanitization (the software process of permanently overwriting storage media).

1. Legal and Privacy Origin: The "Right to be Forgotten"

In privacy law, digital erasure is fundamentally tied to the evolution of the Right to be Forgotten (RTBF).⁷

- **Pre-Digital Roots:** The conceptual framework originates in European legal traditions, specifically the French concept of *le droit à l'oubli* (the right to oblivion) and the Italian *diritto all'oblio*. Historically, this allowed rehabilitated criminals who served their sentences to legally object to the media perpetually bringing up their past misdeeds, allowing them to socially reintegrate.⁸
- **The Digital Leap (2014 Google Spain Ruling):** The modern concept of digital erasure gained massive global prominence following the landmark 2014 *Google Spain v. AEPD* ruling by the Court of Justice of the European Union (CJEU). A Spanish citizen, Mario Costeja González, argued that outdated search results about his past financial debts violated his privacy. The court ruled that individuals have the right to request search engines to de-index links containing personal data that is outdated or irrelevant.^{9,10}

⁷ Park, R. 2022. Forgiving Without Forgetting? Privacy in an Age of Digital Permanence. Political Science Honors Projects. 96. https://digitalcommons.macalester.edu/poli_honors/96

⁸ Dhingra, K., and Tyagi, K. 2025. Historical development of the right to be forgotten, *International Journal of Advanced Legal Research*, 5(4) 1-10

⁹ Allegri, M.R. 2022. The Right to be Forgotten in the Digital Age. In: Comunello, F., Martire, F., Sabetta, L. (eds) *What People Leave Behind*. *Frontiers in Sociology and Social Research*, vol 7. Springer, Cham. https://doi.org/10.1007/978-3-031-11756-5_15

¹⁰ *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, ECLI:EU:C:2014:317

- **Codification in GDPR (adopted 2016/ enforced 2018):** This ruling was officially codified as a statutory framework under Article 17 of the General Data Protection Regulation (GDPR), explicitly titled the "Right to Erasure".¹¹

2. Technological Origin: Data Sanitization

In computer science, data erasure emerged from the structural necessity to destroy information without destroying physical hardware. The erasure methods include (but are not limited to) viz: (a) **Secure wiping**: Overwriting existing data with random undecipherable patterns multiple times; (b) **Cryptographic erasure**: Deleting the encryption keys that protect encrypted data, rendering the encrypted data unreadable; (c) **Factory reset plus**: Enhanced versions of manufacturer reset procedures with additional security measures; (d) **Targeted data removal**: Selectively removing specific files or datasets while preserving others.¹²

- **The Problem with Early Deletion:** Historically, using standard operating system "delete" commands or formatting a drive only removed the file's index pointers, leaving the actual binary data intact on the disk magnetic platters until it was naturally overwritten. Anyone with basic forensic tools could retrieve the information.
- **The 1995 DoD Standard:** To standardize secure digital erasure, the U.S. Department of Defense published the DoD 5220.22-M standard in 1995. It introduced the concept of clearing and sanitizing digital media by overwriting sectors multiple times with specific patterns of ones and zeros.¹³
- **The 1996 Gutmann Method:** In 1996, computer scientists Peter Gutmann and Colin Plumb introduced a highly secure 35-pass data-shredding algorithm designed to securely erase data from magnetic hard drives against advanced laboratory-level forensic recovery techniques.¹⁴
- **Modern Standards:** Today, technological digital erasure is governed primarily by the NIST SP 800-88 Rev 1 guidelines (issued by the National Institute of Standards and

¹¹ European Parliament and of the Council (General Data Protection Regulation - EU) 2016/679

¹² <https://www.clicdata.com/blog/data-destruction-vs-data-erasure-processes/>

¹³ U.S. Department of Defense. (1995). *National Industrial Security Program Operating Manual* (DoD 5220.22-M). U.S. Government Printing Office.

¹⁴ Gutmann, P. 1996. Secure deletion of data from magnetic and solid-state memory. In *Proceedings of the 6th USENIX Security Symposium* (p. 8). USENIX Association.

Technology), which recognize digital overwrite, block erase, and cryptographic erasure as valid methods of sanitization.^{15,16}

3.1 Digital erasure in AI model or blockchain network

Digital erasure is fundamentally limited by the way modern computing systems store, replicate, and optimize data. Once information enters a complex ecosystem like an AI model or a blockchain network, completely deleting it is mathematically and architecturally challenging. The technical barriers to digital erasure across these two major paradigms viz:

3.1.1 AI Training Data: The "Membrane" Problem

In AI, you cannot simply press "delete" on data used to train a neural network. The data has already been digested into billions of mathematical weights.

- The Black Box of Machine Learning: When a model trains on an image or text, it doesn't store a copy of the file; it adjusts its internal parameters (weights) to learn patterns. There is no isolated folder labeled "User X's Data" to delete.
- Catastrophic Forgetting: To erase a specific subset of data using machine unlearning, engineers must update the weights so the model "forgets" that data without destroying everything else it learned. Currently, forced forgetting often causes the model's overall performance to degrade sharply.
- Memorization and Overfitting: Large language models (LLMs) often accidentally memorize rare or highly repeated training examples (like phone numbers, specific code snippets, or copyrighted text). Extracting these specific memorized vectors without retraining the entire model from scratch is an unsolved research problem.
- The Cost of Retraining: For large models, the only 100% reliable way to remove data is to purge it from the raw training dataset and retrain the model. This costs millions of

¹⁵ Blancco. (n.d.). *What's behind the global shift to data erasure?* GovInsider. <https://govinsider.asia/intl-en/article/whats-behind-the-global-shift-to-data-erasure>

¹⁶ Kissel, R., Regenscheid, A., Scholl, M., and Stine, K. 2014. *Guidelines for media sanitization* (NIST Special Publication 800-88 Rev.1). National Institute of Standards and Technology. doi.org

dollars and takes weeks or months, making real-time erasure requests (like GDPR "Right to be Forgotten" mandates) highly impractical.

3.1.2 Blockchain: Immutability by Design

Blockchains were explicitly engineered to prevent data deletion. Overriding this core feature introduces severe security vulnerabilities (Table 2).

- **Cryptographic Chaining:** Each block in a ledger contains a cryptographic hash of the previous block. If you alter or delete data in block 10, its hash changes. This breaks the link to block 11, invalidating the entire subsequent chain.
- **Decentralized Replication:** A blockchain exists simultaneously across thousands of independent nodes globally. Even if one node operator agrees to erase data, the rest of the network will reject their altered version of the history during consensus validation.
- **Hard Forks as the Only Resort:** To truly wipe data from a blockchain's history, the community must execute a "hard fork"—effectively splitting the network into a new chain where that data never existed. This requires overwhelming political agreement among developers, miners, and users (e.g., the 2016 Ethereum DAO fork).
- **The Conflict with Privacy Laws:** Because public ledgers are immutable, putting Personally Identifiable Information (PII) directly "on-chain" creates a permanent legal violation under modern privacy frameworks.

Table 2 Engineering architectural trade-offs to bypass these limitations of digital erasure

Technology	The Workaround	How It Works	The Catch
Blockchain	Off-Chain Storage	Only cryptographic hashes or pointers are kept on the blockchain. The actual data sits in a traditional database or decentralized storage (like IPFS).	If the off-chain data is deleted, the blockchain still retains an indelible hash ("digital fingerprint") proving the data once existed.
Blockchain	Crypto-Shredding	Data is encrypted before being written to the	The ciphertext remains public forever. Future

		blockchain. To "delete" it, the encryption key is destroyed.	quantum computers or cryptographic breakthroughs could eventually decrypt it.
AI Training	Sparsity & Modular AI	Models are broken into smaller, specialized sub-networks or "experts."	It limits the cohesive, emergent reasoning capabilities found in massive, unified models.

4. Algorithmic Disgorgement

The algorithms of large language models and generative AI services are developed by huge amount of data during training process. The developer intends the models to establish a patterns or prediction in the existing data till it attains higher level of accuracy. Thus the appetite for data arose in-order to ensure higher usefulness of the developed algorithms. Hence leading the AI firm to neglect commitment on data privacy.¹⁷

5. Obstacles to Erasure

1. **The Abstract Ingestion Hurdle:** As seen in *Anil Kapoor*, AI does not just copy files; it extracts "style" and biometric attributes. Traditional laws require an exact copyright or trademark match to trigger a takedown, creating an obstacle when trying to erase an AI image built entirely from scratch that merely *looks* identical to a victim.
2. **The "Index vs. Server" Illusion:** As highlighted in *Jorawer Singh Mundy*, removing content from search engine indexes (de-indexing) leaves the actual data alive on the host server or deep within an AI's model weights. True digital erasure requires technical unlearning, which Indian infrastructure is still struggling to enforce on foreign-hosted tech platforms.

6. Judicial Pronouncement under India context

The Madhavan 2026 case deals with unidentified actors utilized generative AI tools to clone the voice, facial features, and overall likeness of actor and created deepfake videos, fake endorsements, and unauthorized promotional content without his consent. The content was

¹⁷ Sokler, B.D., Hecht, A., Fjeld, C.T., and Raj, G. Algorithmic Disgorgement: An Increasingly Important Part of the FTC's Remedial Arsenal — *AI: The Washington Report*, MINTZ, January 24, 2024

widely circulated across various platforms like YouTube and Instagram. The Delhi High Court granted an interim injunction protecting the plaintiff's digital identity. The Court held that an individual's digital persona, voice, and likeness are legally protected elements integral to human dignity under Articles 19 and 21 of the Indian Constitution. Technology cannot bypass the absolute requirement for user consent. The court ordered the immediate removal of the offending synthetic media and mandated that platform registrars reveal the identities of the anonymous creators.¹⁸

The Indian Computer Emergency Response Team (CERT-In) and the Indian Cyber Crime Coordination Centre (I4C) flagged that automated AI "nudification" bots hosted on the Telegram messaging app were being used to strip clothing from photos of women and children. Despite 35 structural consultation requests from Indian authorities, the encrypted platform failed to implement permanent technical blocks. The regulatory and judicial review firmly established that messaging platforms cannot act as passive pipelines when weaponized for non-consensual AI exploitation. The platform was legally ordered to enforce systemic bans on deepfake, sextortion, and child-exploitation material. The case illustrates the jurisdictional and structural nightmare of digital erasure on decentralized apps. When exploitative AI systems operate inside private, end-to-end channels or cloud-hosted bots, traditional public web de-indexing fails, requiring structural, architecture-level interventions against the app itself.¹⁹

The internet website indulged in using frayed public social media photos of emerging actress Khushi Kapoor and fed them into a generative machine learning system to create highly realistic, false commercial endorsements and derogatory synthetic photos. The Delhi High Court granted an extensive injunction protecting her identity from unauthorized AI exploitation. The court utilized dynamic enforcement, requiring internet service providers (ISPs) to automatically block any spin-off or mirror domains that copy the offending synthetic media. The primary obstacle in modern erasure is the "Whack-A-Mole" effect as AI content is infinitely scalable and easily mirrored. This case establishes that legal erasure must be dynamic; a single court order must apply adaptively to future domains that reappear with the exact same exploitative AI assets.²⁰

A customizable and pre-trained AI vocal models were hosted by Jammable Ltd., and other AI-

¹⁸ Ranganathan Madhavan v. G Filmz Studioz & Ors. CS(COMM) 1392/2025.

¹⁹ Telegram FZ LLC & Anr. v. Union of India & Ors. 2026 SCC OnLine Del 4750

²⁰ Khushi Kapoor v. Ashok Kumar/John Doe & Ors. CS(COMM) 869/2026

generation platforms which allowed users to clone the exact voice, singing style, and acoustic signature of playback singer Jubin Nautiyal. These models generated tracks and digital avatars without playback singer consent. The Delhi High Court granted an *ex parte ad-interim* omnibus "John Doe" injunction. The Court restrained the platforms from cloning his voice or imitating his singing style, ordering the immediate takedown of the infringing links and AI models. This case expanded digital erasure from static media files (like MP3s) to the underlying software mechanism. The Court recognized that allowing user-facing generative platforms to hold "cloned" acoustic weights presents irreparable harm to an artist's livelihood, legally forcing the deletion of the generative asset itself.²¹

In Pooja Ramesh Singh 2026 case dealt with corporate dispute tried by the tribunal. During the trial the tribunal admitted insolvency applications and later passed orders as the same was put forth with a series of legal precedents. While examining insolvency application it was found that the advocate adopted AI drafting tools. Further examination revealed the output was completely fake and hallucinated by generative AI drafting tools. The appellate tribunal however upheld the order regardless. The Supreme Court of India set aside the orders and declared a zero-tolerance policy for unverified AI-generated precedents in the legal process. The Court held that any decision resting on fake or hallucinated material is a nullity and "amounts to subversion of the rule of law." While not a case about personal exploitation, this landmark ruling establishes the ultimate hurdle of judicial erasure: AI-generated fiction can corrupt permanent public records. The Supreme Court ruled that citing unverified AI precedents constitutes professional misconduct for lawyers and a serious judicial lapse for judges.²²

Actress Sonakshi Sinha discovered that AI platforms (viz: Character.ai) hosted interactive, hyper-realistic chatbots simulating her personal identity and generating objectionable, unauthorized textual and synthetic outputs. The Delhi High Court indicated it would pass protective orders but strictly directed the plaintiff to compile and file a clear, defendant-wise structured table of specific infringing URLs. Due to the highly sensitive nature of the deepfake material, the court allowed certain documents to be placed in a sealed cover. This highlights a massive procedural hurdle for victims attempting digital erasure. Courts cannot simply issue a blanket order to "delete all references." Victims bear the exhausting, technically demanding

²¹ Jubin Nautiyal v. Jammable Ltd. & Ors., CS(COMM) 166/2026

²² Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd., 2026 INSC 668

administrative burden of mapping out every single dynamic URL and deepfake instance across borderless AI infrastructures before relief is finalized.²³

Fabricated deepfake video clips and synthetically cloned audio of Mumbai-based rheumatologist and prominent spiritual leader "Sadguru Shree Aniruddha Babu" were circulated across social media platforms to falsely depict him for the statements he had never made. The Delhi High Court granted an *ex-parte* interim injunction, recognizing that a person's digital identity and the sanctity of their public discourses are protected attributes of their personality and dignity. This case is a major step forward because it shifts the focus of digital erasure away from just Hollywood/Bollywood "commercial properties." It confirms that any identifiable individual whose face or voice is synthetically hijacked to mislead the public has a constitutional right to demand immediate content suppression and deletion.²⁴

Anonymous commercial entities, online storefronts, and deepfake creators used the name, biometric likeness, historic cricketing imagery, and simulated voice of former Indian cricketer Yuvraj Singh. The data was weaponized across e-commerce platforms and AI chatbots to create unauthorized product promotions and synthetic face-swapped videos. The Delhi High Court granted an interim injunction, ruling that Singh possesses an exclusive right to protect his attributes. Crucially, the Court explicitly declared that "violators of personality and privacy rights need to be dealt with a heavy hand," ordering platforms to scrub the offending URLs. This ruling emphasizes that digital erasure must be absolute and forward-looking. The court granted the plaintiff the explicit liberty to apply the same order dynamically to any future AI-generated infringing instances without needing to file a fresh lawsuit. The court directed that uploaders must remove the infringing material within 48 hours. If they fail, intermediary platforms must take down the content within 36 hours of receiving the notice.²⁵

A highly realistic deepfake videos attributing fabricated political and personal statements to Member of Parliament Dr. Shashi Tharoor began spreading across social media networks, severely damaging his public reputation. The Delhi High Court issued an interim protection order directing major intermediaries, including Meta and X (formerly Twitter), to immediately remove, un-index, and block the specific deepfake audio-visual assets. This case bridges the gap between public interest and informational self-determination. The Court emphasized that

²³ Sonakshi Sinha v. Character Technologies Inc. and Others, CS(COMM) No. 275/2026

²⁴ Dr. Aniruddha Dhairyadhar Joshi v. John Doe / Ashok Kumar, CS(COMM) 178/2026

²⁵ Yuvraj Singh v. Ashok Kumar/John Doe & Ors., CS(COMM) No. 642/2026

in an era where digital records are virtually permanent, masking and erasing personal data from viral, synthetically corrupted streams is essential to preserving individual dignity.²⁶

The Member of Parliament Ravi Kishan, who is also an actor revealed that his digital identity, facial likeness, and vocal delivery had been harvested to generate deepfake video advertisements and synthetic marketing campaigns across virtual platforms without his permission. The High Court issued a sweeping ad-interim injunction restraining any unauthorized use of Kishan's identity via AI, deepfakes, or virtual platforms. The Court set a strict precedent for swift erasure by legally mandating that domain registrars and tech intermediaries (including Meta, Google, and X) must completely dismantle, disable, and remove the offending URLs within 72 hours of receiving the notice.²⁷

Over 44 entities, fake booking agents, and unmoderated websites leveraged generative AI tools to clone the voice and visage of Aman Gupta (co-founder of boAt Lifestyle and *Shark Tank India* investor) to execute fraudulent financial schemes, fake brand endorsements, and misleading social media ads. The Court granted a multi-target interim personality rights protection order, strictly restraining all 44+ defendants from unauthorized exploitation of Gupta's public persona. This case demonstrates that AI identity theft targets commercial leaders, not just performers. Because the fraud was distributed across separate domains, the court allowed an omnibus digital erasure approach, preventing tech platforms from claiming they lacked specific, individualized domain notifications.²⁸

The Member of Parliament Raghav Chadha approached the court seeking the removal of deepfake videos, morphed images, and synthetically altered audio-visual material circulating across major social platforms. The court noted that while political leaders have historically been subject to cartoons and satire, the deployment of hyper-realistic deepfakes that alter actual statements crosses into legal infringement. The Court ordered intermediary platforms to permanently disable and block access to the specific deepfakes. This case solidifies a 24-hour removal standard for high-priority personality violations. The court explicitly commanded tech platforms to execute the erasure within 24 hours from the receipt of the judicial order, bypassing standard internal corporate appeal queues.²⁹

²⁶ Dr. Shashi Tharoor v. Unknown Defendants & Ors., CS(OS) No. 312/2026

²⁷ Ravi Kishan v. Ashok Kumar/John Doe & Ors., CS(COMM) No. 490/2026

²⁸ Aman Gupta v. Artist Booking Company & Ors., CS(COMM) No. 355/2026

²⁹ Raghav Chadha v. Ashok Kumar John Doe & Ors., CS(OS) 466/2026

Anonymous bad actors deployed generative AI software to harvest the face, body likeness, and voice of actor Naga Chaitanya. The resulting data was weaponized to create deepfake pornographic videos, highly graphic explicit content, and unauthorized merchandise. This content was spread across adult portals and unmoderated chat platforms. The Delhi High Court granted urgent interim protection. The Court restrained all defendants and internet users from misusing his name, image, voice, or likeness in any AI-generated or pornographic material. It ordered tech platforms and internet service providers to immediately identify, disable, and erase the targeted URLs. This case positions deepfake pornography as an absolute breach of physical and bodily autonomy. The court held that forcing digital erasure is a fundamental requirement of human dignity under Article 21, establishing that a person's digital identity cannot be weaponized into explicit media without explicit consent.³⁰

A highly realistic deepfake videos emerged across social media platforms falsely depicting Union Minister Nitin Gadkari making controversial policy announcements regarding India's Ethanol-blended fuel policy. The viral synthetic content caused massive public confusion, prompting Gadkari to seek immediate erasure of the content to preserve both public interest and his reputation. The Bombay High Court issued a stern directive targeting social media platforms, including X Corp. The Court ordered the immediate removal of the original links and legally compelled the platforms to monitor for and dismantle "fresh objectionable content" matching the deepfake signature. This judgment combats the "Whack-A-Mole" obstacle of digital erasure. The Bombay High Court ruled that digital erasure cannot be a passive, static action. If a platform is notified that a specific AI video is a fabricated deepfake, the intermediary holds a continuous obligation to clear its system of subsequent mirrors or re-uploads of that exact file.³¹

In *Lakshmi Singh Yadav v. Union of India* (2026) a consolidated batch of over thirty separate petitions was filed by individuals who had been acquitted of criminal charges, or had their matrimonial/civil disputes resolved. Despite their legal exoneration, name-based searches on Google and legal repositories (like Indian Kanoon) prominently indexed their past accusations, destroying their careers and social lives. They sued for complete digital erasure. Justice Sachin Datta delivered a comprehensive judicial framework. The Court ruled that individuals should not face perpetual reminders of concluded past events. It issued binding, operational mandates

³⁰ Naga Chaitanya Akkineni v. Unknown Defendants & Ors., CS(COMM) No. 462/2026

³¹ Nitin Gadkari v. X Corp. & Ors. Interim Application (L) No. 25165 of 2026 in Suit (L) No. 25151 of 2026

ordering Google LLC and Indian Kanoon to disable name-based searches and mask the names/identifiers of the parties. This 2026 judgment is the first to layout the structural rules of digital erasure mechanics in India. It recognizes that while a public record must stay open for historical purposes, search engines cannot weaponize that record through automated algorithmic name-searches. It provides a blueprint for deepfake victims by shifting the practical burden of "forgetting" onto search engines and data intermediaries. The judgment established that open justice does not mandate permanent digital exposure via searchable commercial algorithms. The Court formulated a Three-Tier Test examining the nature of the outcome, public role, and accuracy/relevance of the information. The court further held that masking should be carried out through the originating court, while de-indexing must mirror globally effective.³²

An online entity developed unauthorized deepfake AI-generated videos and synthetic variations of trademarked fictional characters belonging to a prominent television series was distributed in commercial platforms and YouTube. The Court granted an *ex parte ad interim* injunction and a dynamic "John Doe" order. The court noted that synthetic manipulation of registered intellectual properties represents clear infringement of copyright and trademark frameworks. Because AI content spreads faster than victims can identify separate perpetrators, the court enabled a forward-looking erasure strategy. The "John Doe" order legally compelled unnamed websites, domain hosts, and tech platforms to proactively remove infringing synthetic items as soon as they were detected.³³

Karan Johar a filmmaker discovered that several online entities were adopting deepfake face-morphing tools and AI-driven voice cloning to place him in highly derogatory, vulgar, and commercially damaging simulated videos distributed across social media platforms. The Delhi High Court issued a sweeping ad-interim "John Doe" injunction, restraining all defendants and unnamed internet users from misusing Johar's name, image, voice, or persona through AI, machine learning, and deepfakes. Crucially, the court ordered Google and other social media platforms to systematically dismantle and block the content. The court explicitly recognized that deepfake technology inflicts severe, irreparable harm to human dignity under Article 21 of the Constitution. To overcome the obstacle of continuous re-uploads, the court established that tech platforms hold an ongoing responsibility to prevent the recurrence of the erased content

³² Laksh Vir Singh Yadav v. Union of India, W.P.(C) 1021/2016 & Connected Matters (Delhi High Court, 29 May 2026); Neutral Citation: 2026:DHC:4891

³³ Neela Film Productions Private Limited v. Taarakmehtakaooltahchashmah.com & Ors. CS(COMM) 690/2024

once notified.³⁴

Anonymous bad actors used deepfake face-morphing applications to create obscene, highly inappropriate, and *prima facie* defamatory videos resembling veteran actor Ajay Devgan, which was widely received across social networks. The Court issued extensive ad-interim directions forcing tech intermediaries to execute immediate takedowns. Crucially, it ordered the intermediaries to preserve and hand over the Basic Subscriber Information (BSI) of the unidentified uploaders. True digital erasure is impossible if the source is left intact to re-upload. This ruling establishes that Indian courts will treat erasure as a two-part remedy: immediate public containment (blocking links) combined with forensic identity unmasking (BSI tracking) to permanently neuter the threat at its source.³⁵

A highly realistic and sophisticated AI-generated deepfake video began circulating on YouTube and WhatsApp claiming that employees at the historic Taj Lake Palace in Udaipur were systematically poisoning guests. The Tata Group's Indian Hotels Company Limited moved the court, seeking emergency digital erasure of the video to prevent catastrophic damage to their commercial goodwill. The Delhi High Court observed that the content of the video was *prima facie* entirely false and severely damaged the hotel's reputation. The Court ordered a complete takedown and block of all YouTube channels and URLs hosting the AI-generated video. This case extends digital erasure protections to corporate victims of AI disinformation campaigns. The court recognized that because AI-generated video looks authentic, its potential to cause instant financial ruin to an enterprise requires the judiciary to act with immediate, *ex-parte* intervention to scrub the content from public view.³⁶

The unscrupulous online actors deployed deepfake audio-visual tools and voice cloning software to simulate the exact face, voice, and unique speech style of spiritual leader Sri Sri Ravi Shankar. The synthetic videos depicted him endorsing questionable medical remedies and making false scientific claims to sell illicit wellness products. The Delhi High Court granted interim protection. The court restrained unknown parties from using his likeness or style of delivery in any medium, specifically including AI-generated deepfakes and voice clones. Intermediaries like Meta were legally mandated to delete the offending content within a strict 36-hour window. The court explicitly held that allowing AI to clone an individual's speech

³⁴ Karan Johar v. Ashok Kumar/John Doe & Ors. CS(COMM) 974/2025 & I.A. 22608/2025

³⁵ Ajay alias Vishal Veeru Devgan v. The Artists Planet & Ors. CS(COMM) 1269/2025 & I.A. 29557/2025

³⁶ The Indian Hotels Company Limited v. John Doe and Anr. CS(COMM) 1110/2025

pattern risks economic fraud and "nefarious misutilization". The ruling establishes that digital erasure rights protect the holistic autonomy of a person's voice, preventing bad actors from hijacking a public figure's credibility.³⁷

During the past several months, malicious YouTube channels used generative AI text-to-speech tools and deepfakes to create altered, highly misleading videos featuring spiritual leader Sadhguru Jaggi Vasudev. The videos were engineered to trick viewers into clicking fraudulent, high-traffic commercial links. The Delhi High Court directed Google LLC to "make an endeavour to ensure that misleading and deepfake content" violating the plaintiff's personality rights is structurally systematically removed through the deployment of its own tech. The court mandated mutual engineering reviews to isolate and purge the content. This is a major structural shift in the erasure debate. The court acknowledged that manual, link-by-link URL reporting is ineffective against viral AI content. By telling Google to use its own technology to clean its video ecosystem, the court shifted the practical burden of digital erasure from the victim back onto the platform's automated systems.³⁸

An individual Nitin Bhatnagar, a senior professional banker was arrested by the Directorate of Enforcement (ED) in August 2023. The arrest was linked to alleged financial irregularities involving M/s Moser Baer India Limited. Various digital media platforms (including The Indian Express / IE Online Media Services) published news articles reporting the arrest. However, a year later (on August 17, 2024), the jurisdictional court fully discharged Bhatnagar, finding no legally admissible evidence against him. The underlying criminal complaint was entirely dismissed on July 24, 2025. Despite the discharge, major media archives and digital platforms continued to host the original, sensationalized news stories detailing his arrest. The media house argued that freedom of the press under Article 19(1)(a) allowed them to keep historical records online, proposing that adding a small "clarification update" footnote at the bottom of the old article was legally sufficient. The Delhi High Court rejected the media's argument, granting interim de-indexing directions. The court coined the term "Algorithmic Stigma," explaining that because the original accusatory headlines and URLs remain unchanged, standard search engine algorithms continuously prioritize the old allegations rather than the discharge. A footer clarification does not remove the dominant narrative or the ongoing psychological/extra-judicial harm. The court ruled that continuing to widely circulate old arrest

³⁷ Ravi Shankar v. John Doe(s) / Ashok Kumar(s) & Ors. CS(COMM) 889/2025

³⁸ Sadhguru Jagdish Vasudev v. Google LLC & Ors. CDJ 2025 DHC 5216

reports after a formal discharge directly violates an individual's fundamental right to dignity.³⁹

In Arijit Singh 2024 case an AI software developer trained a commercial text-to-speech generative AI model utilizing the unauthorized vocal tracks of playback singer Arijit Singh. The platform allowed users to generate new songs mimicking Singh's distinct voice, which were subsequently distributed across streaming apps. The Bombay High Court granted an interim injunction restraining the defendants from exploiting the singer's voice and identity through emerging generative AI technologies. The court mandated the removal of the platform's ability to synthesize his vocal likeness. This case captures the "machine unlearning" roadblock. While removing an uploaded audio track from a website is straightforward, erasing a person's voice from the underlying parameters of a trained neural network is exceptionally complex, shifting the legal focus from content removal to platform operational bans.⁴⁰

Nirmaan Malhotra case pertains to matrimonial and maintenance proceedings, during the course of which the husband submitted photographic and video evidence to allege adultery by his wife. The wife vehemently contested the evidence, asserting that the media had been synthetically manipulated and fabricated using widely accessible generative AI deepfake tools. A Division Bench of the Delhi High Court refused to rely on the photographs produced by the husband. The Court observed that society is now living in the "era of deepfakes" where visual media can no longer be blindly presumed authentic, ruling that it must be rigorously proven via expert forensic evidence. This case marks a paradigm shift in judicial observation on digital media. It highlights a unique obstacle to digital erasure: before a victim can even seek the legal erasure of damaging content in public records or court files, they face the exhausting evidentiary burden of proving the content is a deepfake.⁴¹

An unregulated commercial technology entities used voice-cloning AI and generative image models to exploit the distinctive voice, face, and popular nicknames (such as "Bhidu") of veteran actor Jackie Shroff in digital advertisements without his permission. The Court ruled in favour of Shroff, granting an omnibus injunction protecting his entire persona from unauthorized digital merchandising, AI exploitation, and deepfake creation. Generative AI does not just copy exact photos; it extracts style, cadence, and cultural likeness. This judgment clarifies that digital erasure rights must cover the holistic identity of the individual, giving

³⁹ IE Online Media Services Private Limited v. Nitin Bhatnagar 2025:DHC:9820

⁴⁰ *Arijit Singh v. Codible Ventures LLP & Ors.*, 2024 SCC OnLine Bom 2445.

⁴¹ *Nirmaan Malhotra v. Tushita Kaul* MAT.APP.(F.C.) 180/2024 &CM Nos.32316-18/2024

victims the right to erase synthetic content that mimics their recognizable traits, even if an exact original photo was not used.⁴²

The unrecognized digital platform facilitated generative AI creators to utilize facial features, body language, photographic likeness, and iconic catchphrases of actor Anil Kapoor to generate unauthorized deepfake advertisements, GIFs, and synthetic explicit media for commercial gain. The Delhi High Court granted an extensive interim injunction restraining the defendants and the public at large from using Kapoor's name, likeness, voice, or persona via generative AI tools. The court directed tech intermediaries to immediately remove all offending synthetic URLs. This foundational judgment established that while free speech allows for genuine parody, the unauthorized mechanical reproduction of an individual's entire identity using generative AI crosses into a violation of human dignity. Erasure must be enforced because the scalability of AI allows the synthetic content to permanently hijack a person's life's work.⁴³

In November 2023, a highly convincing video went viral on social media platforms showing Indian actress Rashmika Mandanna entering an elevator clad in a black workout outfit. The investigation revealed that the footage was actually an AI-generated deepfake. The original video featured a British-Indian influencer named Zara Patel. The creator used artificial intelligence technology to seamlessly superimpose Mandanna's face onto Patel's body. Following a complaint by the Delhi Commission for Women (DCW), the Delhi Police's Intelligence Fusion and Strategic Operations (IFSO) unit initiated a technical probe. In January 2024, they arrested the main culprit, a 24-year-old digital creator from Andhra Pradesh, who confessed he created the deepfake to rapidly grow followers on a fan page he managed. Driven by public outrage, the Ministry of Electronics and Information Technology (MeitY) issued strict legal advisories to all tech platforms. They mandated that social media intermediaries must remove deepfakes and artificially morphed content within 24 to 36 hours of a complaint, or risk losing their "safe harbour" legal immunity under the IT Act 2000. This incident exposed the critical gap in India's legal architecture regarding AI regulation.⁴⁴

In *Vysakh* 2022 case the core takeaway is that court judgments are public records, and the

⁴² Jackie Shroff v. Simply Life India & Ors. 2024:DHC:4046

⁴³ Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.

⁴⁴ State v. Unidentified / Eemani Naveen, registered by the Intelligence Fusion and Strategic Operations (IFSO) Unit, Delhi Police (November 2023). (State prosecution remained at the FIR stage rather than a reported high court or supreme court judgment)

principle of an "Open Court" means that private law repositories have the right to publish them. However, the Right to be Forgotten is recognized under the ambit of Article 21 (Right to Privacy). Until the legislature formulates clear statutory boundaries, courts will dynamically assess and grant name masking requests on a case-to-case basis specifically prioritizing cases involving family disputes and victims of sexual violence to protect personal dignity from perpetual digital exposure.⁴⁵

Jorawer Singh Mundy an American citizen of Indian origin was acquitted of charges under the NDPS Act by an Indian court. However, despite being cleared of all charges, the historical judgment remained permanently cached on public legal databases (like vLex.com) and prominently indexed on Google Search results, severely damaging his employment prospects and digital reputation. The Delhi High Court recognized the emerging "Right to be Forgotten" as an intrinsic component of the Right to Privacy under Article 21. The Court ordered Google and the legal portals to remove the specific judgment from search indexes and public view. This is the bedrock case for digital erasure in India. It proved that information permanence on the internet can act as a lifelong sentence. For modern AI victims, *Jorawer Singh* is highly persuasive because it established the baseline legal rule that just because a piece of data exists on the public web does not mean tech platforms have a permanent right to index, display, or utilize it.⁴⁶

The petitioner challenged a criminal investigation that had been transferred to the Central Bureau of Investigation (CBI) without giving him a prior hearing. The prosecution was dependent on AI-driven forensics, automated surveillance, algorithm-based evidence gathering and digital data extraction. The Supreme Court held that an accused has absolutely no inherent right to be heard at the stage of investigation. Law enforcement can freely use AI-powered data mining, facial recognition, or automated forensic software to build a case. The accused cannot claim a violation of natural justice or demand an early audit of the AI tool; they must wait until the trial to challenge the machine's accuracy.⁴⁷

In April 2018, investigative journalist Rana Ayyub was targeted with deepfake pornographic videos structurally engineered via early AI-stitching to morph her likeness. The case illustrates the sluggishness of international platform compliance and the cross-border jurisdictional

⁴⁵ *Vysakh K.G. v. Union of India* 2022 SCC OnLine Ker 7337

⁴⁶ *Jorawer Singh Mundy v. Union of India*, 2021 SCC OnLine Del 2306.

⁴⁷ *E. Shivakumar v. Union of India and Others*, (2018) 7 SCC 365.

gridlock. Because the servers hosting the deepfakes were outside domestic borders, local law enforcement faced severe delays, leaving the content online for an extended period. This timeline subjects the victim to ongoing, severe psychological trauma and secondary victimization by the digital ecosystem. The Delhi Police eventually filed a closure report in August 2020, stating that they could not identify the anonymous culprits behind the creation and initial distribution of the deepfake video. The case ended in a police closure rather than a definitive case reported at High Court or Supreme Court judgment on its merits, it does not have a standard landmark supreme court/high court case citation. However, it remains globally recognized as one of the earliest and most prominent real-world instances of deepfake pornography being used as a targeted tool of political harassment against a journalist.⁴⁸

The Government of India introduced the Aadhaar project, a massive biometric identification system requiring citizens to surrender their fingerprints, iris scans, and demographic data to access basic public and private utilities. The retired judge, Justice K.S. Puttaswamy, challenged the constitutional validity of the project before a rare nine-judge bench of the Supreme Court. He argued that collecting and permanently storing a citizen's sensitive digital data without strict safeguards violated their fundamental rights. A unanimous nine-judge bench delivered a historic verdict, declaring that the Right to Privacy is an fundamental right under Article 21 (Right to Life and Personal Liberty). Crucially, the bench recognized informational privacy and explicitly stated that the right to privacy encompasses the "Right to be Forgotten" observing that individuals should have the right to evolve and not be permanently held hostage by their digital past. This case completely re-architected Indian digital law. It established that a citizen's data belongs to the citizen, not the state or tech corporations. By recognizing that the "Right to be Forgotten" is part of human dignity under Article 21, the Supreme Court created the absolute legal justification that modern victims use to demand the erasure of deepfakes, AI voice clones, and non-consensual media.⁴⁹

A man was acquitted of criminal charges (which include kidnapping and murder) by the Gujarat High Court. Despite his acquittal, the old judgment showed up on Google whenever someone searched his name, damaging his personal and professional life. The petitioner argued for a "right to be forgotten," but the Gujarat High Court rejected the plea. At that time, India had no formal privacy framework, and the court ruled that judgments are public documents

⁴⁸ Halder, D., and Basu, S. 2025. Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India. *Information & Communications Technology Law*, 34(2), 163-186. <https://doi.org/10.1080/13600834.2024.2408914>

⁴⁹ Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

that cannot be hidden. This was the first major case to explicitly test the concept.⁵⁰

7. Definitive Legislative Blueprint: The Justice B.N. Srikrishna Committee Report (2018)⁵¹

Following the Puttaswamy judgment⁵², the government tasked the committee with drafting a data protection framework. The Committee of Experts was appointed by the Ministry of Electronics and Information Technology (MeitY) which formed the basis for foundational report that formally structured the Right to be Forgotten (RTBF) into draft Indian statutory law. The report dedicated an entire chapter to structural data erasure which legally enforce a citizen's right to restrict or prevent the continuing disclosure of their personal data by internet intermediaries. The report recommended a Five Factor Balancing Test to decide if data should be forgotten. It stated that a "Data Protection Authority" (and not search engines) must decide on removal requests by evaluating: (a) The sensitivity of the personal data. (b) The scale of disclosure and degree of accessibility sought to be restricted. (c) The role of the individual in public life (public figures have less right to be forgotten). (d) Relevance of the personal data to the public (historical, scientific, or archival value). (e) The freedom of speech and expression of other citizens. This exact framework was integrated into India's legislative pipeline, ultimately evolving into the Right to Erasure under Section 12 of the Digital Personal Data Protection (DPDP) Act, 2023.

8. Online de-indexing framework

The Delhi High Court⁵³ established a clear evaluation framework when processing applications for de-indexing (preventing an individual's name from pulling up court records or news via search engines) and masking (anonymising court orders), they apply the following key balancing factors viz:

The Balancing Test Factors for Online De-Indexing

1. Outcome of the Concluded Proceedings: Acquittal, discharge, closure, settlement, or

⁵⁰ Dharamraj Bhanushankar Dave v. State of Gujarat (2015) SCC OnLine Guj 2019

⁵¹ Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Ministry of Electronics and Information Technology, Govt. of India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)

⁵² *Supra*⁴⁹

⁵³ *Supra*³²

quashing. Exception - serious criminal convictions.

- 2. Nature of the Information (Private vs. Public Matters):** Intensely private or family affairs (such as matrimonial disputes, child custody, and sexual offence cases)
- 3. Time Elapsed and Continuing Relevance:** Obsolete or spent over time. Case concluded years ago and no longer serves an active socio-legal purpose, its "continuing relevance" drops, tipping the scale toward de-indexing.
- 4. Proportionality of Harm vs. Open Justice:** Disproportionate harm to the applicant's dignity, reputation, social life, and career prospects. The court histories remain open via citations or case numbers, a name shouldn't serve as a permanent digital stigma.
- 5. Public Role or Status of the Individual:** Public officials and prominent public figures acts performed in their official capacities, and their privacy requests are generally declined.
- 6. Public Interest vs. Personal Privacy:** A strict distinction is drawn between "*of interest to the public*" (idle curiosity) versus being "*in the public interest*" (public welfare, safety, or accountability). De-indexing will be refused if masking the record threatens public safety or shields a matter of genuine public importance.
- 7. Accuracy, Completeness, and Context of the Digital Record:** High Courts look at the systemic impact of name-based searchability. It evaluates whether an un-updated online footprint (e.g., an old news report of an arrest without mentioning the subsequent acquittal) creates an inaccurate, highly prejudicial picture of the individual's current legal status

9. Indian statutory framework

Statutory Frameworks & Regulatory Bodies

- Section 12 DPDP Act 2023 (Data Erasure)
- Section 79 IT Act 2000 (Safe Harbor Provisions)
- IT Rules 2021 (Intermediary Guidelines)

- Data Protection Board of India (DPBI)
- Grievance Appellate Committee (GAC)
- Article 17 GDPR (Right to Erasure) – European Union

9.1 DPDP Act 2023

Section 12 of the Digital Personal Data Protection (DPDP) Act, 2023⁵⁴ establishes the Right to Correction and Erasure of Personal Data.

9.1.1 Statutory Breakdown of Section 12 Regarding Erasure

The mechanism for erasure is specifically governed by **Section 12(1)** and **Section 12(3)** of the Act. Let us look at the exact legal language and its structural implications:

A. The Entry Gate: Section 12(1)

“A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent...”

The Consent Anchor: The rights under Section 12 are explicitly anchored to data processed via prior consent (including deemed consent scenarios under Section 7). If data is being processed under other "legitimate uses" specified by the Act (such as State subsidies, medical emergencies, or employment functions), the Data Principal cannot unconditionally leverage Section 12 to demand erasure.

B. The Operative Mandate: Section 12(3)

“A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.”

- *In such manner as may be prescribed:* Erasure is not a loose or informal request. It must

⁵⁴ The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

follow a formalized, systematic process that complies with upcoming DPDP Rules.

- *The Mandate to Erase:* The phrase “*shall erase*” makes the action strictly mandatory for the Data Fiduciary once a valid request is recognized, stripping the business of arbitrary discretion.

9.1.2 The Statutory Exceptions: The "Unless" Caveats

The Section 12(3) provides two massive statutory carve-outs that stop erasure claims in their tracks:

Exception 1: Necessary for the "Specified Purpose"

If the data is still actively required to fulfill the explicit objective outlined in the initial notice given to the user, the Data Fiduciary can legally refuse erasure.

Exception 2: Compliance with "Any Law for the Time Being in Force"

In case if any sectoral law mandates data retention by viz: RBI's KYC norms for financial entities, the Income Tax Act for financial logs, or TRAI regulations for telecom logs, the statutory obligation to retain data completely supersedes the individual's right to request erasure.

9.1.3 Interplay of Proactive vs. Reactive Erasure

Section 12 must be read alongside with Section 8(9) of the DPDP Act 2023.

- **Section 12(3) is *Reactive*:** It requires the individual (Data Principal) to actively step forward and issue a deletion request.
- **Section 8(9) is *Proactive*:** It legally commands Data Fiduciaries to automatically delete personal data as soon as the specified purpose is fulfilled or when consent is withdrawn, irrespective of whether the user asks for it.

Section 12 operates as a secondary right enforcement tool when businesses fail their proactive cleanup duties under Section 8. The features of DPDP Act and EU's GDPR⁵⁵ in digital erasure

⁵⁵ Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119

are describes in Table 3.

Table 3. Features of DPDP Act and EU's GDPR in digital erasure

Architectural Feature	India's DPDP Act (Section 12)	EU's GDPR (Article 17)
Nature of Right	Conditional Right. Tied tightly to the lifecycle of consent or purpose fulfillment.	Broad Right. Includes standalone grounds like simple objection to processing or public interest.
Ripple-Effect Mandate	Implicitly binds the Fiduciary to clear data downstream from its designated Data Processors.	Explicitly requires the Controller to take "reasonable steps" to inform public downstream links.
State Exemptions	Highly permissive. Notified State instrumentalities are broadly exempt from Section 12(3) data erasure mandates.	Strictly limited. Public bodies must justify retention under narrow public-interest criteria.

9.2 Data Protection Board of India (DPBI)

The Data Protection Board of India (DPBI) is the core enforcement and adjudicatory authority established under Section 18 of the Digital Personal Data Protection (DPDP) Act, 2023. Formally set up by the Ministry of Electronics and Information Technology (MeitY) via the DPDP Rules, the DPBI represents a massive shift towards a centralized, independent data privacy regulator in India. The DPBI's orders are not final. Aggrieved parties can file an appeal before the Telecom Disputes Settlement and Appellate Tribunal (TDSAT), with the final avenue of recourse being the Supreme Court of India. Civil courts are entirely barred from entertaining data disputes covered by the DPBI.

For traditional databases, servers, and companies holding your customer data (Data Fiduciaries), the rules operate on a lifecycle baseline rather than hourly emergency triggers:

- Upon Reasoned Request (Reactive Deletion): Once a Data Principal submits a valid erasure request under Section 12, the Data Fiduciary must delete the data without undue delay, unless it is legally required by an overlapping law (like RBI or Income Tax guidelines).
- 3-Year Automatic Inactivity Trigger (Proactive Deletion): For large digital platforms

(e.g., social media, e-commerce, and online gaming giants with millions of users), data must be automatically deleted after 3 years of total user inactivity. The platform is legally required to send a mandatory pre-erasure notification 48 hours before executing the deletion.

- The 1-Year Retention Minimum Override: Crucially, under the DPDP Rules, Data Fiduciaries must retain access logs, traffic data, and core processing records for a minimum period of 1 year from the processing date. Even if a user requests immediate erasure under Section 12, the backend technical logs must be preserved for this 1-year security window before being completely purged.⁵⁶

9.3 Section 79 IT Act 2000 (Safe Harbor Provisions)

Section 79 of the Information Technology (IT) Act, 2000 serves as the "Safe Harbour" doctrine in Indian cyber law. It legally insulates intermediaries (such as internet service providers, search engines, e-commerce marketplaces, and social media platforms) from civil and criminal liability for third-party user-generated content. However, this immunity is strictly conditional. If an intermediary fails to meet the legal criteria or ignore regulatory directives, this shield drops completely, exposing the corporation to direct liability for user-generated offenses. To maintain their Safe Harbour protection, social media companies, search engines, and websites must completely remove or disable access to flagged content within the following strict emergency windows viz:⁵⁷

- 2 Hours (Non-Consensual Intimate Imagery / Deepfakes)
- 3 Hours (Lawful & Government Orders), *this was slashed from the legacy 36-hour window.*
- 24 Hours (Standard Grievance Acknowledgment)

9.4 IT Rules 2021 (Intermediary Guidelines)

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (commonly known as the IT Rules, 2021) serve as the core secondary legislation that

⁵⁶ The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).

⁵⁷ Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).

operationalizes the Safe Harbour doctrine under Section 79 of the IT Act, 2000. The rules have undergone comprehensive overhauls via the IT Amendment Rules, 2026. These updates address systemic digital harms, specifically regulating Synthetically Generated Information (SGI) including deepfakes, AI-generated text, and fabricated media by imposing strict compliance mandates and drastically compressed content takedown timelines (Table 4).⁵⁸

Table 4. Content Takedown Matrix

Content Category	Legal Trigger	Takedown Window	Previous Window
Non-Consensual Intimate Imagery / Deepfakes	Grievance complaint by victim or authorized representative.	2 Hours	24 Hours
Unlawful AI / Court & Government Orders	Formal direction from an authorized court or government agency.	3 Hours	36 Hours
Standard User Grievances	General copyright, trademark, or general data dispute.	24 Hours (<i>Acknowledge</i>)	48 Hours

9.5 Grievance Appellate Committee (GAC)

The Grievance Appellate Committee (GAC) is a statutory appellate body established under Rule 3A of the IT Rules, 2021. Introduced by the Central Government to bridge a massive gap in platform accountability, it functions as a highly specialized, digital-native tribunal. The GAC provides Indian internet users (Digital Nagriks) with an institutional channel to challenge arbitrary decisions made by the internal Grievance Officers of Big Tech platforms, social media intermediaries, and OTT services.⁵⁹

9.6 Article 17 GDPR (Right to Erasure) – EU

Article 17 of the European Union's General Data Protection Regulation (EU GDPR) establishes

⁵⁸ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

⁵⁹ <https://gac.gov.in/>

the Right to Erasure, commonly known as the "Right to be Forgotten". It empowers individuals (*data subjects*) to demand that an organisation (*data controller*) delete their personal data without undue delay. However, this is a conditional right rather than an absolute rule. A deletion request must satisfy specific grounds, and it remains subject to heavy public interest overrides.

10. Conclusion

The proliferation of non-consensual AI-generated exploitative content represents a critical failure of current legal systems to protect individual dignity in the digital age. The present legal analysis demonstrates that the current barriers to digital erasure are not merely operational bottlenecks, but are fundamentally structural. The true digital erasure cannot be achieved through piecemeal litigation or voluntary platform moderation. Eradicating this systemic crisis demands a comprehensive, forward-looking legislative response. Legal frameworks must evolve from a reactive stance to a proactive mandate by standardizing the federal criminalization of non-consensual deepfakes, conditioning intermediary immunities on the mandatory deployment of robust AI-detection technologies, and pursuing international treaty harmonization. Only by aligning global regulatory mechanisms with the realities of generative technology can the legal system dismantle the barriers to content removal, enforce platform accountability, and meaningfully secure a victim's right to digital erasure.

References

1. Citron, D.K. (2022). *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*. W. W. Norton & Company.
2. Qiwei, L., Kennon, K., Bedera, N., Eaton, A.A., Gilbert, E., and Schoenebeck, S. 2026. Platforms as Crime Scene, Judge, and Jury: How Victim-Survivors of Non-Consensual Intimate Imagery Report Abuse Online. In Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain. ACM, New York, NY, USA, 19 pages. <https://doi.org/10.1145/3772318.3791115>
3. Umbach, R., Henry, N., Shelby, R., Stevens, G., and Gonzalez-Pons, K. 2026. AI-generated image-based sexual abuse: Perpetration and consumption across three regions. *Computers in Human Behavior*, 179, 108935. <https://doi.org/10.1016/j.chb.2026.108935>
4. Nfissi, N. 2025. Protecting human rights in the digital age: Legal frameworks and media literacy as a complementary safeguard, *Digital Law Journal*, 6(3), 1-26. <https://doi.org/10.38044/2686-9136-2025-6-10>
5. Nicola, H., Rebecca, U., Renee S., Gemma B., and Lisa, M. 2026. 'It's still abuse': community attitudes and perceptions on AI-generated image-based sexual abuse, *Information, Communication & Society*, DOI: 10.1080/1369118X.2026.2613437
6. Regenscheid, A., Feldman, L., and Witte, G. 2015. NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=917935 (Accessed September 5, 2026)
7. Park, R. 2022. Forgiving Without Forgetting? Privacy in an Age of Digital Permanence, *Political Science Honors Projects*. 96. https://digitalcommons.macalester.edu/poli_honors/96
8. Dhingra, K., and Tyagi, K. 2025. Historical development of the right to be forgotten, *International Journal of Advanced Legal Research*, 5(4) 1-10
9. Allegri, M.R. 2022. The Right to be Forgotten in the Digital Age. In: Comunello, F., Martire, F., Sabetta, L. (eds) *What People Leave Behind*. Frontiers in Sociology and Social Research, vol 7. Springer, Cham. https://doi.org/10.1007/978-3-031-11756-5_15
10. Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317

11. European Parliament and of the Council (General Data Protection Regulation - EU) 2016/679
12. <https://www.clicdata.com/blog/data-destruction-vs-data-erasure-processes/>
13. U.S. Department of Defense. (1995). *National Industrial Security Program Operating Manual* (DoD 5220.22-M). U.S. Government Printing Office.
14. Gutmann, P. 1996. Secure deletion of data from magnetic and solid-state memory. In *Proceedings of the 6th USENIX Security Symposium* (p. 8). USENIX Association.
15. Blancco. (n.d.). *What's behind the global shift to data erasure?* GovInsider. <https://govinsider.asia/intl-en/article/whats-behind-the-global-shift-to-data-erasure>
16. Kissel, R., Regenscheid, A., Scholl, M., and Stine, K. 2014. *Guidelines for media sanitization* (NIST Special Publication 800-88 Rev.1). National Institute of Standards and Technology. doi.org
17. Sokler, B.D., Hecht, A., Fjeld, C.T., and Raj G. Algorithmic Disgorgement: An Increasingly Important Part of the FTC's Remedial Arsenal — *AI: The Washington Report*, MINTZ, January 24, 2024
18. Ranganathan Madhavan v. G Filmz Studioz & Ors. CS(COMM) 1392/2025.
19. Telegram FZ LLC & Anr. v. Union of India & Ors. 2026 SCC OnLine Del 4750
20. Khushi Kapoor v. Ashok Kumar/John Doe & Ors. CS(COMM) 869/2026
21. Jubin Nautiyal v. Jammable Ltd. & Ors., CS(COMM) 166/2026
22. Pooja Ramesh Singh v. Jammu and Kashmir Bank Ltd., 2026 INSC 668
23. Sonakshi Sinha v. Character Technologies Inc. and Others, CS(COMM) No. 275/2026
24. Dr. Aniruddha Dhairyadhar Joshi v. John Doe / Ashok Kumar, CS(COMM) 178/2026
25. Yuvraj Singh v. Ashok Kumar/John Doe & Ors., CS(COMM) No. 642/2026
26. Dr. Shashi Tharoor v. Unknown Defendants & Ors., CS(OS) No. 312/2026
27. Ravi Kishan v. Ashok Kumar/John Doe & Ors., CS(COMM) No. 490/2026
28. Aman Gupta v. Artist Booking Company & Ors., CS(COMM) No. 355/2026
29. Raghav Chadha v. Ashok Kumar John Doe & Ors., CS(OS) 466/2026

30. Naga Chaitanya Akkineni v. Unknown Defendants & Ors., CS(COMM) No. 462/2026
31. Nitin Gadkari v. X Corp. & Ors. Interim Application (L) No. 25165 of 2026 in Suit (L) No. 25151 of 2026
32. Laksh Vir Singh Yadav v. Union of India, W.P.(C) 1021/2016 & Connected Matters (Delhi High Court, 29 May 2026); Neutral Citation: 2026:DHC:4891
33. Neela Film Productions Private Limited v. Taarakmehtakaooltahchashmah.com & Ors. CS(COMM) 690/2024
34. Karan Johar v. Ashok Kumar/John Doe & Ors. CS(COMM) 974/2025 & I.A. 22608/2025
35. Ajay alias Vishal Veeru Devgan v. The Artists Planet & Ors. CS(COMM) 1269/2025 & I.A. 29557/2025
36. The Indian Hotels Company Limited v. John Doe and Anr. CS(COMM) 1110/2025
37. Ravi Shankar v. John Doe(s) / Ashok Kumar(s) & Ors. CS(COMM) 889/2025
38. Sadhguru Jagadish Vasudev v. Google LLC & Ors. CDJ 2025 DHC 5216
39. IE Online Media Services Private Limited v. Nitin Bhatnagar 2025:DHC:9820
40. Arijit Singh v. Codible Ventures LLP & Ors., 2024 SCC OnLine Bom 2445.
41. Nirmaan Malhotra v. Tushita Kaul MAT.APP.(F.C.) 180/2024 & CM Nos.32316-18/2024
42. Jackie Shroff v. Simply Life India & Ors. 2024:DHC:4046
43. Anil Kapoor v. Simply Life India & Ors., 2023 SCC OnLine Del 6914.
44. State v. Unidentified / Eemani Naveen, registered by the Intelligence Fusion and Strategic Operations (IFSO) Unit, Delhi Police (November 2023). (State prosecution remained at the FIR stage rather than a reported high court or supreme court judgment)
45. Vysakh K.G. v. Union of India 2022 SCC OnLine Ker 7337
46. Jorawer Singh Mundy v. Union of India, 2021 SCC OnLine Del 2306.
47. E. Shivakumar v. Union of India and Others, (2018) 7 SCC 365.

48. Halder, D., & Basu, S. 2025. Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India. *Information & Communications Technology Law*, 34(2), 163–186. <https://doi.org/10.1080/13600834.2024.2408914>
49. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
50. Dharamraj Bhanushankar Dave v. State of Gujarat (2015) SCC OnLine Guj 2019
51. Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, Ministry of Electronics and Information Technology, Govt. of India, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (2018)
52. Supra⁴⁹
53. Supra³²
54. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
55. Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119
56. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023).
57. Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
58. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
59. <https://gac.gov.in/>