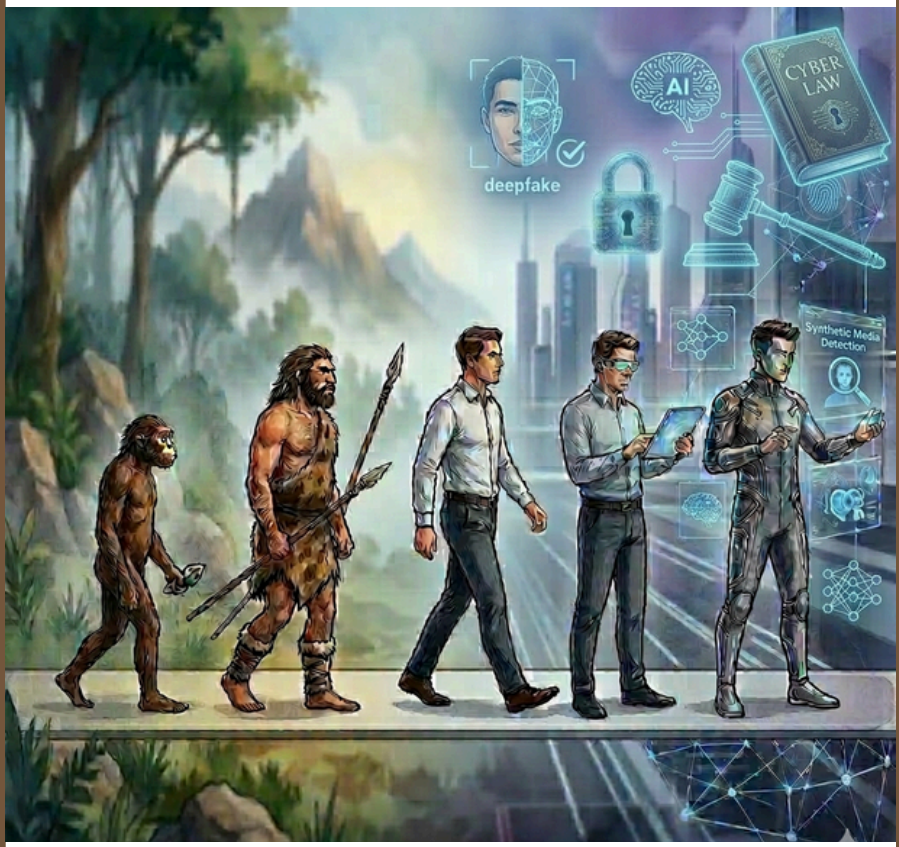
YNZ GROUP

Pixels to Protection: India's Legal Resurrection



Wednesday Wisdom
11-03-2026

Interesting conversation with Grandfather and granddaughter, that during our college days there were no mobile phones, so granddaughter said o my god then how you could enjoy with friends, Grandfather answered we chatted, laughed, clapped, fought with our friends in real world. [1]

Today, digital presence in every sphere of life has become the new normal. Today, it is almost impossible to imagine life without a mobile phone, internet connection, or laptop. Digitisation has transformed the way we live, work, do business and communicate. While it has brought immense convenience and opportunity, it has also introduced complex challenges that society was not fully prepared to confront.

The advent of camera-enabled mobile phones and widespread internet access marked a turning point. What began as a technological convenience soon revealed darker consequences. One of the early and alarming instances involved a student in Delhi who recorded a private moment with his girlfriend and circulated it among friends. Incidents like this began surfacing more frequently, highlighting how technology could be misused to invade privacy and cause irreparable harm[2].

As internet usage expanded, so did the exposure of personal information. Today, almost every website we visit collects data about our behavioural patterns, preferences, and personal details—sometimes shared knowingly, and often unknowingly. Personal data has effectively become a digital asset, tracked, processed, and monetised in ways most users scarcely understand.

[1]The article reflects the general work of the authors and the views expressed are personal. No reader should act on any statement contained herein without seeking detailed professional advice.
[2] DPS MMS Case https://www.telegraphindia.com/india/scandal-in-school-shakes-up-delhi/cid/1667531#goog_rewarded

The rise of digital payments brought another wave of transformation. While offering speed and convenience, it also opened doors to new forms of fraud, such as scams involving fake QR codes and deceptive payment links.

Now, we stand in the era of artificial intelligence. Advanced AI tools are being misused to create manipulated images and videos, commonly known as deepfakes leading to blackmail, defamation, and reputational damage. The ability to fabricate highly realistic digital content has blurred the line between truth and falsehood, raising serious concerns about identity, consent, and accountability.

Recognising the growing impact of internet-related offences, India introduced its first comprehensive legislation to regulate cyberspace—the Information Technology Act, 2000. This marked the beginning of India's legal journey toward addressing the evolving challenges of the digital world.

Phases of Legal Evolution Under the Information Technology Framework in India

Phase I: Foundation of Cyber Law – The Information Technology Act, 2000

India enacted the Information Technology Act, 2000 to provide legal recognition to electronic records and digital signatures, facilitate e-commerce, and address basic cyber offences. At the time, the internet ecosystem was still developing, and the primary focus was on enabling electronic governance and regulating hacking, tampering with computer systems, and online fraud.

However, the law was enacted in an era before social media, digital payments, smartphones, and artificial intelligence became integral to daily life. As a result, it soon faced limitations.

Phase II: Strengthening Cybercrime and Data Protection – The 2008 Amendment

With the rapid expansion of internet usage and the rise of cybercrimes, Parliament introduced significant changes through the Information Technology (Amendment) Act, 2008[3].

Key developments included:

Introduction of Section 43A, imposing liability on companies for failure to protect sensitive personal data.	Recognition of electronic signatures. Expanded definitions of cyber offences, including identity theft and cheating by personation.	Introduction of Section 66A, which criminalised sending offensive messages through communication services. In a landmark decision, the Supreme Court in Shreya Singhal v. Union of India[4] struck down Section 66A of the IT Act, holding it unconstitutional for violating freedom of speech under Article 19(1)(a) of the Constitution.

[3]https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMTk4NzY=
[4] AIR 2015 SUPREME COURT 1523 https://indiankanoon.org/doc/110813550/

This amendment reflected a shift from merely enabling e-commerce to actively addressing cybercrime and data protection concerns.

Phase III: Intermediary Liability and Content Regulation – 2011 Rules

As social media platforms and online intermediaries grew in influence, the government notified the Information Technology (Intermediaries Guidelines) Rules, 2011[5].

These rules required intermediaries to:

- Exercise due diligence.
- Remove unlawful content upon receiving notice.
- Publish privacy policies, user agreements and grievance officer name and address on website.

This phase marked the beginning of formal regulation of online platforms and user-generated content in India.

Phase IV: Social Media Accountability and Digital Governance – 2021 Rules

In response to misinformation, online abuse, and platform accountability concerns, the government notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[6].

These rules introduced:

- Grievance redressal mechanisms.
- Appointment of compliance officers by significant social media intermediaries.
- Traceability requirements for messaging platforms (in certain cases).
- Regulation of digital news media and OTT platforms.

This marked a stronger regulatory assertion over digital platforms operating in India.

[5]https://upload.indiacode.nic.in/showfile?actid=AC_CEN_45_76_00001_200021_1517807324077&type=rule&filename=Information%20Technology%20(Intermediaries%20Guidelines)%20Rules,%202011.pdf

[6] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

Phase V: Comprehensive Data Protection Framework – Digital Personal Data Protection Act, 2023

Recognising the need for a dedicated data protection regime, Parliament enacted the Digital Personal Data Protection Act, 2023[7]. This legislation reflects India's attempt to align with global data protection standards while addressing domestic digital governance needs. To know more about provision of DPDPA, read our article here.

Phase VI: Emerging AI and Deepfake Challenges

With the exponential rise of AI-generated content, deepfakes, and other forms of synthetic media, regulatory attention has increasingly shifted from traditional cyber offences toward technologically sophisticated forms of digital harm. The misuse of artificial intelligence to fabricate highly realistic images, audio, and video has intensified concerns relating to privacy, consent, reputational injury, electoral manipulation, and public order. Unlike conventional misinformation, deepfakes possess a heightened capacity for deception because they replicate human likeness and speech with remarkable accuracy, making detection difficult and enabling harm to occur almost instantaneously.

A media-reported incident in 2025-2026 highlighted the growing misuse of artificial intelligence tools to create manipulated or deepfake images of public figures on social media platforms such as X. The controversy arose when several photos of three prominent Bollywood actresses Deepika Padukone, Shraddha Kapoor, and Alia Bhatt went viral online, allegedly showing them attending a private party.

The situation escalated when a user responded to the same post and prompted the platform's AI chatbot with the instruction, "Dress them in bikinis." Within seconds, the AI reportedly generated altered images depicting the actresses in bikinis.

[7] https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

The rapid creation and circulation of such manipulated images raised serious concerns regarding the misuse of generative AI technologies to produce sexualised content involving real individuals without their consent. The incident sparked widespread criticism from social media users, digital rights advocates, and policymakers, who raised concerns about privacy violations, online harassment, and the broader ethical implications of AI tools capable of generating deepfake or manipulated media.[8]

Ministry of Electronics and Information Technology issued notice to X seeking removal of obscene content[9]. In response, X reported that it had blocked more than 3,500 content items and removed over 600 accounts, assuring authorities that its operations were in compliance with India's online content laws[10].

Another significant reported case involving deepfake and misleading AI-generated content concerned spiritual leader Sadhguru Jaggi Vasudev, founder of the Isha Foundation. The Delhi High Court, while hearing a personality rights case filed by Sadhguru, directed Google to utilise its technological capabilities to identify and remove misleading and AI-generated deepfake content that infringed upon his personality rights. The case involved manipulated videos and advertisements circulating online that falsely portrayed Sadhguru endorsing investment schemes and other commercial products.

[8]https://www.wionews.com/entertainment/bollywood/ai-double-standards-grok-flags-fake-images-of-alia-deepika-and-shraddha-then-creates-bikini-pics-1767866104979
[9] https://www.newsonair.gov.in/ministry-of-electronics-and-information-technology-issues-notice-to-x-seeking-removal-of-obscene-content/
[10] https://www.firstpost.com/tech/x-blocks-3500-posts-deletes-600-accounts-over-obscene-content-as-india-flags-grok-misuse-13967580.html

The matter attracted further attention after reports revealed that a 57-year-old woman from Bengaluru had allegedly lost approximately ₹3.75 crore to scammers who used an AI-generated deepfake of Sadhguru to promote fraudulent investment schemes. Despite an earlier court order directing the removal of such infringing content, the Isha Foundation stated that misleading videos continued to circulate online, including false claims regarding Sadhguru's arrest[11].

In response to these emerging threats, the Ministry of Electronics and Information Technology notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 vide Notification G.S.R. 120(E) dated February 10, 2026[12]. The amendment represents a significant shift in India's regulatory approach, moving toward a more technology-specific and enforcement-oriented framework

The 2026 Amendment introduces four key structural changes.

[11] https://www.indiatoday.in/india/story/delhi-high-court-directs-google-to-curb-fake-sadhguru-arrest-ads-using-technology-2806292-2025-10-21

[12] https://egazette.gov.in/WriteReadData/2026/269993.pdf

a. It provides a statutory definition of "deepfake.":

By formally defining deepfakes within the regulatory framework, the amendment removes ambiguity that previously complicated enforcement. Deepfake is defined as "Synthetically Generated Information (SGI)" which means audio, visual, or audio-visual content that is artificially or algorithmically created, generated, modified, or altered using a computer resource in a manner that makes the information appear real, authentic, or true, and that portrays an individual or event in a way that is, or is likely to be perceived as, indistinguishable from a natural person or real-world occurrence. The definition encompasses AI-generated or algorithmically manipulated content that falsely depicts an individual as saying or doing something they did not. This definitional clarity is crucial for triggering platform obligations and ensuring uniform compliance standards.

a. Obligations of Intermediary:

Intermediaries are now required to:

i.Periodically inform users, at least once every three months through their rules and regulations, privacy policies, user agreements, or other appropriate means, in English or any language listed in the Eighth Schedule to the Constitution, about the consequences of violating platform policies or applicable laws.

ii.Intermediaries must notify users that where such non-compliance involves the creation, publication, transmission, storage, or dissemination of information in contravention of applicable law, the responsible user may be liable to penalties or punishment under the Information Technology Act or other relevant legislation. Where the violation amounts to a criminal offence that require mandatory reporting under laws such as the Bharatiya Nagarik Suraksha Sanhita, 2023 or the Protection of Children from Sexual Offences Act, 2012,

the intermediary must also inform users that such offences may be reported to the appropriate authorities.

iii. Intermediaries which enables the creation or dissemination of synthetically generated information, including AI-generated or algorithmically manipulated content must inform its users that using its platform to generate or disseminate unlawful synthetic content may attract penalties under a range of laws, including the Information Technology Act, the Bharatiya Nyaya Sanhita, 2023, the Representation of the People Act, 1951, and other statutes relating to child protection, indecent representation of women, workplace harassment, and trafficking. Users must also be informed that violations may lead to the immediate removal of the offending content, suspension or termination of their accounts, identification and disclosure of the violator's identity to victims where permitted by law, and mandatory reporting to law enforcement authorities where applicable.

iv. Further, intermediaries are obligated to take expeditious action upon becoming aware, either suo motu or through a complaint, grievance, or other form of notice of any violation involving synthetically generated information. Such action may include disabling access to the content, removing the material, suspending user accounts, and cooperating with authorities in accordance with applicable legal procedures.

c. It reduces the takedown timeline:

- Earlier, intermediaries were required to remove unlawful content within thirty-six hours upon receiving actual knowledge. The amendment compresses this timeline to three hours in cases involving deepfakes and certain categories of synthetic harm.
- Similarly, platforms must remove non-consensual nudity within two hours, down from 24 hours.
- Grievance redressal timelines have also been halved to seven days.[13]

d. It mandates due diligence in relation to synthetically generated information:

Significant social media intermediaries that enable users to display, upload, or publish content on their platforms are required, prior to such display, upload, or publication, to obtain a declaration from users indicating whether the content constitutes synthetically generated information. In addition to collecting this declaration, intermediaries must deploy appropriate technological measures including automated tools or other suitable mechanisms to verify the accuracy of the user's declaration, taking into account the nature, format, and source of the information. Where either the user's declaration or the intermediary's technical verification confirms that the content is synthetically generated, the platform must ensure that the material is clearly and prominently labelled with an appropriate notice indicating that it is synthetically generated

[13] https://indianexpress.com/article/legal-news/indias-new-3-hour-deepfake-removal-rule-experts-urge-strict-compliance-10528122/

Conclusion

Artificial intelligence is now embedded in governance, finance, healthcare, and everyday digital life. India's response has not been to wait for a single AI law, but to build a layered, technology-neutral framework that applies existing statutes while introducing targeted safeguards for emerging harms like deepfakes.

Although the law may not be exhaustive to deal with AI related issues but existing law provides significant safeguards. The Digital Personal Data Protection Act, 2023 which embeds consent, purpose limitation, and fiduciary responsibility into AI systems that rely on personal data. Further there is Consumer and criminal remedies under the Consumer Protection Act, 2019 and the Bharatiya Nyaya Sanhita, 2023 to ensure liability for misleading AI claims, deepfake fraud, impersonation, and synthetic obscenity.

There are still challenges in identifying who is responsible, proving digital evidence, and enforcing laws across borders. However, India's balanced approach that is strict on accountability but flexible in how the rules are applied, makes it a forward-looking country that protects digital rights while supporting responsible AI innovation.

For any feedback or response on this article, the author can be reached on priya.shahdeo@ynzgroup.co.in and atharva.amdekar@ynzgroup.co.in

Author: Priya Shahdeo

Priya is a Senior Manager-Corporate Legal at YNZ Legal. By qualification she has completed her Bachelor of Arts and Bachelor of Law from Bharati Vidyapeeth Deemed University.

Co-author: Atharva Amdekar

Atharva is an Associate at YNZ Legal. By qualification he is Bachelor of Commerce and Bachelor of Law from Mumbai University