INDIALAW

DATA PRIVACY

Ctrl+Alt+Regulate: AI’s Takeover Of Media And Its Legal Crossroads

AUTHOR Abha Shah

PUBLISHED 17 November 2025

Table of contents

Series 1: “Artificial Intelligence and the Media: A Legal Perspective on the New Frontier”

Artificial Intelligence has undeniably become a transformative force in the media and entertainment industry across the globe by enhancing creativity, and opening new frontiers in content production, editing, distribution, analytics, moderation and monetization. From AI-generated scripts and synthetic voices to hyper-personalized recommendations and immersive storytelling, the technology is not just augmenting human creativity — in some cases, it’s beginning to replace it.

Several AI tools have been developed and are developing at accelerated pace globally to ensure advancement of the automation and reduction of human involvement.

While lot of media companies have heavily invested in AI generated machines to get quick and efficient outcomes at effective cost.

Some of the areas where these AI tools are used by the media companies and media personnels are as follows:

1. Content Creation:

- Scriptwriting & Storyboarding: Helping writers generate plots, character arcs, dialogues.
- Video Generation: Creation of short videos or explainer content using text prompts or avatars.
- News Writing: Auto-generation of earnings reports, sports recaps, and weather summaries.

2. Audio & Voice Cloning:

- AI voice cloning for dubbing or voiceovers.
- Text-to-speech narration for audiobooks or podcasts.

3. Image & Video Editing / VFX:

- AI-based editing
- Upscaling, color correction, object removal, and background editing.
- Deepfake tools for realistic face swapping or aging (used in Hollywood VFX).

4. Content Personalization & Recommendation: Streaming platforms (e.g. Netflix, YouTube, Spotify) use AI to:

- Recommend shows/music based on behaviour.
- Auto-generate thumbnails or trailers.
- Adjust recommendation algorithms dynamically.

Netflix uses AI to create **localized thumbnails** for different audiences to boost engagement.

5. Fake News Detection & Fact-Checking:

- Detect **manipulated content** (e.g. deepfakes).
- Flag **misinformation** using NLP and pattern recognition.

6. Content Moderation: Social media platforms (e.g. **Meta**, **X**, **YouTube**) use AI to:

- Flag hate speech, nudity, graphic content.
- Automatically take down violating posts or ads.
- Moderate live content.

7. Audience Engagement & Chatbots:

- **AI news anchors** (e.g. India Today's Sana, China's AI anchor).
- **Chatbots** for media websites, news services, or fan engagement (e.g. ChatGPT plugins, WhatsApp news bots).
- **AI companions** in fandom and entertainment.

8. **Analytics & Ad Targeting**: AI analyses viewer data to:

- Optimize ad placements.
- Predict audience drop-off.
- Recommend best publishing times.

9. Rights Management & Monetization:

- **AI-powered copyright tracking** on YouTube (Content ID).
- Monetization platforms use AI to match content with high-paying ads or partners.
- **AI watermarking** and **provenance** tools for AI-generated media

10. **Archiving, Indexing & Search:** Media houses use AI to:

1. Tag and categorize massive video/audio archives.
2. Use speech-to-text for searching video transcripts.
3. Extract metadata automatically.

In addition to the above,(a) **Digital humans / AI influencers** (e.g. Lil Miquela), (b) **AI co-hosts** in radio shows or live podcasts; (c) **AI-powered documentaries** with dynamic narration (user-customizable storylines); and (d) **Immersive journalism** using generative 3D/VR/AI narration; is being experimented and also cutting-edge in Media.

While the rapid evolution of AI generated tools, technologies and machines have proven to be a boon for the industry, they have also brought parallel set of legal, ethical, and societal concerns

- Deepfakes & misinformation
- Consent & privacy (especially for voice clones)
- Copyright violations
- Transparency in AI-generated journalism
- Labor displacement in creative roles

In light of the aforesaid concerns, number of queries have arisen which needs to be addressed: Are the usage of AI generated machines / tools and their outcome legal or illegal? Are these authorised and fall under fair use principle? Do they require prior approvals?; etc.

Conclusion: As the line between real and synthetic media blurs, the urgency to establish clear regulatory frameworks becomes critical.

Going forward, the challenge lies in balancing innovation with accountability. India like many other jurisdictions must evolve its laws to address the unique risks posed by AI, especially in protecting individual rights, ensuring transparency, and upholding public trust in digital content.

With thoughtful regulation, robust enforcement, and industry self-regulation, AI can be harnessed responsibly to power the future of media without compromising on ethics or legality.

Series 2: Content Moderation vs Freedom of Expression: India's Evolving Legal Framework

In the age of artificial intelligence (AI), content on social media, messaging platforms, and digital publications evolves rapidly. Automatic image generation, deepfakes, algorithmic recommendation, and AI?enabled content filtering are becoming central features of the digital ecosystem.

Hence AI has posed new challenges like:

- **Deepfakes and Synthetic Media:** AI-generated images, videos, or audio can falsely depict people, leading to defamation, identity theft, and privacy breaches.
- **AI Moderation Risks:** Automated tools for detecting harmful content (hate speech, misinformation, etc.) can make errors, show bias, and wrongly suppress legitimate speech.
- **Speed vs. Due Process:** Rapid, large-scale AI moderation may bypass context, appeals, and human review, removing lawful content unfairly.
- **Opacity and Bias:** AI systems often lack transparency and may misinterpret language or cultural nuances, especially in India's multilingual environment.

Hence, these developments and challenges pose difficult questions:

- How much moderation is legally permissible?
- Who should decide?
- How to protect users' rights especially freedom of speech?

> **What are the current legal landscape in India around content moderation in the AI era AND ARE they enough?**

1. Freedom of Speech Under the Constitution

1. **Article 19(1)(a)** of the Indian Constitution guarantees freedom of speech and expression.
2. However, this right is **not absolute**. Article 19(2) allows the State to impose **"reasonable restrictions"** in the interests of *public order, decency or morality, sovereignty and integrity of India, security of the State, friendly relations with foreign states, contempt of court, defamation, incitement to an offence*, etc.

The legal test has to ensure that: The restriction is provided by law. The restriction is for a legitimate state interest (one of those enumerated). It is proportionate, not arbitrary or overbroad.

While **freedom of expression** is a constitutional right with valid legal restrictions, the rise of AI complicates every piece of the puzzle; both enabling novel harms and presenting legal?and?ethical risks and challenges.

2. Key Laws & Statutes

A. Information Technology (IT) Act, 2000 —

- The IT Act, 2000 was enacted to provide legal recognition to electronic communications and transactions, and to combat cybercrime; aligning India with global standards like the **UNCITRAL Model Law on Electronic Commerce.**
- The main objective of this Act was to (i) legalize electronic records and digital signatures; (ii) facilitate e-commerce and e-governance; (iii) penalize cybercrimes; (iv) protect user data and privacy; (v) Imermediary liability i.e. platforms must follow due diligence to avoid liability for user-generated content; and (v) establish regulatory bodies for digital certification.

B. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, commonly known as the "IT Rules, 2021":

- The IT Rules, 2021 were notified under the **Information Technology Act, 2000** to regulate digital platforms, ensure accountability of intermediaries (like social media companies), and establish a code of ethics for digital news and OTT platforms.
- The key objectives of this IT Rules 2021 was to (i) empower users against misuse of digital platforms; (ii) ensure transparency and accountability of intermediaries; (iii) Regulate digital news and OTT content through a structured grievance redressal mechanism.

C. Amendment 2022 to IT Rules, 2021 (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021) —

- The amendment aimed to strengthen user rights, enhance platform accountability, and streamline grievance redressal mechanisms under the existing IT Rules, 2021.
- A new **GAC** was established to hear appeals from users dissatisfied with decisions made by platform grievance officers and is empowered to reverse or modify decisions and ensure timely resolution.
- Furthermore, more obligations were inflicted on intermediaries like ensuring compliance with user agreements and privacy policies and preventing users from uploading or sharing prohibited content.
- Also, platforms were brought under the scanner to have more transparency and accountability.

D. Amendment 2023 to IT Rules, 2021 (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021) —

- This amendment is to focus on **fake news regulation** and **online gaming oversight**.
- Under fake news regulations (i) fact check became mandatory for intermediaries who ae answerable to fact check authority; and (ii) Platforms failing to remove flagged content risk losing legal immunity (safe harbour) from liability for user-generated content.
- Under online gaming regulations (i) Online gaming platforms must register with SRBs to certify games as *"permissible"*—i.e., free from gambling or betting elements; (ii) Platforms must disclose refund policies, KYC norms, and game mechanics; and (ii) Platforms must appoint a **Chief Compliance Officer**, **Nodal Contact Person**, and **Resident Grievance Officer**, all based in India.
- And now with recent **Promotion and Regulation of Online Gaming Act, 2025 effective from October 1, 2025, (i)** All forms of online real-money gaming (RMG) are outlawed, regardless of whether they're skill-based or chance-based; and (ii) Financial institutions are barred from processing transactions for banned platforms.

E. Amendment 2025 to IT Rules, 2021 (Intermediary Guidelines and Digital Media Ethics Code Rules, 2021) —

- On 22 October 2025, the Ministry of Electronics & Information Technology (MeitY) notified the IT (Intermediary Guidelines & Digital Media Ethics Code) Amendment Rules, 2025.
- These amendments are set to come into force from 15 November 2025.
- The key change is in Rule 3(1)(d) — it strengthens the obligations of intermediaries ("platforms") when they have *actual knowledge* of unlawful content.
- The stated goals: more transparency, proportionality, and accountability in how takedowns are done

How has Indian courts reacted to this?

Precedent Case Laws: Here are some of the most significant recent legal / regulatory instances in India involving AI / synthetic media, content misuse, and how they interact with media law / freedom of expression.

- **Shreya Singhal v. Union of India (2015)**: The Supreme Court of India struck down Section 66A of the IT Act (which criminalized sending "offensive" messages via electronic communication.) as unconstitutional because it violated Article 19(1)(a) and was not saved under Article 19(2).The Court held the provision **unconstitutional** for violating **Article 19(1)(a)** (freedom of speech and expression), as it was **vague, overbroad**, and had a **chilling effect** on online speech. The judgment emphasized that restrictions on speech must be **reasonable and clearly defined**, and that vague laws risk arbitrary enforcement. It marked a major victory for **digital rights** and **free expression** in India.
- **Kunal Kamra v. Union of India (2023?/2024)**: The Bombay High Court (through a tie?breaker) struck down the IT Rules (2023 amendment) provision that empowered a government?fact?checking unit to label content about government affairs as false or misleading. It was held to violate Articles 14 (equality), 19(1)(a), and 19(1)(g), in part because of vagueness, arbitrariness, and the chilling effect on speech. The government amended the IT (Intermediary Guidelines & Digital Media

Ethics) Rules in 2023 to include a “fact?check unit” that would identify content about the “business of the Central Government” as fake/false/misleading, and require intermediaries to take “reasonable efforts” to deal with it. Critics argued this could lead to censorship or overreach, especially of satire/parody. Bombay High Court, after a split verdict, referred to a third judge. On **20 September 2024**, Justice A.S. Chandurkar (the third judge) held that the 2023 amendments (Fact?Check Unit provisions) were unconstitutional: they were vague, overbroad, lacked procedural safeguards, threatened freedom of speech and expression and disproportionately restricted expression—especially satire, parody, and criticism. The judgment is a landmark precedent limiting government control over digital content and reinforcing constitutional protections for speech .It sets limits on how much regulatory power government can exercise over content, especially via mandatory “reasonable efforts” clauses and fact?checking units controlled by government.

- Indian Courts have recently ordered takedown of AI?generated images of various celebrities \ being used without consent. This shows how AI?based misuse (image misuse, persona rights) is receiving judicial attention.

Key Lessons from These Indian Developments

From these cases, some consistent themes emerge:

1. **Protection for Satire / Parody / Criticism**: The Kamra case makes clear that satire/criticism (especially of government) is essential speech that needs protection; rules that can suppress such speech risk being struck down. Vague fact?checking or “reasonable effort” clauses, if uncontrolled, may arbitrarily catch satire.
2. **Judicial Demand for Procedural Safeguards and Clarity**: Laws / rules that define vague terms (e.g. “fake or misleading,” “business of the Central Government,” “reasonable efforts”) without guardrails are likely to be held unconstitutional. Citizens / content creators need notice, opportunity to respond, appeals, transparency.
3. **Takedown / Removal Powers in AI Context Are Being Used**: For misuse: courts have ordered websites/platforms to take down AI content (misuse of identity, deepfake images etc.). The law (IT Act, intermediary rules) provides route for removal, but enforcement, speed & effectiveness are variable.
4. **Chilling Effect is a Real Concern**: When regulatory rules risk imbalance (government as arbiter of truth, without safeguards), creators / critics fear penalty, over?censorship. That can suppress speech, even when lawful. The Kamra case shows courts are aware of this and willing to protect speech.

Conclusion:

The Indian legal landscape in 2024?25 shows that courts are pushing back against overbroad attempts by the government to control online speech via AI or content moderation rules that lack clarity or procedural safeguards. The **Kamra** case is especially important—it underscores that while governments may have legitimate aims (combating misinformation, preserving public order, protecting reputation), regulation must respect constitutional rights, due process, transparency, and avoid chilling speech (especially satire, criticism of government). Further, AI?based misuse (image misuse, persona rights) is also receiving judicial attention In general, courts are balancing personality rights, defamation, privacy claims vs free speech.

Series 3: When Fame Becomes a Filter: Deepfakes and the New Legal Battle for Celebrities

Personality Rights vs Privacy Rights

	Personality Rights	Privacy Rights
Definition	Personality rights protect an individual’s identity like name, image, likeness, voice, signature, and other unique trait; from unauthorized commercial use.	Privacy rights safeguard an individual’s personal life from intrusion, surveillance, or unauthorized disclosure.

Laws	**Article 21 of the Constitution**: Rooted in the right to life and personal liberty, which includes dignity and autonomy.**Copyright Act, 1957**: Sections 38A and 38B protect performers' rights and moral rights.**Trade Marks Act, 1999**: Allows individuals to trademark names, catchphrases, and other identifiers.**Common Law Tort of Passing Off**: Prevents false endorsement or misrepresentation.	**Article 21 of the Constitution**: Recognized as a **fundamental right** (Justice K.S. Puttaswamy v. Union of India, 2017). **Information Technology Act, 2000**: Sections 43A and 72 protect digital privacy and data handling. **Digital Personal Data Protection Act, 2023**: Regulates collection, storage, and processing of personal data. **The Bharatiya Nyaya Sanhita (formerly known as Indian Penal Code (IPC))**: Sections on voyeurism, defamation, etc.
Protected Interests	Public persona, celebrity image, economic value of identity	Personal life, family, communications, health records, biometric data, etc.
Who is Protected?	Mostly **public figures, celebrities, performers**, and individuals with commercial value attached to their identity	**All individuals**, regardless of status or fame.
Nature of Right	**Economic + dignitary** right – protects against **commercial exploitation**	**Fundamental right** – protects **personal autonomy, dignity, and liberty**
Posthumous Rights	May survive the death of the person (e.g., heirs controlling use of image, name)	Typically do **not survive death**, unless tied to other rights (e.g., defamation of deceased)
Violation Examples	Using a celebrity's photo in an ad without consent Creating merchandise with a famous person's likenessDeepfake videos used for marketing	Surveillance without consent Unauthorized disclosure of medical records Publishing intimate or private details without permission
Key Case Laws	*ICC Development v. Arvee Enterprises* (2003) *Titan Industries v. Ramkumar Jewellers* (2012) *DM Entertainment v. Baby Gift House* (2003)	*K.S. Puttaswamy v. Union of India* (2017) *R. Rajagopal v. State of Tamil Nadu* (1994) *Justice K.S. Puttaswamy (Retd.) v. Union of India* (Aadhaar case)

What are Deepfakes and why it has become a hot topic?

Deepfakes refer to realistic but artificially generated or altered audio-visual content, where a person's likeness (face, voice, body) is replaced or mimicked using AI techniques, often without their consent, to create misleading or false representations.

They've become a hot topic because they **threaten truth, trust, and privacy** in the digital age:

1. **Misinformation & Political Manipulation**
   - Deepfakes can spread false narratives during elections or crises, misleading the public.
   - Example: fake political speeches or doctored news clips shared on social media.
2. **Defamation & Harassment**
   - They're often used for non-consensual sexual content, especially targeting women and celebrities.
   - Victims face emotional and reputational damage with limited legal recourse.
3. **Fraud & Identity Theft**
   - Deepfake voice or video can impersonate CEOs, officials, or relatives to scam individuals or organizations (so-called "voice cloning scams").
4. **Erosion of Trust**
   - The line between truth and fabrication blurs — people begin doubting even real content ("liar's dividend").
5. **Legal & Ethical Challenges**
   - Most countries lack specific laws addressing deepfakes.
   - Raises complex questions of consent, copyright, privacy, and free speech.
6. **Rapid Technological Growth**
   - AI tools for generating deepfakes are now cheap, fast, and accessible — anyone can create realistic synthetic media with minimal skill.

Latest Developments in Indian Courts

The Indian courts are increasingly treating misuse of likeness, voice, image in AI content as a legal harm — not just "free speech" exceptions. Identity misuse has real reputational, privacy, and sometimes commercial harm.

The Indian courts have issued orders in last couple of years against the platforms, websites, URLs against using or monetizing unauthorised and infringing content (i.e. deepfakes, voice cloning, face morphing, etc through various Artificial Intelligence (AI) tools, Generative Artificial Intelligence tools) of the various personalities i.e **Asha Bhosale, Anil Kapoor, Amitabh Bachchan, Abhishek Bachchan, Aishwarya Rai Bachchan, Jackie Shroff, Karan Johar, Suniel Shetty, Akshay Kumar, Cheeranjeevi, Arijit Singh and Hritik Roshan** – where courts have protected their moral rights, personality rights including their name, voice, signatures, photograph, images, caricatures and other various attributes of these personalities; by immediate removal/ takedown of these unauthorised and infringing content of these personalities.

Comparative Analysis in Various Jurisdictions

Jurisdiction	Key Laws / Regulations	Focus Areas	Obligations / Requirements	Penalties / Enforcement
European Union	EU AI Act (2024), Digital Services Act (DSA)	Risk-based AI regulation; transparency; platform accountability	– Label AI-generated & deepfake content – Transparency about training data – Risk assessment for high-risk AI – Mandatory takedown for harmful content	Heavy fines (up to 7% of global turnover); enforcement by national & EU bodies
United Kingdom	Online Safety Act (2023) + AI White Paper (2024)	Harmful content moderation; deepfake regulation	– Duty of care for platforms – Transparency & risk-mitigation – Labelling manipulated media	Large fines (up to 10% of global turnover); Ofcom enforcement
United States	Take It Down Act (2025), DEFIANCE Act (2024), State-level laws (e.g., CA, TX, NY)	Non-consensual intimate deepfakes; platform responsibility	– 48-hour takedown of reported deepfake content – Civil remedies for victims – Disclosure rules in elections (some states)	Civil damages; platform penalties; criminal sanctions in certain states
France / Denmark (EU examples)	National deepfake & likeness rights laws (2024–25)	Non-consensual deepfakes; individual image rights	– Consent required for sharing manipulated media – Protection of personal likeness & voice	Criminal & civil liability; fines and imprisonment
South Korea	Amended Sexual Violence Punishment Act (2024)	Creation, distribution, or viewing of explicit deepfakes	– Ban on producing, sharing, or even watching non-consensual deepfakes	Up to 3 years in prison + fines (~USD 30,000)
Japan	Draft AI Regulation Bill (2025)	Deepfake labelling; data transparency	– Mandatory labelling for AI-altered content – Data disclosure for AI models	Administrative fines; platform obligations
China	Deep Synthesis Provisions (2023)	Deepfake transparency & real-name verification	– Label AI-generated media – Platforms must review & verify content origin	Fines, suspension of services, criminal charges for malicious use

India	IT Act, 2000, IT Rules (2021), Digital Personal Data Protection Act, 2023	No specific AI/deepfake law yet; general IT & data privacy laws apply	– Platforms must remove harmful/deceptive content on notice – Personal data requires consent – Government exploring AI framework	Penalties for non-compliance under IT Act & DPDP Act; potential criminal liability

Is it worth for these Bollywood celebrities to go to court for protecting their personality rights especially when they cannot enforce Indian orders aboard?

Indian court orders have limited enforceability abroad, especially when the deepfake or misuse happens on foreign platforms or servers:

- **Cross-border enforcement** is complex; orders may not bind a person or company without presence in India.
- **Anonymity & decentralization** make it hard to identify creators or original uploaders.
- **Speed vs. spread**: Deepfakes often go viral faster than legal remedies can act.

However, even if enforcement abroad is tough, it is still worth to file in India due to **strategic and practical reasons**:

(a) Immediate Deterrence within India

- Courts can issue **injunctions** to stop local sharing, block links, or order takedowns under the **IT Rules, 2021**.
- Platforms with Indian operations (YouTube, Meta, X, etc.) must comply with Indian orders — even if the servers are overseas.

(b) Reputation Management & Legal Record

- Filing a case publicly asserts ownership over one's **digital identity and brand**.
- It creates a **legal trail** — useful for future global takedown requests or negotiations.

(c) Basis for International Enforcement

- Indian injunctions can be presented to **foreign platforms or courts** as supporting documents.
- Under **comity of nations**, some jurisdictions consider such orders persuasive, even if not binding.

(d) Leverage for Platform Compliance

- Global tech companies generally follow a **"notice-and-takedown"** policy — and an Indian court order provides legal legitimacy for removal requests.

Legislative & Policial Currents

- India's Digital India Act (expected 2026) is likely to modernize AI and deepfake regulation, improving enforceability.
- Global cooperation on AI ethics and digital identity (e.g., G20, EU–India tech dialogues) is growing.
- Platforms are under mounting global pressure to detect and label AI-generated media proactively.

Conclusion:

The aforesaid orders passed by Indian Courts shows that law is adapting: remedying identity misuse, unauthorized use of likeness, non?consensual AI?generated content. These are essential tools in protecting individuals.

However,the AI era will keep creating new challenges (synthetic media, automated moderation errors, algorithmic bias, malicious uses), so legal frameworks must be agile, rights?sensitive, and backed by strong judicial oversight.

Further in comparison with the other jurisdictions, India can refine regulation: focus on definitions, procedural fairness, transparency, tailored regulation, and balancing obligations with rights.

Series 4: Untraceable URLs in India Travelling to Servers Across the World: Navigating the Complex Web of Technology, Law, and Accountability

Introduction

In today's digital world, every online action—from clicks to website visits—begins with a URL (Uniform Resource Locator), which functions as a digital address directing browsers to specific web content. A typical URL (e.g., "www.example.com/page") consists of components like the protocol ("https://"), domain name ("example.com"), and a path ("/about-us"). Creating a URL involves registering a domain name via registrars such as GoDaddy or Namecheap, obtaining web hosting, and linking it to website content. In India, except for government-registered domains through the NIC Portal (registry.gov.in), no government identification is required, making the process accessible and democratizing online expression. Understanding "untraceable" URLs—those whose creators, owners, or hosts cannot be easily identified—is essential for developing effective frameworks that balance digital freedom with security, enabling India to build robust cybersecurity infrastructure while protecting individual rights and national interests.

Understanding URL Traceability: The Technical Foundation

URLs are inherently traceable because they point to specific resources on the internet. However, the degree to which a URL can be traced depends on several factors, creating opportunities for both transparency and privacy:

What Makes a URL Traceable? • Domain registration provides transparency and accountability. • Server logs track IP addresses, timestamps, and user agents. • Shortened URLs maintain redirect logs for accountability. • Tracking parameters help businesses understand user behaviour.

Can URLs Be Partially or Sometimes Untraceable?

- Self-hosted redirectors offer flexible logging policies.
- Ephemeral URLs provide enhanced privacy through quick expiration.
- Tor hidden services offer enhanced anonymity.
- Peer-to-peer protocols (IPFS) provide decentralized alternatives.
- Privacy techniques create partial protection while maintaining some accountability.
- Complete untraceability is extremely difficult to achieve in practice.

Benefits and Applications of URL Privacy

Privacy Benefits: Enhanced user anonymity, protection from behavioural tracking, reduced commercial surveillance, and secure communication for activists, journalists, and whistleblowers.

Practical Considerations: Website analytics improve services; logging assists security and technical troubleshooting. Balance drives innovation in digital governance.

India's Coordinated Multi-Agency Framework

- MeitY handles IT policy and content management.
- CERT-In provides technical cyber incident response.
- MHA addresses national security considerations.
- I4C facilitates inter-agency collaboration and joint operations.
- DoT regulates ISPs; TRAI oversees digital communication.
- State cyber cells and CBI implement enforcement actions.
- Coordinated approach enables swift, unified responses.
- Traceable URLs provide clear ownership trails through WHOIS records.
- Privacy-enhanced URLs use legitimate services like WhoisGuard and VPNs.
- International cooperation through MLAT helps cross-border investigations.

Building Proactive Solutions: Technology Meets Policy

India, rather than relying solely on reactive measures, the government is developing forward-looking AI-based detection systems like "***Cyber Swachhta Kendra"***. These systems use machine learning to identify concerning patterns, understand coordinated activities, and anticipate emerging challenges. Drawing inspiration from frameworks like the EU's AI Act, India is crafting technology-neutral principles and AI-specific provisions that strengthen cyber regulatory capabilities while respecting innovation and fundamental rights.

Conclusion

While untraceable URLs may never be entirely eradicated, consistent legal evolution, technological innovation, and international collaboration can make them increasingly manageable. Backed by its expanding digital infrastructure, growing cybersecurity expertise, and strong political resolve.

The upcoming **Digital India Act** offers India a major chance to modernize digital governance by balancing security, accountability, and fundamental rights. Through stronger institutions, innovative laws, advancing technology, and international cooperation, the country is developing more sophisticated responses to digital challenges.

Supported by expanding digital infrastructure, improved cybersecurity capabilities, and firm political commitment, India is steadily positioning itself as a global model for secure, rights-based, and future-ready digital governance.

Related Practice Areas

Information Technology