INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

# INTELLECTUAL PROPERTY RIGHTS AND CYBERSECURITY IN INDIA'S DIGITAL MEDIA AND ENTERTAINMENT INDUSTRY: A COMPARATIVE ANALYSIS OF LEGISLATIVE CONVERGENCE

**AUTHOR –** POTTA V N VAMSI KRISHNA, STUDENT AT CHRIST (DEEMED TO BE UNIVERSITY) LAVASA, PUNE

**BEST CITATION –** POTTA V N VAMSI KRISHNA, INTELLECTUAL PROPERTY RIGHTS AND CYBERSECURITY IN INDIA'S DIGITAL MEDIA AND ENTERTAINMENT INDUSTRY: A COMPARATIVE ANALYSIS OF LEGISLATIVE CONVERGENCE, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (8) OF 2026, PG. 797-806, APIS – 3920 – 0001 & ISSN - 2583-2344.

**Abstract**

India's digital media and entertainment industry, valued at approximately USD thirty billion and growing at ten to twelve percent annually, confronts a convergent regulatory crisis: intellectual property violations and cybersecurity breaches are no longer separable phenomena. Digital piracy, ransomware attacks on production infrastructure, pre-release content leaks, and AI-generated deepfakes impose estimated annual losses of USD 2.8 to 3.5 billion. India's regulatory response—anchored in the Copyright Act, 1957 and the Information Technology Act, 2000—operates in structural isolation, without coordinated enforcement mechanisms, a statutory notice-and-takedown regime, mandatory cybersecurity standards, or legislative provisions addressing synthetic media. This article undertakes a doctrinal and comparative analysis of India's legal architecture benchmarked against the United States Digital Millennium Copyright Act, the EU General Data Protection Regulation, the EU Directive on Copyright in the Digital Single Market, the EU AI Act, and the WIPO Internet Treaties. Five structural legislative gaps are identified: absent anti-trafficking provisions in anti-circumvention law, no statutory notice-and-takedown mechanism, inadequate mandatory cybersecurity obligations, insufficient platform filtering liability, and a regulatory void on AI-generated content and deepfakes. A targeted five-point reform agenda is proposed.

**Keywords:** intellectual property; cybersecurity; Copyright Act 1957; DMCA; DSM Directive; deepfakes; intermediary liability; digital piracy; India

## I. INTRODUCTION

The digital transformation of the global media and entertainment industry has rendered the traditional regulatory separation between intellectual property law and cybersecurity law analytically untenable. Creative content is now produced, stored, and distributed through digital networks that are simultaneously vectors of intellectual property infringement and targets of cyberattack. A ransomware attack on a major film studio's post-production facility is both a cybersecurity incident and an enabler of intellectual property theft; a data breach exposing a streaming platform's unreleased content is simultaneously a violation of data security obligations and a copyright infringement event. These phenomena demand integrated regulatory treatment that India's existing legal architecture does not provide.[965]

India's digital media and entertainment sector occupies a position of global significance. Bollywood and regional cinema, large-scale

[965]FICCI-EY, India's Media & Entertainment Sector: Resilient, Repurposed, Reimagined 14 (2023); Nishith Desai Assocs., The Indian Media & Entertainment Industry 2 (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

recorded music, rapidly expanding over-the-top (OTT) streaming platforms, live sports broadcasting, gaming, and digital publishing together constitute one of the world's most prolific and economically consequential creative economies. The sector faces a commensurately acute threat landscape: systematic digital piracy of theatrical and streaming content, ransomware attacks on production and post-production infrastructure, pre-release leaks of high-value original productions, and the weaponization of generative artificial intelligence for deepfake fraud and non-consensual identity appropriation. Industry estimates attribute USD 2.8 to 3.5 billion in annual revenue losses to digital piracy alone, a figure that excludes downstream effects on employment, investment incentives, and the competitive disadvantage imposed on licensed platforms relative to piracy operators who bear no content acquisition costs.[966]

India's current regulatory framework—primarily the Copyright Act, 1957 and the Information Technology Act, 2000—was constructed in different eras, for distinct purposes, and administered by separate institutional actors operating without coordination mechanisms. These statutes exist without shared institutional oversight or a common conceptual framework for addressing threats that simultaneously constitute intellectual property violations and cybersecurity incidents. The resulting structural disjuncture generates five compounding legislative gaps: absent anti-trafficking provisions in anti-circumvention law; no statutory, structured notice-and-takedown mechanism; inadequate mandatory cybersecurity obligations for the entertainment sector; an insufficiently demanding intermediary liability framework; and a complete regulatory void concerning AI-generated content and deepfakes.[967]

This article examines each gap through doctrinal and comparative analysis. Part II analyses India's legal architecture and its judicial innovations. Part III compares the DMCA, the EU's integrated multi-layered framework, and the WIPO Internet Treaties. Part IV diagnoses the specific legislative and enforcement gaps in India's framework. Part V proposes a targeted five-point reform agenda. Part VI concludes with observations on the broader significance of India's reform for the global digital creative economy.

## II. INDIA'S LEGAL FRAMEWORK: ARCHITECTURE AND LIMITATIONS

### A. The Copyright Act, 1957: Digital Adaptation and Residual Gaps

The Copyright (Amendment) Act, 2012 inserted Sections 65A and 65B into the Copyright Act, providing legal protection for Technological Protection Measures (TPMs) and Rights Management Information (RMI) respectively—India's primary legislative implementation of the WIPO Internet Treaty obligations. Section 65A prohibits circumvention of effective TPMs and prescribes penalties of up to two years' imprisonment and fine. Section 65B prohibits unauthorized removal or alteration of RMI and bars distribution of works from which RMI has been illegally stripped.[968]

However, unlike Section 1201(a)(2) of the Digital Millennium Copyright Act (DMCA), which prohibits the manufacture, importation, and distribution of circumvention devices—the anti-trafficking prohibition—Section 65A addresses only the act of circumvention itself. The upstream commercial ecosystem of circumvention tool development and distribution—including DRM-stripping software, streaming rippers, and circumvention services marketed directly to consumers—accordingly falls entirely outside the statute's reach. This creates an exploitable gap enabling the supply of circumvention tools without legal consequence under Indian law, directly

[966]FICCI-EY, India's Media & Entertainment Report 2024: The Age of Resilience 84 (2024) (estimating annual digital piracy losses at USD 2.8–3.5 billion).

[967]Copyright Act, No. 14 of 1957 (India); Information Technology Act, No. 21 of 2000 (India) [hereinafter IT Act].

[968]Copyright (Amendment) Act, No. 27 of 2012, §§ 65A–65B (India).

undermining the effectiveness of any TPM-based content protection strategy.[969]

Section 52 of the Copyright Act sets out fair dealing exceptions in a closed and exhaustive list—a structure increasingly ill-suited to the digital environment. Unlike the open-ended, four-factor balancing test of Section 107 of the United States Copyright Act, Section 52 cannot accommodate AI model training data mining, content caching by internet service providers, hyperlinking, or the creation of user-generated remixed content. The Bombay High Court's ruling confirmed that Section 31D's statutory licensing regime applies exclusively to traditional broadcast organizations and not to internet streaming services, imposing disproportionate licensing transaction costs on smaller OTT platforms building content libraries.[970]

**B. The Information Technology Act, 2000: Intermediary Liability**

Section 79 of the IT Act provides online intermediaries with a conditional safe harbour from third-party content liability. The Supreme Court's landmark decision in Shreya Singhal v. Union of India interpreted the 'actual knowledge' requirement of Section 79(3)(b)—which removes the safe harbour when an intermediary fails to expeditiously remove or disable access to unlawful content—as necessitating a court order or government notification rather than a private complaint from a rights holder.[971] This interpretation created a procedural delay irreconcilable with the economics of digital piracy enforcement: the commercial value of a pre-release film can be catastrophically diminished within hours of an unauthorized upload, yet rights holders must obtain interim injunctions before intermediaries' removal obligations are triggered.

The IT Rules, 2021 introduced a 36-hour takedown window for 'manifestly illegal' content and designated obligations for 'Significant Social Media Intermediaries' meeting specified user thresholds. However, without prescribed notice formats, counter-notification procedures, or sanctions for bad-faith notices, the Rules fall materially short of the operational clarity provided by DMCA Section 512. The manifestly illegal standard introduces threshold ambiguity that platforms routinely invoke to resist expedited removals in contested infringement cases, further extending the effective delay before removal occurs.[972]

**C. The Digital Personal Data Protection Act, 2023**

The Digital Personal Data Protection Act, 2023 (DPDP Act) imposes data security obligations on Data Fiduciaries—including OTT platforms, music streaming services, and digital gaming operators—and requires notification of personal data breaches to the Data Protection Board of India under Section 8(6). Its intersection with intellectual property enforcement is significant: a cyberattack on a major streaming platform simultaneously exposes subscriber personal data and commercially sensitive pre-release creative assets, engaging obligations under the DPDP Act and the Copyright Act without any statutory coordination between the two regimes. The DPDP Act's technology-neutral 'reasonable security' standard provides no sector-specific technical benchmarks for protecting unreleased content—a gap starkly apparent by comparison with the prescriptive mandatory standards of the EU's NIS2 Directive.[973]

**D. Judicial Innovations and Their Inherent Limits**

Indian courts have developed several remedial innovations that partially compensate for legislative gaps. The dynamic injunction framework, established by the Delhi High Court in UTV Software Communications Ltd. v. 1337X.to & Ors., enables automatic extension of website

[969] 17 U.S.C. § 1201(a)(2) (2018); Pamela Samuelson, Anticircumvention Rules: Threat to Science, 293 Science 2028, 2030 (2001).
[970] Tips Indus. Ltd. v. Wynk Music Ltd., CS(OS) No. 3088 of 2018 (Bombay H.C. 2019).
[971] Shreya Singhal v. Union of India, (2015) 5 SCC 1, ¶ 119 (India).
[972] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India) [hereinafter IT Rules 2021].
[973] Digital Personal Data Protection Act, No. 22 of 2023, § 8(6) (India) [hereinafter DPDP Act].

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

blocking orders to newly identified mirror sites without fresh litigation—addressing the proliferation problem of piracy platforms that circumvent blocking by registering new domains. Pre-emptive 'John Doe' injunctions issued in advance of theatrical releases grant rights holders a procedural advantage against anticipated piracy.[974]

In Anil Kapoor v. Simply Life India & Ors., the Delhi High Court issued India's first major injunction against AI-mediated celebrity identity appropriation—a significant doctrinal development. These judicial innovations are reactive, however: they require initiation and funding of High Court proceedings, creating access asymmetries that systematically disadvantage smaller rights holders and individual creators relative to institutional content owners with specialist litigation capacity. They cannot create systemic obligations—mandatory cybersecurity standards, upload filtering requirements, or breach reporting duties—that effective regulatory governance demands.[975]

## III. INTERNATIONAL COMPARATIVE FRAMEWORK

### A. The Digital Millennium Copyright Act (United States)

Title I of the DMCA (17 U.S.C. §§ 1201–1205) remains the primary international reference point for integrating copyright protection with cybersecurity measures. Its anti-trafficking prohibition—closing the gap between banning circumvention acts and banning the commercial supply of circumvention tools—directly addresses the structural deficiency in India's Section 65A. Title II's Section 512 safe harbour conditions platform immunity on structured notice-and-takedown compliance: rights holders submit standardized notices containing specified identification information; platforms must expeditiously remove identified content; alleged infringers may submit counter-notifications for content restoration; and parties submitting materially false notices face civil liability for resulting damages, costs, and attorneys' fees.[976][977]

The DMCA's documented limitations are instructive for India's reform design. The court in Universal City Studios, Inc. v. Reimerdes held DRM-decryption software to constitute an illegal circumvention device even when used to enable lawful fair use of legitimately purchased content on unsupported platforms—creating what scholars have characterized as a 'super-copyright' overriding legislated exceptions. The notice-and-takedown system's economics have been criticized as systematically favoring platforms over rights holders, requiring repeated re-notification as infringing content is immediately re-uploaded following removal. These limitations suggest India should adopt the DMCA's structural features while building in stronger procedural safeguards against over-removal and more efficient re-upload deterrence mechanisms.[978]

### B. The European Union: An Integrated Multi-Layered Framework

The EU has developed the most structurally integrated framework globally, combining data protection, copyright, cybersecurity, and AI governance across a suite of coordinated instruments. The General Data Protection Regulation (GDPR) intersects directly with IP enforcement strategies: the Court of Justice's ruling in Breyer v. Germany classified IP addresses as personal data, significantly complicating enforcement methods dependent on identifying infringers through technical network data. The Schrems II ruling, invalidating

[974]UTV Software Commc'ns Ltd. v. 1337X.to & Ors., CS(OS) 821/2017 (Delhi H.C. 2019) (extending blocking injunction automatically to mirror sites on rights-holder application).
[975]Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi H.C. 2023); Bobby Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Calif. L. Rev. 1753, 1758 (2019).
[976]Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.) [hereinafter DMCA].
[977]17 U.S.C. § 512(c)(1)(A)–(C) (2018); see Niva Elkin-Koren, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, 9 J. Telecomm. & High Tech. L. 39, 42 (2010).
[978]Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 325 (S.D.N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 8 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

the EU-U.S. Privacy Shield, imposed operational complexity on entertainment companies maintaining cross-border rights enforcement databases and content protection systems.[979][980]

The DSM Directive's Article 17 requires online content-sharing platforms to obtain licences from rights holders or demonstrate best efforts to prevent availability of identified works on their platforms—effectively mandating deployment of automated content recognition systems at scale. The Court of Justice upheld Article 17 in Republic of Poland v. European Parliament & Council, confirming that mandatory upload filtering is constitutionally permissible when accompanied by adequate procedural safeguards including an effective complaint and redress mechanism for users whose content is wrongly removed. The NIS2 Directive imposes twenty-one enumerated mandatory cybersecurity risk-management measures on digital service providers—creating binding minimum-security obligations that complement copyright enforcement with data integrity requirements significantly more prescriptive than India's reasonable security standard. The EU AI Act requires providers of general-purpose AI models to maintain copyright-compliant training data policies and imposes machine-readable watermarking obligations on AI systems generating synthetic audio-visual content.[981][982][983]

### C. WIPO Internet Treaties

The WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) establish the foundational international obligations for digital copyright governance. WCT Article 11 requires Contracting Parties to provide adequate legal protection and effective legal remedies against circumvention of effective TPMs used by authors in connection with protected works. India acceded to both treaties in 2018, implementing TPM obligations through Sections 65A–65B. This implementation is deficient in two material respects: the anti-trafficking gap in Section 65A, and the static character of the exceptions framework, which lacks the DMCA's adaptive triennial rulemaking mechanism enabling periodic calibration of permitted circumvention exceptions to evolving technological realities.[984]

## IV. CRITICAL LEGISLATIVE AND ENFORCEMENT GAPS

Five structural legislative gaps interact and compound within India's current framework. First, the absence of anti-trafficking provisions in Section 65A of the Copyright Act leaves the circumvention-tool ecosystem entirely unregulated under Indian IP law. DRM-stripping software, streaming rippers, and circumvention services marketed commercially to Indian consumers operate without statutory prohibition, directly undermining the effectiveness of TPM-based content protection and contravening India's obligations under WCT Article 11 and the WPPT's parallel provision, which require protection against both circumvention acts and the supply of circumvention means.

Second, the absence of a structured statutory notice-and-takedown mechanism is the most practically consequential gap. The Shreya Singhal interpretation of Section 79(3)(b) requires rights holders to obtain court orders before intermediary removal obligations are triggered. A pre-release film's entire commercial value window may be exhausted before interim relief can be secured. No comparable creative economy—the United States, the United Kingdom, the European Union, Australia, or Japan—operates its major digital content market without a structured private notice-and-

[979]Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR]; Case C-582/14, Breyer v. Bundesrepublik Deutschland, ECLI:EU:C:2016:779 (classifying IP addresses as personal data).
[980]Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. (Schrems II), ECLI:EU:C:2020:559.
[981]Council Directive 2019/790, 2019 O.J. (L 130) 92 (EU) [hereinafter DSM Directive], arts. 17(1), 17(4); Case C-401/19, Republic of Poland v. Eur. Parliament & Council, ECLI:EU:C:2022:297.
[982]Council Directive 2022/2555, 2022 O.J. (L 333) 80 (EU) [hereinafter NIS2 Directive], art. 21 (enumerating twenty-one mandatory cybersecurity risk-management measures).
[983]Regulation (EU) 2024/1689, 2024 O.J. (L) (EU) [hereinafter EU AI Act], arts. 50(2), 50(4), 53(1)(c).
[984]WIPO Copyright Treaty art. 11, Apr. 12, 1997, 2186 U.N.T.S. 121 [hereinafter WCT]; WIPO Performances & Phonograms Treaty art. 18, Apr. 12, 1997, 2186 U.N.T.S. 203 [hereinafter WPPT].

takedown mechanism. India's 36-hour window under the IT Rules 2021 addresses only manifestly illegal content and lacks the procedural architecture—prescribed notice formats, counter-notification, and false notice sanctions—needed for systematic enforcement.

Third, the intermediary liability framework imposes no proactive content filtering obligations on even the largest digital platforms. The IT Rules 2021's designation of Significant Social Media Intermediaries by user-number threshold does not require deployment of automated content recognition technology as a condition of safe harbour eligibility. This approach is increasingly indefensible as India's OTT market serves hundreds of millions of subscribers, and the technical capacity for automated content recognition is commercially available and routinely deployed in comparable jurisdictions.[985]

Fourth, the regulatory void concerning AI and synthetic media is the most urgent emerging gap. The Copyright Act's definition of 'author' cannot accommodate generative AI systems; no text-and-data-mining exception clarifies whether AI model training on copyrighted works is permissible under Indian law; and no statutory right of publicity protects individuals against non-consensual AI appropriation of name, likeness, voice, or performance. The judiciary's only available response—injunctive relief from the High Court—is reactive, financially inaccessible to ordinary individuals, and structurally unavailable against the systematic scale of AI-generated identity misappropriation on digital platforms at the speed at which such content propagates.

Fifth, enforcement architecture is fragmented across copyright, cybercrime, cybersecurity, and data protection authorities without any statutory coordination mechanism. Copyright enforcement is administered through the DPIIT; cybercrime through state police Cyber Crime Cells; cybersecurity incident response through CERT-In; and data protection through the Data Protection Board. No mechanism enables coordinated response to incidents—such as a ransomware attack exposing pre-release content—that simultaneously engage all four regulatory domains. The abolition of the Intellectual Property Appellate Board in 2021 concentrated IP adjudication in High Courts already burdened with substantial civil dockets, systematically disadvantaging smaller rights holders who cannot sustain High Court IP litigation.[986]

## V. REFORM AGENDA: TOWARD AN INTEGRATED FRAMEWORK

### A. Amend Sections 65A–65B: Anti-Trafficking Provisions and Security Research Exception

Section 65A must be amended immediately to add anti-trafficking provisions prohibiting the manufacture, importation, distribution, offering for sale, and commercial provision of any technology, device, or service primarily designed to circumvent effective TPMs—mirroring the prohibition in DMCA § 1201(a)(2). The legislative record should specify that this prohibition extends to software distributed online and to cloud-based circumvention services. Simultaneously, a bounded security research exception should permit circumvention for the purpose of identifying and responsibly disclosing vulnerabilities in content protection systems, conducted in controlled environments with reasonable prior notification to the rights holder. This exception is essential to India's growing cybersecurity research ecosystem and prevents the anti-trafficking prohibition from inadvertently chilling legitimate security research.

[985]Tribunals Reforms (Rationalisation and Conditions of Service) Ordinance, No. 2 of 2021 (India) (abolishing IPAB); Amlan Mohanty, The Abolition of the IPAB and Its Implications for IP Enforcement in India, 26 J. Intell. Prop. Rts. 234, 241 (2021).

[986]U.S. Trade Representative, Special 301 Report 47 (2024); Agreement on Trade-Related Aspects of Intellectual Property Rights art. 61, Apr. 15, 1994, 1869 U.N.T.S. 299 [hereinafter TRIPS].

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 8 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

**B. Enact a Statutory Notice-and-Takedown Mechanism**

A dedicated statutory provision—superseding the Shreya Singhal court-order interpretation for IPR-related removal requests—should establish: mandatory standardized notice content including identification of the copyrighted work, the URL of the infringing material, and a declaration of good-faith belief in unauthorized use; a 48-hour removal window for clearly infringing material; a structured counter-notification procedure enabling alleged infringers to contest removal with an accompanying statement of lawful use; content-restoration timelines following valid counter-notification; civil liability for materially false notices; and a re-notification mechanism enabling expedited action when removed content is re-uploaded without authorization. An independent adjudicatory body should be designated for contested removals, relieving High Courts of case volumes that an operational notice-and-takedown system will generate.

**C. Graduated Platform Liability with Upload-Filtering Obligations**

A tiered platform liability regime should distinguish small platforms (fewer than 2.5 million registered users retaining the current safe harbour), significant platforms (2.5 to 10 million users required to implement best-efforts content identification for works for which rights holders provide reference fingerprinting data), and major platforms (over 10 million users subject to mandatory upload-filtering obligations). This graduated approach draws on DSM Directive Article 17 while incorporating the Court of Justice's safeguard requirements from Republic of Poland v. European Parliament & Council—an effective complaint and redress mechanism, transparency reporting, and prohibited general monitoring obligations—adapted to India's constitutional right to freedom of speech and expression under Article 19(1)(a).

**D. Sector-Specific Mandatory Cybersecurity Standards**

Mandatory cybersecurity standards specific to digital media and entertainment entities should prescribe: end-to-end encryption of pre-release creative content in storage and transit; multi-factor authentication for all personnel accessing unreleased productions; documented and biannually tested incident response plans; annual penetration testing of content management systems; and supply chain security requirements for third-party vendors handling creative assets. Non-compliance should attract regulatory penalties and civil liability to rights holders suffering consequential losses from cybersecurity failures—comparable to the NIS2 Directive framework that holds European digital service providers accountable.

**E. Dedicated Synthetic Media and AI Legislation**

A Synthetic Media and Artificial Intelligence (Regulation) Act should establish: mandatory disclosure of AI-generated or AI-manipulated audio-visual content through machine-readable metadata embedded at creation, publication, and distribution; a statutory right of publicity providing a cause of action where AI-generated synthetic media appropriates an individual's name, likeness, voice, or performance without consent; copyright clarifications for AI-assisted works; transparency obligations on AI developers to maintain and disclose training data records demonstrating copyright compliance or reliance on available exceptions; and a designated regulatory authority for AI transparency compliance monitoring, with enforcement powers including fines and take-down directions against non-compliant synthetic media. India's engagement with the Council of Europe's Framework Convention on Artificial Intelligence should be elevated from observer to treaty-party status, aligning domestic legislation with

the emerging international human rights framework for AI governance.[987]

## VI. CONCLUSION

India's media and entertainment industry is a globally significant creative economy confronting regulatory instruments designed for an earlier technological era. The structural disjuncture between copyright law and cybersecurity law—manifesting in five compounding legislative gaps—produces systemic enforcement failures whose economic costs are measurable, growing, and disproportionately borne by smaller creators and independent producers who lack resources to access High Court remedies. The estimated USD 2.8 to 3.5 billion in annual piracy losses is not merely a commercial statistic; it represents the systematic under-investment in original Indian content production that results when legal protection is structurally inadequate.[988]

The comparative analysis demonstrates that the most advanced international frameworks—the DMCA, the EU's integrated DSM Directive, GDPR, NIS2, and AI Act regime, and the WIPO Internet Treaties—each offer discrete elements India's reform agenda should absorb. The DMCA's anti-trafficking prohibition and structured notice-and-takedown procedure address India's first and second gaps. DSM Directive Article 17's graduated upload-filtering obligations address the third. NIS2's mandatory cybersecurity risk-management standards address the fourth. The EU AI Act's deepfake watermarking and training data transparency obligations address the fifth. Together, these elements constitute the architecture of a comprehensive integrated framework that India can construct, avoiding each source model's documented limitations.

The five-point reform agenda proposed in this article is achievable within India's existing legislative framework without constitutional amendment. Amendment of Sections 65A–65B, a statutory notice-and-takedown mechanism, graduated platform liability with upload-filtering, sector-specific mandatory cybersecurity standards, and a Synthetic Media and AI Act are individually targeted and collectively transformative. These reforms would simultaneously address the United States Trade Representative's longstanding concerns regarding Indian IP enforcement deficiencies, position India as a proactive architect of the international standards governing AI-generated content rather than a reactive recipient of norms shaped by others, and provide India's creative economy with the integrated regulatory protection commensurate with its global cultural and economic significance.[989]

REFERENCES

I. Cases

1. Anil Kapoor v. Simply Life India & Ors., CS(COMM) 652/2023 (Delhi H.C. 2023) (India).
2. Breyer v. Bundesrepublik Deutschland, Case C-582/14, ECLI:EU:C:2016:779 (Court of Justice of the EU 2016).
3. Data Prot. Comm'r v. Facebook Ireland Ltd. (Schrems II), Case C-311/18, ECLI:EU:C:2020:559 (Court of Justice of the EU 2020).
4. Republic of Poland v. Eur. Parliament & Council, Case C-401/19, ECLI:EU:C:2022:297 (Court of Justice of the EU 2022).
5. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).
6. Tips Indus. Ltd. v. Wynk Music Ltd., CS(OS) No. 3088 of 2018 (Bombay H.C. 2019) (India).

[987]Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, C.E.T.S. No. 225 (adopted Sept. 5, 2024); EU AI Act, supra note 17, art. 53(1)(c).
[988]See FICCI-EY, supra note 2, at 84; Chirag Mavani et al., The Role of Cybersecurity in Protecting Intellectual Property, 12 Int'l J. on Recent & Innovation Trends in Computing & Commc'n 529, 531 (2024).
[989]Poorva Bhaswar, Intellectual Property Rights and Cybersecurity in India: Comprehensive Analysis, 3 Indian J. Advanced Legal Rsch. 45, 52 (2023); U.S. Trade Representative, supra note 22, at 47.

7. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), aff'd sub nom. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).
8. UTV Software Commc'ns Ltd. v. 1337X.to & Ors., CS(OS) 821/2017 (Delhi H.C. 2019) (India).

II. Legislation

A. India

1. Copyright Act, No. 14 of 1957 (India).
2. Copyright (Amendment) Act, No. 27 of 2012, §§ 65A–65B (India).
3. Digital Personal Data Protection Act, No. 22 of 2023, § 8(6) (India).
4. Information Technology Act, No. 21 of 2000, §§ 43, 66, 79 (India).
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
6. Tribunals Reforms (Rationalisation and Conditions of Service) Ordinance, No. 2 of 2021 (India).

B. United States

1. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).
2. 17 U.S.C. §§ 107, 512, 1201–1205 (2018).

C. European Union

1. Council Directive 2019/790, 2019 O.J. (L 130) 92 (EU) [Directive on Copyright in the Digital Single Market].
2. Council Directive 2022/2555, 2022 O.J. (L 333) 80 (EU) [NIS2 Directive].
3. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [General Data Protection Regulation].
4. Regulation (EU) 2024/1689, 2024 O.J. (L) (EU) [Artificial Intelligence Act].
5. III. International Instruments
6. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299.
7. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, C.E.T.S. No. 225 (adopted Sept. 5, 2024).
8. WIPO Copyright Treaty, Apr. 12, 1997, 2186 U.N.T.S. 121.
9. WIPO Performances and Phonograms Treaty, Apr. 12, 1997, 2186 U.N.T.S. 203.

IV. Books and Reports

1. FICCI-EY. India's Media & Entertainment Report 2024: The Age of Resilience. EY India, 2024.
2. FICCI-EY. India's Media & Entertainment Sector: Resilient, Repurposed, Reimagined. EY India, 2023.
3. Nishith Desai Associates. The Indian Media & Entertainment Industry. Nishith Desai Associates, 2023.
4. U.S. Trade Representative. Special 301 Report. Office of the United States Trade Representative, 2024.

V. Journal Articles

1. Bhaswar, Poorva. Intellectual Property Rights and Cybersecurity in India: Comprehensive Analysis. 3 Indian J. Advanced Legal Rsch. 45 (2023).
2. Chesney, Bobby & Danielle Keats Citron. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. 107 Calif. L. Rev. 1753 (2019).
3. Elkin-Koren, Niva. Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic. 9 J. Telecomm. & High Tech. L. 39 (2010).
4. Mavani, Chirag et al. The Role of Cybersecurity in Protecting Intellectual Property. 12 Int'l J. on Recent & Innovation Trends in Computing & Commc'n 529 (2024).

5. Mohanty, Amlan. The Abolition of the IPAB and Its Implications for IP Enforcement in India. 26 J. Intell. Prop. Rts. 234 (2021).
6. Samuelson, Pamela. Anticircumvention Rules: Threat to Science. 293 Science 2028 (2001).
7. Saikia, Nandita. Data Protection and Content Regulation in India: Toward a Comprehensive Framework. 9 Indian J.L. & Tech. 71 (2024).