

# Why Piracy Keeps Winning Despite India's Legal Framework

Author | **Jhanvi Anam**

Edited by | **Dedipyaman Shukla**

# Introduction

The Media and Entertainment (**M&E**) sector is transforming content consumption methods and distribution patterns, prompting parallel evolution in methods of piracy. The piracy ecosystem has moved from shaky camcorder recordings to torrent files, and now, to high-quality streaming. Consumers increasingly expect better-quality pirated content, and there is a lesser inclination to access low-resolution camcorder leaks. This shift indicates a piracy ecosystem that primarily targets digital platforms, such as over-the-top (**OTT**) services, rather than theatrical releases, implying that OTT platforms may now bear a greater share of revenue loss compared to cinemas.

To deter piracy, a range of legal safeguards have been put in place. Indian courts have introduced tools such as John Doe (Ashok Kumar) orders, dynamic and dynamic± injunctions to allow rights holders to block infringing websites. These have been supplemented by a strong legislative framework. Despite the range of legal safeguards already in place, piracy in India continues to grow at an alarming rate. Approximately 90 million users accessed pirated video content in 2024 alone, resulting in an estimated USD 1.2 billion in revenue loss, which is equivalent to around 10% of the legal video industry. If left unaddressed, this number is projected to grow to 158 million users by 2029, pushing cumulative losses up to USD 2.4 billion.

The following analysis explores the structural and operational shortfalls within existing legal mechanisms and examines where targeted interventions may be required.

# Current Legal Safeguards Against Piracy

|    | LEGISLATION / JUDICIAL MECHANISM   | OFFENCE / TARGETED ACTIVITY   | PUNISHMENT / REMEDY  |
|----|--|---|--|
| 1. | Section 51 and Section 63 of the Copyright Act, 1957   | Infringing or abetting the infringement of the copyright in a work.   | Imprisonment from 6 months to 3 years; fine ranging from INR 50,000 to INR 2,00,000.   |
| 2. | Section 63B of the Copyright Act, 1957   | Knowingly using a pirated copy. Aimed at the end user of the pirated product, and not the person who is responsible for creating an infringing copy.  | Imprisonment from 7 days to three years; fine ranging from INR 50,000 to INR 2,00,000.   |
| 3. | Section 65A of the Copyright Act, 1957   | Circumvention resulting in copyright infringement.  | Maximum imprisonment up to 2 years and fine.   |
| 4. | Section 65B of the Copyright Act, 1957   | Tampering with or removing Rights Management Information (RMI) from copyrighted content and distributing such content after altering or deleting RMI. | Maximum imprisonment up to 2 years and fine.   |
| 5. | Rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 | Hosting or transmitting content that infringes intellectual property rights, including copyright on intermediary platforms.                           | Internet service providers (ISPs) and other intermediaries are required to inform users not to host infringing content. Non-compliance with these obligations could strip intermediaries of their 'safe harbour' protection under Section 79 of the IT Act, rendering them liable for third-party content. |
| 6. | John Doe Orders  | Rampant infringement or unlawful exploitation such that it is practically impossible for a rights owner to identify all infringing parties.           | A court order that allows a copyright holder or rights owner to initiate legal action against unknown defendants.  |

|    |                               |  |   |
|----|-------------------------------|--|---|
| 7. | <b>Dynamic Injunctions</b>    | Mirror link, redirect, or alphanumeric variant of already taken down website.  | Rights-holders can approach the Joint Registrar of the High Court to extend an already granted injunction. The Court has vested powers to the Registry to issue such injunctions under Order 1 Rule 10 of the CPC to save the Plaintiff from the burdensome process of obtaining a judicial blocking order. |
| 8. | <b>Dynamic+ injunction</b>    | Repeated infringement or making public any content where copyright ownership is undisputed. This includes the future movies, shows, and more of the rights holder. | A dynamic+ injunction protects yet-to-be created content that is exclusively owned by the rights holder from piracy. This means a copyright holder does not need to come back to court for every new title that gets pirated by that specific infringer.  |
| 9. | <b>Superlative Injunction</b> | Live-streaming, whether through URLs or mobile apps.   | It is a limited-duration injunction, an enhanced form of dynamic+ injunction in order to tackle the unauthorised streaming causing real-time commercial loss.   |

# The Limits of Legal Remedies in Combating Digital Piracy

The recent report of IP House and Media Partners Asia launched at WAVES 2025 suggests that piracy is continually growing both in terms of volume and sophistication. This makes it essential to analyse deficiencies within the legal framework to understand why piracy persists. As seen above, most legal and technical interventions are triggered after infringement has already occurred. Whether it is a takedown under Rule 3(1)(b) of the Intermediary Guidelines or a domain block via an injunction, action typically follows a complaint or judicial order, making it a litigation-heavy framework. A fundamental issue here is that though platforms can keep removing infringing content, new versions reappear within hours, making legal enforcement into a 'game of catch-up' and not a preventative exercise. Therefore, remedies often result in temporary relief rather than a sustained deterrence.

Additionally, a litigation-heavy model may work for live shows and new releases, but it is hard to sustain. Rights holders must continuously monitor infringing websites and initiate legal requests, sometimes within days of the previous one. This makes enforcement difficult and expensive, especially for mid-sized platforms with limited capacity.

Even though the Copyright Act has stringent criminal provisions like Section 63 and 65B, these laws are not always enforced well. Therefore, enforcement mechanisms have also been put in place in each state. Several states have established dedicated copyright enforcement cells or cybercrime units within their crime branches. These specialised units are tasked not just with tackling digital piracy, but also other cybercrimes like fraud and hacking. Their decentralised structure allows for more localized and agile response, improving coordination with law enforcement and copyright holders.

However, the creation of these units remains inconsistent across India, and their effectiveness often depends on state-level prioritisation, resource allocation, and capacity-building. In many other regions, the absence of such infrastructure continues to leave piracy unchecked pointing towards a need for stronger inter-state coordination and institutional support at the central level. Moreover, according to official statistics from the National Crime Records Bureau, the annual number of criminal copyright cases filed in India is relatively low as a percentage when compared with overall offences, and the number of convictions even lower.

It would be inaccurate to suggest that the remedies currently in place ranging from injunctions and takedown provisions to criminal penalties serve no purpose. In many cases, they have offered immediate relief, particularly during high-stakes releases or targeted enforcement drives. However, the persistence and adaptability of piracy networks indicate that these tools, while well-intentioned, may not be structurally designed to address the full scale and evolving nature of the problem.

---

# Recommendations

---

## 1

---

**Developing inter-ministerial coordination:** As per the Government of India (Allocation of Business) Rules, 1961 policy matters relating to information technology, electronics, and internet, other than licensing of ISPs fall within the ambit of Ministry of Electronics and Information Technology (**MEITY**). The Department of Telecommunications (**DoT**) has in the past instructed ISPs for blocking of the websites as ordered by the Hon'ble Courts. However, ensuring compliance for each link hosted by an intermediary is a time-consuming and complex task especially in view of multiplicity of orders of Hon'ble Courts, and websites/links to be blocked. In case the web server happens to be in India, the copyright holder can inform the same to MEITY. In addition, the Ministry of Information and Broadcasting (**MIB**) has already appointed nodal officers to act on pirated films online. This indicates that enforcement still happens in silos. An inter-ministerial approach from MIB, MEITY, DPIIT, DoT, and state-level law enforcement can centralise piracy response mechanisms.

---

## 2

---

**Shift towards proactive detection:** Current anti-piracy measures rely heavily on taking action after infringing content is available. By that time, even blocked URLs there is a possibility that it can be mirrored or downloaded at scale, rendering enforcement efforts largely reactive. A proactive approach focuses on identifying and disabling piracy before it gains traction, thereby reducing both distribution and impact.

This may involve use of watermarking and content fingerprinting to recognize original works and flag piracy at its source across websites and apps. Additionally, the employment of advanced detection tools to detect new piracy channels by scanning for known signatures or metadata patterns may yield positive results.

---

## 3

---

**Incentivise co-regulation and industry coalitions:** Anti-piracy cannot rely solely on government action. OTT platforms, broadcasters, and digital intermediaries can be encouraged to form joint anti-piracy task forces to share threat intelligence, flag repeat offenders, and build interoperable reporting systems.



The Indian Governance And Policy Project (IGAP) is an emerging think tank focused on driving growth, innovation, and development in India's digital landscape. Specializing in areas like AI, Data Protection, FinTech, and Sustainability, IGAP promotes evidence-based policymaking through interdisciplinary research. By working closely with industry bodies in the digital sector, IGAP provides valuable insights and supports informed decision-making. Core work streams include policy monitoring, knowledge dissemination, capacity development, dialogue and collaboration.

---

For more details visit: [www.igap.in](http://www.igap.in)

[relations@igap.in](mailto:relations@igap.in) | [igap.in](http://igap.in)