

**INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES**
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to submission@ijlmh.com.

Digital Piracy and Intellectual Property Enforcement in the Age of Streaming

VARSHA RAMESHKUMAR*

ABSTRACT

The rise of streaming platforms has transformed how audiences access and consume digital content, offering convenient and legal alternatives to traditional media formats, yet digital piracy remains a persistent and evolving challenge. This paper examines the dynamics of digital piracy in the streaming era, exploring the factors that sustain it, including subscription fatigue, geo-restrictions and exclusive-content fragmentation, alongside increasingly sophisticated methods such as stream-ripping, illegal IPTV services and cloud-based sharing. It evaluates the effectiveness of current legal and technological enforcement mechanisms, including copyright laws, site-blocking, digital rights management and automated content monitoring, and situates these within a comparative and international framework spanning the United States, India, the European Union and China, together with the TRIPS Agreement and the WIPO Copyright Treaty. It finds that enforcement is frequently undermined by cross-border jurisdictional limits, anonymity tools and public indifference toward piracy, and that India's statutory framework in particular has not kept pace with streaming-based infringement. The paper argues for a comprehensive and adaptive approach that combines stronger international cooperation, platform accountability, public education and more affordable, user-friendly legal alternatives to safeguard intellectual property in the age of streaming.

Keywords: *Digital piracy, Streaming services, Intellectual property, Copyright infringement, Digital rights management, Illegal streaming, IP enforcement, Stream-ripping, Geo-restrictions, Anti-piracy measures.*

I. INTRODUCTION

The rapid growth of digital technology and the rise of streaming platforms have transformed the way people access and consume media. Services such as *Netflix*, *Spotify*, *YouTube* and *Amazon Prime* have made it easier than ever to enjoy films, music and television programmes legally and conveniently. Despite these advances, digital piracy remains a major global problem. Rather than disappearing, piracy has adapted to the digital age, with new methods such as illegal streaming sites, stream-ripping tools and unauthorised IPTV services becoming widespread.

* Author is a student at STM University, India.

This ongoing problem poses serious challenges to the enforcement of intellectual property (IP) rights and threatens the revenue and sustainability of the creative industries. As content becomes more digital and globally distributed, finding effective ways to protect intellectual property while maintaining user accessibility is more important than ever.

The primary objective of this paper is to provide a comprehensive analysis of digital piracy in the context of the rapidly growing streaming industry. This includes understanding how piracy has evolved with advances in technology and shifts in consumer behaviour, particularly with respect to modern methods such as illegal streaming platforms, stream-ripping and unauthorised IPTV services. The paper evaluates the current intellectual property enforcement mechanisms, both legal and technological, used by governments, content creators and streaming platforms to combat piracy. It also identifies the major challenges these stakeholders face, including jurisdictional limitations, technological barriers and user attitudes toward piracy. Finally, it proposes multi-dimensional strategies that seek to balance the protection of intellectual property rights with the provision of accessible, affordable and user-friendly legal alternatives, thereby supporting the sustainability of the creative industries in the digital era.

This paper focuses on digital piracy relating to streaming content such as films, television programmes, music and live broadcasts. It covers the various forms of piracy prevalent today, including illegal streaming sites, stream-ripping and unauthorised IPTV services. Its scope includes an examination of intellectual property enforcement methods, such as legal frameworks, digital rights management (DRM) and platform-based monitoring systems. It also considers the roles of content creators, streaming services, internet service providers and governments in combating piracy. While it acknowledges global differences in enforcement and regulation, the focus is primarily on trends and challenges relevant to major markets with significant streaming activity. The paper does not examine piracy of software or video games in depth, nor does it cover offline piracy in detail.

II. UNDERSTANDING DIGITAL PIRACY IN STREAMING

A. Digital piracy in the context of streaming platforms

Digital piracy refers to the unauthorised use, reproduction or distribution of copyrighted content. In the context of streaming platforms, it specifically involves illegal activities relating to the consumption and sharing of digital media such as films, television programmes, music and live broadcasts. With the rise of streaming services, piracy has taken on new forms that exploit the technology behind digital content delivery.

Illegal streaming websites and apps. These are platforms that offer access to copyrighted content without obtaining proper licensing or permission from rights holders. Unlike legitimate services such as *Netflix* or *Spotify*, these sites do not pay royalties or subscription fees to creators. They may provide free or low-cost access to a vast library of media, often funded through advertising or subscriptions, which directly violates intellectual property rights. Examples include unauthorised streaming portals and apps that aggregate pirated content.

Stream-ripping. Stream-ripping involves downloading or extracting audio or video files from legitimate streaming services. For instance, users might rely on third-party software to save songs from *Spotify* or videos from *YouTube* as offline files. These ripped files can then be shared, uploaded or redistributed without permission. This practice bypasses the intended streaming-only use, undermining content creators' ability to control distribution and generate revenue.

Unauthorised IPTV services. Internet Protocol Television (IPTV) delivers television content over the internet. While many legitimate IPTV providers exist, some offer unauthorised access to live channels or on-demand content without paying for licences. These illegal IPTV services often sell subscriptions at a fraction of the cost of legitimate providers, attracting users seeking cheaper alternatives. They distribute copyrighted content on a large scale, making enforcement difficult because of the global and decentralised nature of these services.

Rebroadcasting and simulcasting pirated streams. Some piracy operations capture legitimate streams, for example of live sports or exclusive premieres, and rebroadcast them illegally through websites or social media platforms. This form of piracy can generate significant revenue through advertising or subscriptions while depriving rights holders of their income.

Circumvention of geo-restrictions. Although not piracy in itself, many users employ virtual private networks (VPNs) or proxy servers to bypass geographical restrictions on streaming platforms. This often results in access to content that is not licensed for the user's region, which indirectly supports piracy ecosystems that redistribute restricted content.

Content aggregation and indexing. Certain websites do not host pirated content directly but provide indexes or links to illegal streams hosted elsewhere. These aggregators facilitate piracy by making it easier for users to find unauthorised content.

B. Evolution of piracy with the rise of OTT platforms

The rise of over-the-top (OTT) platforms has dramatically transformed how people consume media, offering convenient legal access but also inadvertently shaping the evolution of digital piracy. Pirates have shifted from copying physical media to sophisticated digital methods such

as illegal streaming, stream-ripping, unauthorised IPTV services and content aggregation. Factors such as content fragmentation, geo-restrictions and subscription costs have further fuelled piracy by pushing some consumers toward illegal alternatives. Meanwhile, piracy networks have embraced new technologies to evade enforcement, making intellectual property protection in the OTT era a complex and ongoing challenge.¹

From physical copies to digital streams. Before the digital streaming era, piracy mainly involved physical formats such as DVDs, CDs and VHS tapes, which were copied and distributed illegally. The introduction and rapid growth of OTT platforms shifted media consumption to digital streaming. This transition changed piracy from physical copying to the unauthorised online access, download and redistribution of digital content. The intangible nature of streaming content made piracy easier to commit and harder to control globally.

Proliferation of illegal streaming websites and apps. OTT platforms host large libraries of high-quality, exclusive content behind paywalls. Pirates responded by creating illegal streaming websites and mobile apps that host or link to this content for free or at very low cost. These pirate sites often mimic legitimate OTT platforms, offering user-friendly interfaces and vast content selections that attract users unwilling or unable to pay for multiple subscriptions. For example, sites such as *Putlocker* and unauthorised apps have provided access to streaming originals and other exclusive shows.

Stream-ripping from legitimate OTT sources. Technological tools have evolved to allow users to rip or download content directly from streaming services. Although OTT platforms intend content to be viewed only by streaming, stream-ripping software enables users to capture video or audio streams and save copies offline. This content can then be redistributed without authorisation, undermining subscription-based revenue models.²

Rise of unauthorised IPTV and live streaming services. Many OTT platforms also offer live streaming of events such as sports and premieres. Piracy has evolved to include unauthorised IPTV services that rebroadcast live channels or streaming content illegally. These services often sell subscriptions at a fraction of the cost of legal providers, gaining popularity among users seeking live access to premium content without paying. They frequently use complex networks of servers and encryption to avoid detection, making enforcement difficult.

Fragmented content rights and subscription fatigue. OTT platforms typically acquire exclusive rights to different content, leading to fragmentation in which popular shows and films

¹ Jane C. Ginsburg, *The Right to Claim Authorship in U.S. Copyright and Trademarks Law*, 41 HOUS. L. REV. 263 (2004).

² Joseph P. Liu, *Copyright Law's Theory of the Consumer*, 44 B.C. L. REV. 397 (2003).

are spread across multiple services. Consumers who want access to all their favourite content face the high cost of subscribing to many platforms. This subscription fatigue has driven some users to piracy as a cheaper alternative, seeking all-in-one access through illegal means rather than multiple paid subscriptions.

Geo-restrictions and regional licensing. Because of licensing agreements, OTT platforms often restrict content by geographic region, so that users in some countries cannot access certain shows or films legally. This drives demand for pirated versions that bypass such geo-blocks. Pirates exploit this by redistributing region-locked content worldwide, sometimes with the help of VPNs and proxy services that conceal users' locations and help them circumvent restrictions.

Aggregation and indexing of pirated content. Piracy has become more organised through websites and apps that aggregate links to pirated OTT content across multiple sources. Instead of searching several illegal sites, users can access a centralised directory of pirated films, series and live streams. This aggregation improves accessibility and user experience for pirates and helps drive traffic to pirate platforms.

Sharing on social media and peer-to-peer networks. Pirated OTT content is increasingly distributed through social media platforms, messaging apps and peer-to-peer networks. These decentralised and often encrypted channels allow rapid sharing of clips, episodes and even full-length content, sometimes before or shortly after official release dates. The scale and speed of this distribution make detection and takedown efforts more complex.

Use of technology to evade enforcement. Pirates continually adopt new technologies to avoid detection and takedown, such as encrypted communications, decentralised file sharing and blockchain-based hosting. They also frequently change domain names and hosting locations and employ proxy servers to keep pirate sites operational despite legal action.

C. Technologies used by pirates to bypass legal streaming protections

Pirates employ a variety of sophisticated technologies to bypass the protections that OTT streaming platforms implement. Stream-ripping tools allow unauthorised downloading, while VPNs and proxies help bypass geographic and network restrictions. Peer-to-peer networks distribute pirated files in a decentralised way, complicating enforcement. Custom apps, browser extensions and illegal IPTV services exploit vulnerabilities in streaming protocols and DRM systems. Emerging decentralised and encryption technologies further increase piracy's resilience and pose ongoing challenges for content protection. This constant technological arms race demands innovative and adaptive countermeasures from the industry and regulators.

Stream-ripping software and tools. Stream-ripping tools are programs or online services that allow users to download or capture video and audio content from streaming platforms. These tools work by intercepting the data stream as it plays and saving it in a usable file format such as MP4 or MP3. This bypasses the streaming-only access that OTT platforms intend, enabling offline viewing and redistribution without authorisation. Some popular stream-ripping tools target *YouTube*, *Spotify* or even premium OTT services, allowing pirates to build large libraries of pirated content.

Virtual private networks and proxy servers. VPNs and proxies mask a user's real IP address by routing internet traffic through servers in different geographic locations. This technology helps users bypass the geo-restrictions that OTT platforms impose because of regional licensing agreements. For instance, a user in a country where a show is unavailable can connect through a VPN server in a country where it is available, gaining access illegally. VPNs also help users avoid network-level blocks that target pirate sites or streaming services. Proxies offer similar functions but are typically less secure.

Peer-to-peer networks and torrents. Peer-to-peer file-sharing networks, such as *BitTorrent*, enable the decentralised sharing of large media files among users. Pirates distribute ripped or recorded content through torrents or magnet links, allowing anyone to download pieces of a file from multiple sources simultaneously. Because there is no central server hosting the files, enforcement agencies find it harder to track or shut down piracy at the source.

Scraping and crawling bots. Automated bots scrape streaming platforms to extract URLs, metadata or even content itself. These bots mimic human browsing behaviour to avoid detection while gathering large amounts of data quickly. Pirates use scraped URLs to create unauthorised streaming links or to populate illegal streaming sites. Crawling bots can also monitor legal content releases so that pirated copies are made available soon after launch.

Custom streaming apps and modified clients. Pirates develop unauthorised applications or modify official streaming clients to remove or bypass DRM protections. These apps may allow users to access premium content for free or to circumvent content restrictions. They often bundle content from multiple pirate sources, making it easier for users to find and watch pirated material on devices such as smartphones, tablets and smart televisions.

Browser extensions and downloaders. Certain browser extensions or standalone downloader software intercept streaming data in real time, saving videos locally on users' devices. These tools exploit weaknesses in browser security or in streaming protocols, including HTTP Live Streaming (HLS) and Dynamic Adaptive Streaming over HTTP (DASH), to capture protected

content. Because these extensions operate on the user's device, they can be difficult for platforms to detect and block effectively.

Illegal IPTV services and encrypted streaming servers. Unauthorised IPTV services stream live channels and on-demand content over the internet without proper licences. These services often use encrypted streaming protocols to prevent interception and avoid detection. They also employ proxy servers, frequently change domains and use content-delivery techniques to stay online despite legal efforts to shut them down.

Content delivery network abuse. Pirates sometimes exploit legitimate content delivery networks (CDNs) to distribute pirated content, taking advantage of the fast, reliable delivery and trusted reputation of these networks. By hosting pirated files on CDNs, they mask the true origin of the content, making it more challenging for authorities to identify and block pirate servers.

Decentralised technologies and blockchain. Emerging technologies such as blockchain and decentralised peer-to-peer streaming protocols offer pirates new ways to distribute content without a central server or authority. These decentralised systems make it difficult to remove pirated content because there is no single point of control. Content is stored and shared across many nodes globally, increasing resilience against enforcement.

Encryption, obfuscation and steganography. Pirates use encryption and obfuscation to hide the nature or location of pirated content. This includes encrypting files, scrambling metadata, renaming files with misleading names and even embedding content within other files using steganography. These methods help pirates avoid automated detection tools and make it harder for platforms to identify infringing content.

III. IMPACT OF STREAMING ON TRADITIONAL IP ENFORCEMENT

The shift from physical media, such as CDs, DVDs and Blu-ray discs, to streaming has significantly transformed the enforcement mechanisms for intellectual property rights and content distribution.³ The principal changes are set out below.

Transformation of piracy models. In the era of physical media, piracy centred on the illegal reproduction and sale of tangible goods such as DVDs, CDs and Blu-ray discs. Enforcement focused on seizing counterfeit goods, conducting raids on black markets, intercepting shipments and arresting those involved in manufacturing and distributing pirated content. With the rise of digital streaming platforms such as *Netflix*, *Amazon Prime* and *Disney+*, however, piracy has

³ Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. § 512).

moved online. It now involves illegal live streaming, torrent sharing, IPTV services and digital downloads, making it borderless, more anonymous and harder to track.

Shift in enforcement tactics. The transition to streaming has necessitated a change in enforcement methods. Instead of relying solely on physical raids or customs interventions, authorities now use digital enforcement tools. These include automated takedown notices under DMCA procedures, AI-powered content-detection systems and cyber forensics to trace digital footprints. Law enforcement also collaborates with anti-piracy firms to monitor, identify and remove pirated content from the web in real time.

Rise of DRM and technical countermeasures. Streaming platforms use digital rights management technologies such as Google Widevine, Apple FairPlay and Microsoft PlayReady to protect their content from unauthorised use. These technologies encrypt digital content and restrict access to authorised devices and users. Pirates nonetheless often bypass DRM using stream-ripping tools, modified apps or screen-capture software. As a countermeasure, companies integrate watermarking and content fingerprinting to track leaks and trace the origin of pirated files.

Collaboration with ISPs and governments. Another significant development is the collaboration between OTT platforms, governments and internet service providers (ISPs). Courts in countries such as India, the United Kingdom and Australia allow rights holders to obtain site-blocking orders enabling ISPs to restrict access to known piracy sites. In addition, domain seizures and the blacklisting of piracy-related URLs help prevent users from accessing illegal content. These legal tools are particularly effective in minimising large-scale public access to pirated material.

Role of private anti-piracy firms. Streaming platforms now depend heavily on third-party companies such as Irdeto, MUSO and MarkMonitor for enforcement. These firms offer services such as round-the-clock monitoring, piracy intelligence and takedown automation. They use web crawlers, bot detection and even dark-web monitoring to track where and how pirated content is being distributed, and they act quickly to issue legal or automated takedown notices.

Public education and deterrence. In addition to enforcement, streaming services and governments have recognised the importance of public education in combating piracy. Campaigns warning users about the risks of malware, data theft and the legal consequences of using pirated content are now common. These efforts aim to reduce demand by encouraging responsible digital behaviour and supporting affordable legal alternatives.

Ongoing challenges in enforcement. Despite significant progress, modern enforcement still faces challenges. Pirates often use VPNs and anonymous hosting to evade detection. Jurisdictional issues arise when piracy websites operate in countries with weak IP laws. Decentralised technologies such as torrents and blockchain also make it difficult to identify and shut down operators. Moreover, leaked content can go viral within minutes, making rapid enforcement both crucial and difficult.

A. Challenges in enforcing copyright online

Anonymity and identity masking. Online pirates often operate behind layers of anonymity using VPNs, proxy servers and false domain registrations. These tools hide their physical locations and identities, making it extremely difficult for copyright holders to identify or prosecute them. Even if a pirated stream or download is traced to a source, the responsible party may remain unreachable or legally protected in their own jurisdiction.

Jurisdictional and legal limitations. One of the most significant hurdles in online enforcement is the international nature of the internet. Pirated content is often uploaded in one country, hosted in another and accessed globally. This creates a legal maze in which copyright holders must navigate different laws, enforcement practices and levels of cooperation. Countries with weak intellectual property enforcement or without extradition treaties can become safe havens for piracy operations.⁴

Speed and scale of piracy. Piracy today occurs at a much faster pace than traditional enforcement can handle. New content is often pirated within minutes of its release, especially high-profile films or series. Pirates use stream-ripping tools or screen recording to distribute content immediately across multiple platforms, giving enforcement teams very little time to respond before the content has spread widely.

Proliferation of mirror and clone sites. When one piracy website is taken down, others quickly appear in its place. These clone or mirror sites copy the original site's content and branding, making it hard for users to distinguish them and for copyright holders to keep up. This endless cycle of takedown and re-emergence makes enforcement resemble a digital game of whack-a-mole.

Technological sophistication of pirates. Modern piracy is technologically advanced. Pirates now use sophisticated software to bypass DRM, remove watermarks and access encrypted content. They also engage in credential theft and API abuse to illegally stream premium content.

⁴ Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement*, 89 OR. L. REV. 81 (2010).

This forces copyright owners to invest heavily in constantly evolving technological countermeasures, making enforcement both complex and costly.

Cost and resource constraints. Effective copyright enforcement requires substantial financial and technical resources. Independent creators and smaller studios often cannot afford ongoing surveillance, legal teams or subscriptions to anti-piracy monitoring services. Even large companies face high operational costs to detect, report and legally pursue violations across global jurisdictions.

Limitations of takedown processes. Platforms such as *YouTube*, *Facebook* and file-sharing sites offer takedown mechanisms such as DMCA notices, but these are typically reactive. Pirates often re-upload the same content repeatedly, forcing creators to submit repeated claims. Automated filters are not always effective, and enforcement lags behind content distribution, reducing the impact of takedown efforts.

Infringement on private and encrypted platforms. Piracy is not limited to public platforms. Encrypted messaging apps such as *Telegram*, *WhatsApp* and *Discord* are now popular for sharing full films, shows and music files within private groups. These channels are harder to monitor because of end-to-end encryption and their lack of public visibility, limiting copyright owners' ability to detect or act against infringement.

Delays or non-cooperation by platforms. Not all platforms respond promptly, or at all, to copyright complaints. Some delay action until formally compelled by a court order, while others are hosted in jurisdictions that do not recognise foreign takedown notices. This lack of timely cooperation allows pirated content to remain accessible long enough to reach a large audience.

Public attitudes and demand for free content. A cultural challenge also exists: many users do not perceive piracy as a serious offence. Especially in regions where content is expensive or not easily accessible, people justify piracy as necessary or harmless. This perception encourages demand for pirated material, making it harder for creators to compete with free illegal versions of their work.⁵

IV. LEGAL AND TECHNOLOGICAL MEASURES FOR IP ENFORCEMENT

A. Effectiveness of legal tools

DMCA takedown notices. The DMCA takedown process is one of the most commonly used legal tools, especially in the United States, to combat online copyright infringement. Rights holders identify infringing content and send formal notices to hosting platforms, compelling

⁵ William F. Patry, PATRY ON COPYRIGHT (Thomson Reuters 2024).

them to remove the content in order to maintain safe-harbour protection. This system is effective in quickly removing large volumes of unauthorised material from platforms such as *YouTube* and social media sites. However, the process is inherently reactive and requires constant monitoring, as infringing content often resurfaces shortly after removal. Platforms may also face an overwhelming volume of takedown requests, which can delay enforcement or result in incomplete removals. The DMCA does not require platforms to prevent re-uploads proactively, which limits its deterrent effect.⁶

Dynamic injunctions. Dynamic injunctions provide a more proactive and flexible remedy than DMCA takedowns. Courts can issue orders that allow rights holders to block not only existing infringing URLs or domains but also future mirror sites or clones that emerge to circumvent takedowns. This approach has proven effective in jurisdictions such as the United Kingdom and parts of Europe, significantly reducing access to major piracy websites. Its effectiveness nonetheless depends heavily on the cooperation of ISPs and legal systems within particular jurisdictions. Pirates often bypass these injunctions using VPNs or by relocating servers to countries with weaker enforcement, which limits their overall impact.⁷

Site-blocking orders. Site-blocking orders require ISPs to restrict user access to entire piracy websites, typically at the domain or IP-address level. These orders have been successful in reducing casual piracy by making it more difficult for average users to access unauthorised streaming platforms. Countries such as Australia and the United Kingdom have seen measurable decreases in piracy traffic following the implementation of site blocking. Despite their benefits, such orders can be circumvented by technically adept users through VPNs or proxy services. Piracy sites also often respond by creating mirror or clone domains, necessitating continual enforcement. Jurisdictional limitations further mean that site-blocking orders protect only users within certain regions, while users elsewhere can still access pirated content freely.⁸

Overall assessment. While DMCA takedowns, dynamic injunctions and site-blocking orders each contribute important tools to the fight against digital piracy, none is wholly sufficient on its own. The reactive nature of takedowns, jurisdictional fragmentation, technical circumvention methods and the vast scale of online piracy reduce their long-term effectiveness. These legal tools are most effective when combined with technological measures such as content-recognition software, digital rights management, international cooperation and public-education

⁶ Niva Elkin-Koren, *It's All About Control: Rethinking Copyright in the New Information Landscape*, in THE COMMODIFICATION OF INFORMATION 79 (Niva Elkin-Koren & Neil Weinstock Netanel eds., Kluwer Law Int'l 2002).

⁷ Peter K. Yu, *The Copyright Divide*, 25 CARDOZO L. REV. 331 (2003).

⁸ Talat Fatima, CYBER CRIMES (3d ed., Eastern Book Co. 2021).

campaigns to reduce demand. Together, they form a multi-layered defence that can mitigate piracy's impact in the fast-evolving streaming landscape.

B. Role of watermarking, fingerprinting and DRM in enforcement

Together, watermarking, fingerprinting and DRM form a multi-layered technological defence against digital piracy. Watermarking provides traceability and legal evidence, fingerprinting enables automated detection and rapid enforcement, and DRM restricts content access to authorised users only. While none of these technologies alone can eliminate piracy, their combined use strengthens enforcement by making piracy more traceable, detectable and technically challenging. These tools complement legal and policy measures to protect intellectual property rights in the increasingly digital, streaming-focused content landscape.

Watermarking. Watermarking embeds invisible or visible identifiers directly into digital content such as video or audio streams. These identifiers can be unique to each copy or user, allowing rights holders to trace the source of leaked or pirated material. In enforcement, watermarking acts as a forensic tool, helping to identify where and how content was illegally redistributed. This can be critical in legal cases, as it provides evidence linking piracy back to a particular user, device or distribution channel. Watermarking also serves as a deterrent, since users aware of traceable watermarks may be less likely to share or leak content illegally.

Fingerprinting. Fingerprinting is a content-recognition technology that creates a unique digital signature or pattern based on the audio or visual characteristics of a piece of content. Unlike watermarking, it does not require embedding additional data; instead, it analyses the content itself to detect matches. This technology is widely used by platforms such as *YouTube's* Content ID system to identify copyrighted material in user uploads automatically. Fingerprinting enables rapid, automated detection of unauthorised content, facilitating faster enforcement through automated takedowns or blocking. It is especially useful for monitoring vast amounts of content across multiple platforms and for identifying pirated streams even when the files have been altered slightly.

Digital rights management. DRM refers to a suite of technologies designed to control access to and use of digital content. DRM systems encrypt streaming content and require authorised decryption keys, which are typically provided only to legitimate users or devices. This prevents unauthorised copying, redistribution or playback on unapproved devices. In enforcement, DRM acts as a preventive barrier by restricting how content can be accessed or shared, making piracy technically more difficult. DRM also supports licensing models that enable content providers to monetise their works securely. DRM is not foolproof, however; determined pirates often

develop methods to bypass its protections, yet DRM significantly raises the cost and complexity of unauthorised distribution.⁹

C. The role of AI and blockchain in enhancing copyright protection

AI for automated detection and enforcement. Artificial intelligence (AI) plays a transformative role in monitoring and enforcing copyright on streaming platforms. Through machine-learning algorithms, AI can automatically scan and analyse large volumes of content to detect unauthorised use. Technologies such as content fingerprinting and pattern recognition allow AI to identify pirated material even when it has been slightly altered, for instance by changing resolution, cropping or adding filters. AI systems can also generate real-time alerts during live streaming events to detect and disrupt illegal broadcasts. In addition, AI-powered tools assist in managing DMCA takedown requests, making the enforcement process faster and more accurate. Over time, AI systems improve through exposure to new types of infringement, helping platforms adapt to evolving piracy tactics.¹⁰

Blockchain for rights management and transparency. Blockchain technology offers a decentralised and tamper-proof way to manage copyright ownership, licensing and transaction records. By storing copyright data and content licences on a blockchain, creators and distributors can create a transparent, immutable ledger of who owns what and under what conditions content may be used. This helps reduce disputes over ownership and usage rights. Smart contracts, which are automated agreements stored on the blockchain, can facilitate real-time royalty payments to rights holders whenever their content is streamed or used. This is particularly useful in environments with multiple stakeholders, such as the film and music industries, where revenue-sharing is complex.

Combating piracy through traceability and accountability. Blockchain can also enhance anti-piracy efforts by enabling the traceability of digital content. Each piece of licensed content can be assigned a unique identifier recorded on the blockchain. When paired with digital watermarking, this makes it easier to track the origin of leaks and take appropriate legal action. If content is found on unauthorised platforms, blockchain records can help verify its legitimate source and usage conditions, strengthening copyright enforcement in court.

Challenges and considerations. While AI and blockchain hold great promise, they also have limitations. AI systems can be expensive to develop and may produce false positives or miss

⁹ Julie E. Cohen, Lydia Pallas Loren, Ruth L. Okediji & Maureen A. O'Rourke, COPYRIGHT IN A GLOBAL INFORMATION ECONOMY (4th ed., Wolters Kluwer 2015).

¹⁰ Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (SSRN Working Paper No. 2580664, Mar. 10, 2015).

cleverly disguised infringements. Blockchain adoption is still limited by scalability issues, a lack of standardisation and the need for broad industry cooperation. Smart contracts also require careful programming to reflect complex licensing terms. Despite these challenges, both technologies offer long-term solutions to improve the efficiency, accuracy and trustworthiness of digital rights management.¹¹

V. INTERNATIONAL AND COMPARATIVE LAW DIMENSIONS

A. Comparative enforcement of IPR in digital streaming

United States: comprehensive legal framework and technologically capable enforcement.

The United States offers one of the most robust legal systems for enforcing intellectual property rights in the digital streaming domain. The cornerstone of United States copyright law is the Copyright Act of 1976, supplemented by the Digital Millennium Copyright Act (DMCA) of 1998. The DMCA introduced critical tools such as the notice-and-takedown mechanism, which allows rights holders to request the swift removal of infringing content by online service providers. It also includes anti-circumvention provisions to combat the tampering with DRM technologies. United States courts are generally friendly to rights holders, and both civil and criminal penalties, sometimes amounting to hundreds of thousands of dollars per infringement, can be pursued. Federal agencies such as the FBI and Immigration and Customs Enforcement are involved in cracking down on piracy rings, and major streaming services work closely with law enforcement. Despite the strength of its legal toolkit, the United States still faces challenges from offshore servers, anonymous networks and the rise of encrypted sharing tools such as VPNs and torrent platforms.¹²

India: judicial creativity amid infrastructural challenges. India enforces copyright through the Copyright Act, 1957, last amended in 2012. While this law provides general protection for intellectual property rights, it does not specifically address digital streaming, leaving gaps that the courts have attempted to fill. The Indian judiciary, particularly the Delhi High Court, has developed distinctive remedies such as John Doe orders, also called Ashok Kumar orders, to pre-emptively block unknown pirates and websites before content is even released. Dynamic injunctions further empower courts to extend existing orders to mirror or clone sites without fresh proceedings. These innovations are widely used to protect high-value content such as Bollywood films and cricket broadcasts. However, enforcement remains hampered by poor ISP

¹¹ W. Michael Schuster, *Fair Use, Girl Talk, and Digital Sampling: An Empirical Study of Music Sampling's Effect on the Market for Copyrighted Works*, 67 OKLA. L. REV. 443 (2015).

¹² Daniel J. Gervais, *The TRIPS Agreement and the Doha Round: History and Impact on Development*, in 4 INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE 23 (Peter K. Yu ed., 2007).

compliance, delays in litigation and the limited technological capabilities of enforcement agencies. As a result, although India's judiciary is adaptive, its enforcement remains reactive rather than preventive or systemic.

European Union: harmonised legislation with an emphasis on platform accountability.

The European Union employs a harmonised legal approach to enforcement, combining Union-wide directives and national implementations. Core legislation includes the InfoSoc Directive (2001), the Enforcement Directive (2004) and the Digital Services Act (2022). These collectively address the rights of authors in the digital space, establish remedies for infringement and impose compliance obligations on platforms and intermediaries. Member states frequently use site-blocking injunctions issued by courts, compelling ISPs to restrict access to infringing websites. The Court of Justice of the European Union (CJEU) has played a central role in balancing enforcement with digital freedoms, delivering landmark rulings on the limits and duties of intermediaries. Enforcement levels nonetheless differ across member states because of varying judicial capacity, language barriers and procedural delays. While the European Union is progressive in adopting laws that recognise the complexities of streaming piracy, implementation often lacks speed and consistency.

China: centralised enforcement with selective transparency. China's approach is distinct because of its state-led, centrally controlled model. The Copyright Law of the People's Republic of China, revised in 2020, grants strong legal rights to creators and includes digital provisions. Enforcement is carried out through both judicial channels, such as specialised intellectual property courts in cities such as Beijing and Guangzhou, and administrative authorities such as the National Copyright Administration and the Cyberspace Administration of China. China frequently launches high-profile campaigns, such as Sword Net, targeting illegal content on streaming platforms, websites and mobile apps. Despite these efforts, many foreign rights holders face difficulties owing to regulatory opacity, local protectionism and censorship controls. Piracy thrives on third-party mobile apps, illegal set-top boxes and peer-to-peer networks. While legal tools exist, enforcement is often uneven, and domestic companies may receive more lenient treatment, leading to distrust among global stakeholders.

B. The role of international treaties in regulating streaming-related piracy

In the global digital era, the enforcement of intellectual property rights across borders has become increasingly important because online piracy often transcends national jurisdictions. International treaties such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the WIPO Copyright Treaty (WCT) provide foundational standards and

obligations for protecting copyright in all member states. Although these treaties were not designed specifically for modern streaming platforms, they have become critical in framing how nations legally approach streaming-related piracy.¹³

TRIPS Agreement. The Agreement on Trade-Related Aspects of Intellectual Property Rights is one of the most comprehensive international treaties on intellectual property, enforced under the World Trade Organization (WTO). Concluded in 1994, TRIPS sets minimum standards that all WTO member countries must follow to protect and enforce intellectual property rights, including copyright. Even though TRIPS was established before digital streaming became popular, its provisions are technology-neutral, meaning that they are broad enough to apply to both traditional and digital forms of content delivery.¹⁴

Coverage of copyright in TRIPS. TRIPS recognises copyright as one of the key forms of intellectual property and mandates protection for literary and artistic works, which include films, music, software and video content, and for the rights of authors to control the reproduction, distribution and public performance or communication of their works. In the context of streaming, this is critical because unauthorised digital broadcasting or sharing of copyrighted content, such as a film or a show on a pirated website, violates the copyright holder's exclusive right to communicate the work to the public.

Enforcement provisions. One of TRIPS' most important contributions is that it includes detailed enforcement mechanisms that countries must adopt in their national laws. These include civil remedies, under which rights holders can seek injunctions, damages and orders to destroy infringing goods; border measures, under which customs authorities can act to block the import or export of pirated content or illegal streaming devices; and criminal penalties, under which, for cases involving wilful piracy on a commercial scale, TRIPS requires countries to implement criminal laws, including fines and imprisonment. These tools can be used to combat piracy of streaming content, such as illegal streaming boxes, unlicensed IPTV services and pirated film distribution networks.

Technology-neutral language. Although TRIPS does not specifically mention streaming, it is written so that its principles can be applied flexibly to new technologies. The language focuses on the acts of reproduction and public communication rather than on the medium or platform.

¹³ Graeme B. Dinwoodie et al., INTERNATIONAL INTELLECTUAL PROPERTY LAW AND POLICY (2d ed., LexisNexis 2008).

¹⁴ Agreement on Trade-Related Aspects of Intellectual Property Rights art. 9-14, 41-61, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

This means that streaming content without authorisation falls under the same legal violations as copying and distributing DVDs or CDs.

Dispute resolution. TRIPS provides a mechanism for countries to file disputes against one another before the WTO Dispute Settlement Body if they believe that a member is not complying with its intellectual property obligations. This adds a layer of accountability, encouraging better enforcement and legal reform worldwide.

WIPO Copyright Treaty: digital-era protections. The WIPO Copyright Treaty, adopted in 1996 under the World Intellectual Property Organization, was one of the first international agreements specifically created to address the challenges that digital technology poses to copyright protection. Unlike the TRIPS Agreement, which is more general, the WCT focuses on authors' rights in the digital environment. It was developed as a special agreement under the Berne Convention and is legally binding on its signatories. This treaty plays a crucial role in tackling streaming-related piracy, as it deals directly with the unauthorised use and distribution of content over digital networks.¹⁵

Recognition of digital transmission rights. One of the WCT's most important features is its recognition of the right of communication to the public, which includes making works available over interactive digital platforms. This means that any unauthorised uploading, streaming or sharing of protected content such as films, music or television programmes violates the exclusive rights of the author. This principle is fundamental in the streaming era, where platforms such as *Netflix*, *Amazon Prime* and *Disney+* rely on legal licences to distribute content online. The WCT makes it clear that these digital forms of distribution require permission from the copyright holder, which forms the legal basis for taking down pirated streams.

Protection of technological protection measures. The WCT also obliges member countries to protect technological protection measures (TPMs), such as digital rights management, encryption and access controls, in law. These are the technical tools that streaming platforms use to prevent copying or unauthorised access to content. For example, when a user tries to record or redistribute a film from a paid streaming platform, DRM systems block the attempt. Under the WCT, circumventing such technologies is itself a legal violation, even where no actual copying occurs, which is important for stopping the hacking tools and illegal IPTV software used by pirates.

Protection of rights management information. Another important WCT requirement is the protection of rights management information (RMI). RMI includes digital data such as

¹⁵ WIPO Copyright Treaty, Dec. 20, 1996, S. Treaty Doc. No. 105-17, 36 I.L.M. 65 (1997).

watermarks, metadata and author information embedded in content. These markers help track the origin of pirated content and prove ownership. Under the treaty, it is illegal to remove or alter RMI for the purpose of piracy. This provision supports content owners and platforms in monitoring where their content is being misused and in enforcing their rights effectively.

Influence on national laws. The WCT has had a significant impact on copyright law reform globally. For instance, the United States Digital Millennium Copyright Act includes provisions that outlaw the circumvention of DRM and protect RMI, directly in line with the WCT; the European Union's InfoSoc Directive integrates WCT rules into European law, requiring platforms to remove infringing content and protect digital rights; and India's 2012 copyright amendment introduced provisions for anti-circumvention and digital licensing, aiming to align its law with WCT standards. These reforms have helped create a more consistent global framework to combat piracy across borders and hold violators accountable, especially in the context of digital and streaming content.

Limitations and ongoing challenges. While the WCT is progressive, it still faces limitations. It does not provide enforcement mechanisms itself; it depends on member countries to implement and enforce its provisions. Many developing countries struggle to implement strong anti-piracy infrastructure because of limited resources or a lack of political will. The treaty also does not fully account for newer technologies such as decentralised streaming, illegal mirror sites and torrent-based streaming platforms, requiring continued updates and interpretation.

C. National implementation influenced by treaties

International treaties such as the TRIPS Agreement and the WIPO Copyright Treaty establish broad standards for copyright protection and enforcement, but their real impact depends largely on how individual countries implement these obligations within their national legal systems. This process of national implementation is crucial for regulating digital streaming and combating piracy, as it translates treaty principles into practical laws, regulations and enforcement mechanisms tailored to each country's legal, economic and technological context.

United States. The United States has been a pioneer in implementing treaty obligations, particularly through the Digital Millennium Copyright Act of 1998. The DMCA incorporates the WCT's anti-circumvention provisions by making it illegal to bypass DRM and other technological protection measures; establishes the notice-and-takedown system, allowing copyright holders to request the removal of infringing content on online platforms; protects rights management information by prohibiting the alteration or removal of digital rights data; and enables strong civil and criminal enforcement against digital piracy. The DMCA has

become a global model, influencing copyright enforcement worldwide, especially in relation to streaming platforms and digital piracy.

European Union. The European Union has integrated treaty standards into its regional legal framework through directives such as the InfoSoc Directive (2001) and the more recent Digital Services Act (2022). The InfoSoc Directive enforces copyright protections aligned with TRIPS and the WCT, including exclusive rights over digital transmission and anti-circumvention measures. The Digital Services Act places responsibilities on online intermediaries and platforms to monitor and remove pirated content, improving enforcement in the age of streaming and user-generated content. The European Union's collective licensing schemes and statutory exceptions also reflect efforts to balance enforcement with user rights. These laws collectively strengthen copyright enforcement and provide a harmonised system across member states to tackle streaming piracy.

India. India's Copyright (Amendment) Act, 2012, was a significant step toward compliance with international treaty obligations. It introduced provisions specifically targeting digital rights management and anti-circumvention; established legal frameworks for statutory licensing, helping legitimise digital distribution; and expanded enforcement mechanisms to cover online piracy and unauthorised streaming. Challenges nonetheless remain because of limited enforcement capacity, digital-literacy gaps and judicial delays. India's evolving legal framework reflects efforts to modernise copyright law in line with global standards while grappling with the country's distinctive market and infrastructural challenges.

Other countries and regional variations. China has strengthened its copyright laws with increased enforcement against digital piracy, introducing specialised intellectual property courts and harsher penalties, although enforcement inconsistencies persist, especially regarding foreign content on domestic platforms. Many developing countries have made legislative changes inspired by TRIPS and the WCT but face resource constraints and weak judicial systems, resulting in patchy enforcement. Regional trade agreements sometimes incorporate TRIPS-plus provisions demanding higher standards than TRIPS itself, influencing national legislation beyond treaty minimums.

Challenges in national implementation. Despite treaty obligations, countries face common challenges. Resource limitations hinder effective enforcement, especially in policing online piracy. The rapid evolution of streaming technologies often outpaces legislative updates. Balancing copyright enforcement with digital access and fair-use rights remains complex.

Finally, jurisdictional issues and the global nature of digital piracy require cooperation beyond national borders, which can be difficult to coordinate.

D. Cross-border enforcement challenges in digital piracy

In the era of global digital streaming, the regulation of intellectual property rights has become increasingly complex. Streaming-based digital piracy does not recognise national boundaries, but legal systems do. The territorial nature of copyright law, coupled with inconsistencies in international cooperation, creates significant hurdles for effective enforcement. From a legal standpoint, several structural and procedural issues must be examined to understand the depth of the challenge.

Territorial nature of copyright law. At its core, copyright is a territorial right, protected and enforced within the boundaries of a particular state. This principle, enshrined in foundational international agreements such as the Berne Convention and the TRIPS Agreement, allows countries to create their own laws and enforcement mechanisms. However, the same principle becomes a hindrance when infringement occurs across borders. For example, a pirated film hosted on a server in one country but viewed globally cannot easily be tackled by a single jurisdiction's court order. Foreign judgments often require recognition and enforcement procedures, which are time-consuming and may not be granted, especially in countries with weak intellectual property regimes or political resistance.¹⁶

Lack of harmonisation in enforcement mechanisms. Even though treaties such as TRIPS and the WIPO Copyright Treaty establish minimum standards for protection, they leave significant discretion to member states as to how to implement and enforce those standards. As a result, while the underlying rights may be universally acknowledged, procedural enforcement, such as injunctive relief, site blocking and penalties, varies greatly. For instance, countries such as the United Kingdom and Germany allow dynamic injunctions, whereas others require rights holders to return to court for every new infringing URL. This inconsistency creates a patchwork legal environment that pirates exploit by operating from jurisdictions with minimal enforcement capacity.

Limited cross-border injunctive power. Courts in one country often lack the authority to enforce rulings across borders unless treaties or bilateral agreements are in place. Even when successful, enforcement mechanisms such as blocking orders are geographically limited. For example, a court in India may order ISPs to block access to a piracy site within the country, but

¹⁶ Ruth L. Okediji, *The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries* (ICTSD-UNCTAD Issue Paper No. 15, 2006).

the site can continue operating for global users. While some courts, notably in the European Union, have begun to explore extraterritorial jurisdiction in copyright cases, especially where the harm occurs in their territory, this remains controversial and subject to challenge. Moreover, platforms may comply only partially, or may challenge such orders on the basis of freedom of expression or intermediary-liability protections.

Challenges in criminal jurisdiction and extradition. Criminal prosecution of digital pirates across borders is rare because of the complexity of international criminal law. The principle of dual criminality, that the offence must be illegal in both jurisdictions, combined with the requirement for extradition treaties, slows down or even prevents enforcement against foreign perpetrators. Some countries do not treat piracy as a serious criminal matter, regarding it instead as a civil or administrative issue. This further reduces the likelihood of successful prosecution, asset seizure or incarceration for major piracy-network operators, even where the damage to copyright holders is significant.

Intermediary liability and safe-harbour limitations. Another legal challenge lies in the differing standards for intermediary liability. Under the United States DMCA, internet intermediaries such as *YouTube* or cloud providers are protected by safe-harbour provisions, provided that they respond expeditiously to takedown notices. These standards are not universal, however. In the European Union, the Digital Services Act and the prior e-Commerce Directive outline conditional liability, but some non-Western countries impose no clear obligations on intermediaries. This lack of a uniform global regime makes cross-border enforcement unpredictable, as platforms and ISPs respond differently depending on local regulations, business interests or even political considerations.

Evidence gathering and procedural barriers. Enforcing copyright across borders also involves the challenge of evidence collection, which often requires compliance with strict procedural rules such as chain of custody, data-localisation laws or court-ordered discovery. In some cases, rights holders must initiate separate proceedings in each country to compel platforms to release IP addresses, payment records or logs relating to infringing activity. Moreover, privacy laws such as the European Union's General Data Protection Regulation may prevent or delay access to this information, even for legitimate enforcement purposes. These procedural hurdles are especially problematic when dealing with anonymous actors or those using decentralised and encrypted services.

Diplomatic and geopolitical friction. In some instances, geopolitical tensions influence cross-border enforcement. Countries may hesitate to cooperate on intellectual property enforcement

if diplomatic relations are strained or if there is a broader ideological divide about internet freedom and digital sovereignty. For example, efforts by one country to shut down piracy operations in another may be resisted if the target nation views such enforcement as an intrusion on its legal sovereignty. These political frictions complicate otherwise lawful enforcement efforts, creating conditions in which piracy can persist under the guise of national interest or economic development.

Need for international legal reform and cooperation. The limitations of current legal mechanisms call for a more unified international response. While global treaties provide a basic structure, they must be updated to reflect the realities of digital streaming, including mechanisms for real-time site blocking, automatic recognition of injunctions and expedited data-sharing protocols. The establishment of an international copyright-enforcement tribunal or a multilateral fast-track system for takedown cooperation could significantly improve enforcement. Legal reforms must also be supported by diplomatic initiatives to build trust, standardise procedures and reduce resistance to foreign enforcement requests.

VI. ROLE OF PLATFORMS AND INTERNET SERVICE PROVIDERS

A. Responsibility of OTT platforms for copyrighted content

As the consumption of content moves from traditional broadcast media to over-the-top (OTT) platforms such as *Netflix*, *Amazon Prime Video*, *YouTube* and *Hotstar*, the question of legal responsibility for copyrighted content has become a central concern. These platforms can function in different capacities: some act purely as content distributors or hosts, while others allow users to upload and share material. The nature and extent of their liability depend largely on their operational model and the legal framework of the jurisdiction in which they operate.

Nature of OTT platforms: intermediary or publisher. Legally, an OTT platform can fall into two broad categories. As a content owner or publisher, a platform such as *Netflix* or *Disney+* creates or licenses the content it hosts; in such cases, it is fully responsible for ensuring that it has the necessary rights to stream the content, and any infringement makes it directly liable. As an intermediary or host, a platform such as *YouTube* or *Vimeo* allows user-generated content; such platforms act as intermediaries, and their liability is governed by safe-harbour provisions if they follow certain due-diligence and takedown procedures. The legal classification affects the extent to which a platform is liable for infringement and the enforcement obligations it must meet.

Safe-harbour provisions and conditional immunity. The concept of safe harbour comes from laws such as the United States DMCA and similar laws in other jurisdictions, which protect

intermediaries from liability for infringing content uploaded by users, provided that certain conditions are met: the platform must not have actual knowledge of the infringing content; upon receiving a valid takedown notice, it must act expeditiously to remove or disable access to the content; and the platform must not benefit financially from the infringing content where it has the right and ability to control it. These provisions recognise that platforms cannot proactively monitor every piece of uploaded content but are expected to take reasonable action once aware of infringement. Safe harbour is not automatic, however. Courts have held that where platforms are found to be wilfully blind or to encourage infringement, for example by promoting pirated content or making it monetisable, they lose immunity and can be held legally responsible.

European Union Directive on Copyright in the Digital Single Market (Article 17). The European Union's 2019 Copyright Directive, particularly Article 17, significantly expands the responsibilities of platforms. Platforms must obtain licences from rights holders where possible; they must take proactive steps to prevent unauthorised content from being available; and they are held directly liable for infringing content unless they demonstrate best efforts to prevent access and promptly remove material once notified. This means that platforms in the European Union are now expected to monitor uploads actively using tools such as content-identification systems, watermarking and AI. Unlike the United States DMCA, this places proactive rather than reactive obligations on platforms.

India's legal framework for OTT platforms. In India, OTT platforms are regulated under the Copyright Act, 1957, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Under these rules, OTT platforms such as *Netflix*, *Amazon Prime* and *Hotstar* are considered digital publishers and are therefore directly responsible for the content they host, whereas user-generated-content platforms such as *YouTube* are treated as intermediaries and must comply with due-diligence requirements to enjoy safe harbour under Section 79 of the Information Technology Act. Platforms must respond to takedown notices, establish a grievance-redressal mechanism and appoint a compliance officer. Failure to meet these conditions can lead to loss of intermediary status and expose platforms to civil and criminal liability.

China: government-controlled enforcement. In China, OTT and streaming platforms are subject to stringent content regulation. All platforms must pre-screen and license content through the National Radio and Television Administration. Platforms are required to implement automated content filtering and real-name user registration to prevent copyright infringement. A platform is strictly liable for infringing content, and the government enforces penalties with

strong administrative and criminal measures. The Chinese system, while efficient at enforcement, is often criticised for blending intellectual property enforcement with censorship.

B. Liability of ISPs and hosting providers in streaming piracy

Internet service providers and hosting providers play a crucial role in delivering digital content to users. While they do not typically generate or upload pirated content themselves, their infrastructure can be used to access, distribute or host infringing content. The question of their liability turns on whether they knowingly enable, or fail to act against, such activities, and whether they meet the legal requirements to qualify for immunity, often referred to as safe-harbour protection.

United States: safe harbour under the DMCA. In the United States, the Digital Millennium Copyright Act, codified at 17 U.S.C. § 512, provides ISPs and hosting providers with safe harbour from liability, provided that they meet specific conditions. These include not having actual knowledge of infringement, not benefiting financially from it, and acting promptly to remove infringing content when notified. In addition, they must implement a policy to terminate repeat infringers. *BMG Rights Management (US) LLC v. Cox Communications, Inc.* is a pivotal example, in which Cox lost safe-harbour protection because of its failure to enforce its repeat-infringer policy. Thus, while the DMCA shields service providers, it also demands proactive enforcement from them.¹⁷

European Union: from intermediary to primary responsibility. In the European Union, legal responsibility is governed by a combination of the InfoSoc Directive (Directive 2001/29/EC) and the Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790). Under Article 8(3) of the InfoSoc Directive, courts can order ISPs to block access to websites engaged in copyright infringement. The 2019 Directive, especially Article 17, marks a shift by placing direct liability on hosting platforms such as *YouTube* or social networks unless they obtain licences or implement effective anti-piracy technologies. The decision in *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH* affirmed that even non-infringing ISPs can be ordered to block access to piracy websites.¹⁸

India: conditional immunity under the Information Technology Act and the Copyright Act. In India, Section 79 of the Information Technology Act, 2000, provides conditional safe harbour to intermediaries, including ISPs and hosting providers. To retain immunity, these entities must not initiate or modify transmissions, must observe due diligence and must act

¹⁷ *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc.*, 881 F.3d 293 (4th Cir. 2018).

¹⁸ *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH*, Case C-314/12, ECLI:EU:C:2014:192 (Mar. 27, 2014).

swiftly upon receiving actual knowledge of infringement through court orders or government directives. This is complemented by the Copyright Act, 1957, particularly Section 51, which sets out the scope of infringement, including indirect facilitation. The judiciary has actively supported enforcement through dynamic injunctions; the Delhi High Court, for instance, has directed ISPs to block newly identified rogue websites carrying unauthorised live-sports streams as those websites appear.

China: strict regulatory oversight and limited safe harbour. Unlike the United States and India, China lacks an explicit safe-harbour framework comparable to the DMCA. The Copyright Law of the People's Republic of China (2020 revision), together with regulations such as the Measures for the Administration of Internet Information Services, imposes strict obligations on ISPs and hosting providers to prevent the dissemination of infringing content. Service providers must monitor and remove infringing materials or risk administrative penalties and, in serious cases, criminal prosecution under the relevant provisions of the Criminal Law. Government agencies such as the Cyberspace Administration of China have broad powers to block access, shut down platforms or penalise non-compliant ISPs.

Trends in enforcement and global comparisons. Globally, enforcement mechanisms are evolving to increase the accountability of ISPs and hosts. Courts are increasingly issuing site-blocking orders and dynamic injunctions and requiring repeat-infringer policies. The balance between enforcement and freedom of expression continues to shape the debate. In jurisdictions with robust safe-harbour regimes, ISPs are expected to remain neutral but responsive. In others, particularly the European Union after Article 17 and China, platforms are shifting toward proactive monitoring and licensing, effectively becoming gatekeepers of digital content legality.

VII. POLICY AND REGULATORY CHALLENGES

A. Legislative gaps in India's anti-piracy framework

India's legal framework for addressing digital piracy relies primarily on three key statutes: the Information Technology Act, 2000, the Copyright Act, 1957, and the Cinematograph Act, 1952. However, each of these laws was either enacted or last substantively updated in a pre-OTT or early-digital era and thus fails to address fully the distinctive challenges posed by streaming-based piracy.

Information Technology Act, 2000. The Information Technology Act focuses mainly on cybercrime and intermediary liability but contains no specific provisions relating to streaming piracy or illegal digital broadcasting. Although Section 79 offers safe-harbour protection to intermediaries, the law does not clearly define the responsibilities of OTT platforms or ISPs in

actively curbing access to pirated content. Furthermore, takedown procedures under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, are not robust or efficient enough to deal with fast-evolving piracy networks and mirror links. There is also no statutory provision for dynamic injunctions, which courts have granted only through judicial innovation.¹⁹

Copyright Act, 1957. The Copyright Act, 1957, though amended in 2012 to include some digital rights, still reflects an era focused on physical media. It does not mention OTT platforms, live-streaming technologies or dynamic content hosting, leaving a gap in its applicability to contemporary piracy. Moreover, there is no codified notice-and-stay-down system, making enforcement against repeat or modified uploads difficult. Enforcement mechanisms under the Act, both civil and criminal, are also notoriously slow, and the penalties under Sections 63 and 65 are often inadequate to deter organised digital piracy operations. The law also creates ambiguity regarding platform liability, especially where services passively host or facilitate the distribution of pirated content through user-generated links.²⁰

Cinematograph Act, 1952. The Cinematograph Act, 1952, is similarly outdated. While the Cinematograph (Amendment) Act, 2023, addresses the issue of camcording piracy in theatres, it falls short of dealing with the larger problem of digital film piracy, especially post-release streaming on unauthorised platforms. The law does not contemplate the piracy of films that release directly on OTT platforms, nor does it mandate the use of technological enforcement tools such as watermarking or forensic tracking.

Overall, India's current legislative structure does not reflect the complexities of digital piracy in the streaming era. There is a pressing need to introduce OTT-specific regulation, clearly define platform obligations, integrate technology-based enforcement mechanisms and develop cross-border enforcement protocols. Without a comprehensive legal overhaul, enforcement will remain fragmented, slow and ineffective against modern digital piracy operations.

B. Digital IP tribunal versus fast-track court mechanism

With the explosion of digital content creation and streaming platforms, India has witnessed a corresponding rise in online copyright infringement, unauthorised streaming and piracy of OTT content. Traditional enforcement mechanisms under the Copyright Act, 1957, the Information Technology Act, 2000, and the Code of Civil Procedure are no longer sufficient to keep pace with the speed and technical sophistication of these infringements. The idea of setting up a

¹⁹ The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).

²⁰ The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).

dedicated digital intellectual property tribunal or a fast-track court has therefore gained increasing relevance.

Digital IP tribunal. A dedicated digital intellectual property tribunal would offer specialised adjudication of cases involving online infringement, OTT piracy, data scraping of copyrighted works and emerging issues such as AI-generated content. Such a tribunal could operate under the umbrella of existing intellectual property law but be staffed with technical experts, digital-forensic professionals and judges trained in cyber law and digital rights. This would help ensure both legal precision and procedural efficiency.

Fast-track IP court. Alternatively, setting up a fast-track intellectual property court mechanism, possibly under the existing commercial-courts framework, could significantly improve the speed of enforcement. This model has already been used in India for cases under the Commercial Courts Act, 2015, and could be adapted to handle time-sensitive injunctions, dynamic site-blocking orders and emergency takedown petitions under copyright law.

Comparing the two models. Several considerations bear on the choice between a dedicated tribunal and a fast-track court. On speed and specialisation, a dedicated tribunal would help ensure the swift resolution of disputes involving illegal streaming, unauthorised re-uploads and platform liability, with specialised judges and technical members deciding cases on the basis of both legal merit and digital evidence, including blockchain verification, digital watermarking and content fingerprints. On the handling of new types of dispute, new forms of infringement, such as those involving AI-generated content, non-fungible-token-based violations and algorithmic plagiarism, require adjudicators who understand emerging technologies, expertise that a general court may lack. On support for rights holders, independent creators and small studios often lack the financial means to pursue prolonged litigation, and a low-cost, expedited forum would offer them a practical mechanism to enforce their rights, especially for injunctions and takedown orders before release windows are breached. On the uniform application of law, a centralised or regional tribunal system would help ensure the consistent application of digital intellectual property rules, including on platform liability, DMCA-style takedowns and cross-border piracy responses, which are at present applied inconsistently across different high courts.
