IP ENFORCEMENT IN DIGITAL MARKETPLACE

Shreya Datta Gupta, LLM, Christ (deemed to be) University, Bangalore, Karnataka

ABSTRACT

The rapid expansion of digital commerce has generated unprecedented potential for global commerce, while increasing risks of violations of intellectual property rights (IPR). Counterfeit and replica goods, unauthorised use of trademarks, copyright piracy, and patent violations have become widespread on e-commerce platforms. The TRIPS Agreement and Anti-Counterfeiting Trade Agreement (ACTA) have attempted to address these challenges, but enforcement, especially in cyberspace, is still lacking. The new advancements in artificial intelligence (AI) technology have altered the landscape of monitoring and enforcement by providing new automated and timely solutions. The advancement of AI raises new issues such as who is liable, questions of privacy, and the difficulty of detecting nuanced violations. In India, although the digital commerce market is developing rapidly, the existing IP regime is not equipped to combat online violations due to issues of jurisdictional uncertainties, loopholes in intermediary liability and scant statutory guidance. This paper aims to highlight international trends, technological advancements, and domestic realities, to propose a hybrid enforcement model that refines AI detection, increases intermediary liability and harmonization of legal changes. These changes are essential to balancing innovation, trade facilitation, and protection of intellectual property in the digital age.

Keywords: intellectual property, counterfeit, artificial intelligence, cyberspace, digital commerce.

INTRODUCTION

The evolution of digital commerce has helped to change the global economy, allowing transactions from one country to another as easily as sending an email and giving businesses and consumers more options than ever. Online marketplaces like Amazon, Flipkart, and eBay have become the preferred remote mechanism for conducting trade, offering convenience, choice, and access to shops from around the globe. However, the growth has also highlighted the weaknesses arising from intellectual property rights (IPR) infringements, with the prevalence of counterfeit goods, impersonation of trade marks, and copyright piracy on these sites. Many of the positive features of e-commerce, such as low barriers to entry, seller anonymity, and the cross-border aspect of trading, make e-commerce an attractive reality for infringers.[1]

The Agreement on Trade-Related Aspects of Intellectual Property Rights laid the foundation for harmonized IP protection, but the enforcement mechanisms were inadequate to deal with the complexities of cyberspace.[2] To fill these gaps, developed nations spearheaded the Anti-Counterfeiting Trade Agreement (ACTA, 2011), which introduced advanced enforcement tools specifically targeting the digital environment.[3] Despite its innovations ACTA has been criticized by developing countries for imposing unequal obligations on intermediaries and for potentially restricting access to knowledge and digital freedoms.[4]

In addition to legal structures, technology has arisen as a powerful means of enforcing intellectual property. By providing automated detection and analysis, and given that artificial intelligence (AI) technology is broadly available, AI systems are increasingly being deployed to monitor e-commerce sites. AI systems can monitor for counterfeit listings, identify transaction patterns, and flag content with questions, all at a greater speed than humans would be able to observe. However, there are limits to these technologies such as false positives, inability to assess less straightforward infringements of intellectual property, and unanswered issues of liability.[5]

---

[1] A.V. Pokrovskaya, Intellectual Property Rights Infringement on E-Commerce Marketplaces: Application of AI Technologies, New Challenges, 522 E3S Web Conf. 01057 (2024).
[2] Mohammad Bagherpour, The Enforcement of Intellectual Property Rights in Digital Environment Based on ACTA, 4(11) Mediterranean J. Soc. Sci. 615 (2013).
[3] Id.
[4] **Id.** at 617–19.
[5] Pokrovskaya, supra note 1, at 2–4.

In India, there is a lot of concern for the future of IP enforcement. The digital commerce industry is booming and is to surpass the $100 billion mark in a few years.[6] Yet the existing legal framework for IP - the Copyright Act, the Patents Act, and the Trademarks Act - were not set up for the digital world. The treatment of significant issues surrounding IP in online commerce is still sporadic when applying the existing IP laws. Indian courts are beginning to consider these issues in landmark cases like Ericsson v. Xiaomi and L'Oréal v. ShopClues, but the absence of a clear statutory framework creates uncertainty.[7] In combination, issues of jurisdiction, intermediary liability, and enforcement continue to challenge a rights holder's protection in the digital marketplace.[8]

This paper investigates the enforcement of IPR in a digital commerce setting in three key ways: (i) the global context with a specific focus on ACTA, (ii) how AI technologies can assist in the identification and pre-emption of infringements, and (iii) an Indian viewpoint on addressing digital IP enforcement. By combining the three approaches taken above, we propose a hybrid context that considers the need of innovators to innovate, to facilitate trade, and enforcement of intellectual property rights.

STATEMENT OF THE PROBLEM

The meteoric rise of online marketplaces has created new opportunities and serious challenges to the implementation of intellectual property rights. The anonymity of the sellers, lack of geographical borders, and sheer numbers of transactions occurring online largely enables counterfeiting, piracy, and misuse of trademarks. The TRIPS Agreement, and the Anti-Counterfeiting Trade Agreement (ACTA) have made distinct progress in addressing enforcement gaps but lack a unified and lasting approach to enforcement in the changing landscape of cyberspace. Further, while technology, including artificial intelligence, to combat infringement offers new solutions to the problem of enforcement there are issues regarding false positives, liability, and limited capacity for complex infringing situations. In India, where it is forecast that the digital commerce sector will exceed $100 billion, the current intellectual property regime has not been sufficiently developed to meet the challenges of online infringements especially with jurisdictional questions, vague provisions of intermediary

[6] Reach of Intellectual Property Rights in Digital Commerce: An Indian Perspective *(2022),* https://ssrn.com/abstract=4037926.
[7] Id.; Telefonaktiebolaget LM Ericsson v. Xiaomi Tech., Order, Delhi High Court (Dec. 8, 2014); L'Oréal SA v. ShopClues, Order, Delhi High Court (Oct. 2014).
[8] Reach of Intellectual Property Rights in Digital Commerce: An Indian Perspective*,* supra note 6, at 8–12.

liability, and the disparity in how the Judiciary, including the High Courts, has approached enforcement making enforcement sporadic and ineffective. There's still no harmonised implementation framework completely decoupled from the potentially adaptable terrain of technology, which not only threatens innovation and investment but also consumers' trust in the digital economy altogether.

RESEARCH QUESTIONS

1. How well do the current international frameworks—TRIPS and ACTA in particular—address the difficulties in implementing intellectual property rights in online trade?

2. How can artificial intelligence be used to identify and stop online intellectual property rights violations, and what are its accuracy, liability, and ethical limitations?

3. How well does online IPR enforcement get covered by the current Indian legal system, which includes the Copyright Act, Patents Act, Trade Marks Act, and Information Technology Act?

4. What discrepancies or holes in the legal system still exist in the way Indian courts have construed and applied intermediary liability in cases involving digital infringement?

5. How may successful protection of intellectual property rights in the digital economy be achieved by a hybrid enforcement strategy that combines legal reform, intermediary accountability, and AI-based technical solutions?

RESEARCH OBJECTIVES

1. To explore the challenges of enforcing rights relating to intellectual property in digital markets, particularly in terms of anonymity, cross-border jurisdiction and counterfeiting.

2. To assess the impact of international legislation like TRIPS and ACTA on online infringements and how that legislation applies to a digital environment.

3. Examine the role of AI in the detection and prevention of IP infringements and examine its limitations, ethical considerations and liability issues.

4. To investigate the adequacy of the Indian laws including the Copyright Act, Patents Act, Trademarks Act and the Information Technology Act, in protecting IPRs in digital commerce.

5. To recommend a hybrid enforcement model that combines legal reform, intermediary liability and technology, to ensure IPRs can be adequately protected in the digital economy.

RESEARCH METHODOLOGY

The present research will adopt a doctrinal legal methodology, combined with analytical and comparative approaches, in order to investigate the enforcement of intellectual property rights (IPR) in digital marketplaces. The study draws on secondary sources including, including statutes, international treaties, appellate court law, legal articles, reports, and case studies.

Nature of Research

This is a qualitative and exploratory study involving the interpretation, analyses and evaluation of laws, case studies, and scholarly debate; not statistics or empirical data. The goal to critically examine how adequate the existing legal frameworks - international and domestic - respond to the challenges of IPR infringements in the digital space.

Sources of Data

Primary Sources: International conventions (TRIPS, ACTA), national legislation (Copyright Act, Patents Act, Trademarks Act, Information Technology Act), and case law from India and other jurisdictions (e.g., Ericsson V. Xiaomi, L'Oréal V. ShopClues and L'Oréal V. eBay).

Secondary Sources: Legal academic journals, law review articles, reports from entities such as WIPO, OECD, and others that have explored scholarly infringements to IPR enforcement in cyberspace. Research papers by Pokrovskaya (2024), Bagherpour (2013), and the SSRN article (2022), will form a significant part of the related literature.

Research Design and Approach

Doctrinal analysis will study legislative law and judicial interpretation on the issue of IP enforcement, in contemplation of the authors who have critiqued digital infringement of

trademarks and copyright for example. As a methodological consideration, a deductive using summarising, analytical and inductive approaches, coupled with reviewing the highs and lows of current enforcement mechanisms exists within a larger framework (Ridgeway and Tom, 2010).

Comparative Approach: Compare how Indian enforcement mechanisms contrast with the EU, U.S., and China's approaches to draw on identified lessons learned and best practices.

Analytical Approach: Review artificial intelligence, how it can be utilized within IP enforcement, the pros and cons of artificial intelligence and its legal implications for IP enforcement.

Prescriptive Approach: Outline suggestions and reforms for a hybrid enforcement model that balances certainty about the law, adapting to technology, and ensuring fairness.

1. INTERNATIONAL FRAMEWORK ON IPR ENFORCEMENT

1.1 TRIPS Agreement

The primary international agreement for harmonising intellectual property norms is still the 1994 Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPS), which was reached within the framework of the World Trade Organisation (WTO). Member states are required by TRIPS to establish efficient enforcement procedures, including as border controls and civil, administrative, and criminal remedies.[9] However, while TRIPS prescribes minimum standards, it does not provide detailed mechanisms for enforcement in cyberspace. Its provisions were drafted in a pre-digital era, leaving unresolved questions of online jurisdiction, intermediary liability, and enforcement of infringements occurring across borders.[10]

TRIPS has come under fire from academics for being "technology-neutral," a feature that was once thought to be adaptable but now leads to enforcement gaps in digital contexts.[11] For example, TRIPS Article 61 mandates criminal penalties for piracy and counterfeiting, but it says nothing about how these requirements apply to e-commerce sites where violators might

[9] Agreement on Trade-Related Aspects of Intellectual Property Rights arts. 41–61, Apr. 15, 1994, 1869 U.N.T.S.
[10] Graeme B. Dinwoodie, The International Intellectual Property System: Treaties, Norms, National Courts, and Private Ordering, 23 *U. Pa. J. Int'l Econ. L.* 433, 455–58 (2002)
[11] Rochelle C. Dreyfuss, TRIPS and Essential Facilities, 12 *Marq. Intell. Prop. L. Rev.* 1, 12–14 (2008).

be anonymous or based outside of national borders.[12]

Even while the TRIPS Agreement is still the mainstay of global intellectual property protection its shortcomings are clear in online environments. TRIPS obligations, as demonstrated by WTO rulings, such as the China – Intellectual Property Rights (2009) dispute, are frequently insufficient to overcome systemic enforcement deficiencies, especially in online counterfeiting and piracy. Once praised for its adaptability, TRIPS' "technology-neutral" draughting today leaves room for interpretation when it comes to modern digital phenomena like streaming platforms, cloud storage, and NFTs. Guidelines for anonymous merchants operating from offshore jurisdictions are not included in Article 61, which stipulates criminal consequences for piracy. Because of this, member states' enforcement of the law is wildly inconsistent due to the absence of specific provisions suited to digital trade.

1.2 Anti-Counterfeiting Trade Agreement (ACTA)

In 2011, developed economies led the charge to create the Anti-Counterfeiting Trade Agreement (ACTA) in order to overcome the shortcomings of TRIPS. Particularly in the digital sphere, ACTA included sophisticated enforcement tools, such as duties for Internet service providers (ISPs) and channels for collaboration between intermediaries and rightsholders.[13] By specifically acknowledging the part that digital commerce plays in enabling violations, its measures on border enforcement and civil remedies aimed to modernise the framework for international enforcement.[14]

ACTA, however, proved controversial. Its obligations, according to critics from developing countries, disproportionately taxed intermediaries and ran the risk of limiting access to digital freedoms and knowledge.[15] In 2012, the European Parliament rejected ACTA on the grounds that the fundamental rights were violated specifically the right to privacy and freedom of expression. As a result, even if ACTA was a daring attempt to update international enforcement, its limited acceptance lessens its usefulness for the global enforcement system.

Signed in 2011, the Anti-Counterfeiting Trade Agreement (ACTA) introduced strong measures

[12] TRIPS, supra note 1, art. 61.
[13] Anti-Counterfeiting Trade Agreement, Oct. 1, 2011, available at https://ustr.gov/acta
[14] Daniel J. Gervais, ACTA: The Negotiation of the Anti-Counterfeiting Trade Agreement, 55 *J. World Intell. Prop.* 13, 25–29 (2012).
[15] Peter K. Yu, ACTA and Its Controversial Provisions, 26 *Am. U. Int'l L. Rev.* 645, 662–66 (2011).

for intermediary responsibility and border enforcement in an effort to close these loopholes. However, because of the confidentiality of its discussions and the perception that it imposed Western enforcement norms on underdeveloped nations, ACTA was very controversial. Concerns over censorship and the potential to stifle online freedoms were raised by civil society organisations who claimed that the law's provisions for internet service providers to implement proactive monitoring effectively privatised enforcement. The European Parliament rejected ACTA in 2012 after the widespread demonstrations in a number of European nations, citing a lot of concerns about privacy and the freedom of speech. ACTA's legacy endures even in the absence of official approval, as evidenced by its influence on subsequent frameworks, including EU Directives on digital enforcement, despite its failure.

1.3 Comparative Assessment

A fragmented international enforcement environment is revealed by the combined experience of ACTA and TRIPS. While ACTA attempted but was unsuccessful to expand these duties into the digital realm, TRIPS offers the bare minimum of a harmonised framework. As a result, enforcement strategies differ greatly among nations. While developed nations like the US and the EU have enacted more robust intermediary liability laws and technology safeguards but emerging nations like India are still having difficulty striking a balance between enforcement, information access, and digital commerce.[16]

Therefore, even though TRIPS and ACTA mark significant advancements in international IPR enforcement, effective enforcement in digital commerce is still hampered by the lack of a well recognised and modernised instrument. This fact emphasises the necessity of hybrid local solutions that combine technology advancements with international commitments.

The fragmentation of enforcement is highlighted by comparing worldwide models. The widely used "notice-and-takedown" mechanism was created by the US Digital Millennium Copyright Act (DMCA 1998) and it provides safe harbour protection for intermediaries who swiftly respond to takedown notices. Despite its impact, this strategy has come under fire for misuse as automatic takedowns stifle legitimate uses like satire and fair use. The EU Digital Services Act (DSA 2022), on the other hand, it takes a more stringent stance, mandating algorithmic

[16] Shamnad Basheer, The Enforcement of IPR in India's Digital Economy, 4 *Indian J. L. & Tech.* 1, 18–21 (2010).

transparency, proactive platform monitoring, and the participation of "trusted flaggers" in reporting violations.

2. ARTIFICIAL INTELLIGENCE AND IPR ENFORCEMENT IN DIGITAL COMMERCE

2.1 The Role of AI in Enforcement

In digital commerce, artificial intelligence (AI) has become a game-changing tool for monitoring and enforcing intellectual property rights (IPR). AI systems can search through enormous volumes of internet content to find illegal content, fake listings, and questionable transaction patterns by utilising machine learning algorithms and automated data analytics.[17] AI can process millions of listings across platforms in real time, providing previously unheard-of efficiency in violation identification, in contrast to human enforcement, which is limited by scale and time.[18]

Prominent e-commerce sites like Amazon and Alibaba have implemented AI-powered enforcement tools to keep an eye on listings, warn dubious vendors, and take down illegal content before it reaches customers.[19] Additionally, AI helps rightsholders by easing takedown procedures in compliance with national laws' notice-and-takedown systems and providing statistics on repeat offenders.

In the fight against intellectual property infringement in digital commerce, artificial intelligence (AI) has become essential. With billions of uploads processed each year, platforms such as YouTube use Content ID, an advanced AI-driven technology that automatically compares submitted content to a database of copyrighted works. In a similar vein, brand owners can utilise AI to proactively identify and eliminate fake listings through Amazon's Project Zero. These illustrations show how AI improves enforcement's scalability and efficiency using machine learning and data analytics. Furthermore, the new developments that integrate blockchain technology and artificial intelligence (AI) allow digital watermarking of protected content to ensure authenticity and monitor illegal reproductions across platforms.

[17] A.V. Pokrovskaya, *Intellectual Property Rights Infringement on E-commerce Marketplaces: Application of AI Technologies, New Challenges*, E3S Web Conf. (2024)
[18] Id.
[19] Alibaba Group, *Intellectual Property Rights Protection Annual Report* (2021).

2.2 Advantages of AI in IPR enforcement

AI improves enforcement in a number of important ways:

I. **Scale and Speed:** AI systems are capable of analysing hundreds of transactions per second and identifying violation patterns that are beyond human comprehension.[20]

II. **Predictive Monitoring:** By analysing the seller behaviour, pricing irregularities and product similarities AI systems can use predictive analytics to foresee possible infringement activities.[21]

III. **Cost-effectiveness:** Automated monitoring lowers enforcement expenses for governments and rightsholders, particularly in regions with limited resources.[22]

IV. **Data-Driven Enforcement:** AI makes it possible to gather evidence, which provides precise infringement data to support legal actions and policy decisions.[23]

AI's advantages include customisation in addition to speed and scalability. To increase detection accuracy, rights holders might create AI models specifically for their portfolios of intellectual property. Another important benefit is real-time monitoring, which reduces harm to both consumers and rights holders by flagging or blocking infringing listings before they reach consumers. AI systems' affordability adds to their allure, particularly for non funded governments and law enforcement agencies. Crucially, AI-generated evidence supports better informed court rulings by bolstering the evidential foundation for litigation and policymaking.

2.3 Limitations and Challenges

AI is not a cure all, despite its potential. Its efficacy is limited by a lot of issues:

I. **False Positives:** AI systems have the potential to mistakenly see permissible applications, including fair dealing or satire, as violations.[24]

[20] OECD, *Misuse of E-commerce for Trade in Counterfeits* (2021).
[21] Id.
[22] World Intellectual Property Organization (WIPO), *Technology Trends 2022: Artificial Intelligence* 74–76 (2022).
[23] Id.
[24] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 *Geo. L.J.* 1147, 1162–64 (2017)

II. **Nuanced Violations:** Current AI models are still unable to handle complex problems like identifying significant copyright similarity or evaluating deceptive trademark similarity.[25]

III. Jurisdictional and Enforcement Gaps: Because of the anonymity of sellers and uneven international cooperation, cross-border enforcement is still hard even when AI detects infringers.[26]

IV. **Access Inequality:** Small enterprises and individual producers frequently lack the funds to implement comparable tools, but major corporations can afford powerful AI systems.[27]

Despite its potential, enforcing AI is fraught with difficulties. The emergence of adversarial AI, in which infringers employ algorithms to covertly change product photos, keywords, or metadata in order to avoid detection systems, is one urgent problem. Furthermore, the disparity in access to AI technologies widens the enforcement gap because small and medium-sized businesses (SMEs) sometimes lack the funding necessary to implement comparable safeguards, whereas multinational organisations can afford more complex systems. Over-blocking is still a major issue since automated systems commonly mistakenly identify legitimate applications like memes, satire, or instructional reproductions, which results in excessive limitations on the right to free speech.

2.4 Liability and Ethical Considerations

There are new ethical and legal issues brought up by the growing use of AI in IPR enforcement. Who is responsible if non-infringing content is mistakenly flagged by AI systems the platform, the rightsholder, or the AI developer?[28] Although early reasoning indicates platforms may carry main responsibility as intermediaries under safe harbour provisions, courts have not yet offered definite solutions.[29]

The growing use of AI brings up some important ethical and liability issues. If an AI system

[25]Mark A. Lemley & Bryan Casey, Remedies for Robots, 86 *U. Chi. L. Rev.* 1311, 1322–25 (2019).
[26]Shamnad Basheer, The Enforcement of IPR in India's Digital Economy, 4 *Indian J. L. & Tech.* 1, 21–23 (2010).
[27] OECD, supra note 5, at 32–34
[28] Coglianese & Lehr, supra note 9, at 1170–72
[29] *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 27–28 (2d Cir. 2012)

improperly removes the legitimate content, does responsibility reside with the developer, the platform, or the rights holder? Given their potential to violate fundamental rights, some enforcement-related AI systems have been categorised as "high-risk" under the EU AI Act (2024). Arguments concerning automatic DMCA takedowns in the US draw attention to the dangers of algorithmic prejudice, where political expression and artistic creations have been unjustly silenced. The balance between the preservation of digital liberties and the effectiveness of enforcement is still up in the air in the absence of clear legal direction.

Furthermore, possible over-enforcement raises ethical concerns. Over-reliance on automated systems may stifle acceptable uses, like transformative works, fair use, and exceptions for education. About Careful calibration of AI deployment and legislative measures to prevent abuse are necessary to strike a balance between consumers' digital freedoms and strict enforcement.

2.5 Towards a Hybrid Model

The most practical approach, is a hybrid model that blends human oversight with AI efficiency. While the human evaluators guarantee some sophisticated judgements in borderline circumstances, automated detection methods can manage the volume of online transactions. Collaboration between the public and private sectors is also essential since governments might fund the creation of shared AI technologies that law enforcement and SMEs could use. A more equitable distribution of enforcement skills would be ensured by such an inclusive strategy, which would also stop big firms from monopolising enforcement technology.

AI's incorporation into the enforcement systems is a crucial step towards modernising the IPR protection in the digital economy, even though it cannot completely replace human judgement. The most promising course forward is a hybrid enforcement paradigm that combines the effectiveness of AI with human monitoring and strong legal protections. In addition to improving the efficacy of enforcement, such a strategy would maintain the harmony between defending digital liberties and intellectual property.

3. THE INDIAN PERSPECTIVE ON IPR ENFORCEMENT IN DIGITAL COMMERCE

3.1 Statutory Framework

A set of laws developed in the pre-digital age control India's intellectual property rights (IPR)

system. The foundation of IPR protection is provided by the Copyright Act of 1957, the Patents Act of 1970, the Trade Marks Act of 1999, and the Patents Act of 1970. In addition to this, internet conduct is covered under the Information Technology Act, 2000 (IT Act), which includes section 79 on intermediary liability.[30]

The legal foundation for IP enforcement in digital commerce in India is still disjointed. Online licensing regulations were implemented by the Copyright (Amendment) Act of 2012, however it provided minimal enforcement guidance. In a similar vein, marketplaces are subject to transparency requirements under the Consumer Protection (E-commerce) Rules, 2020, although IP infringement are not directly addressed. The Information Technology Act of 2000's Section 79, which grants safe harbour to intermediaries, is similar to the U.S. DMCA in several ways but lacks specific procedural guidelines like a notice-and-takedown system. Platforms and courts must therefore negotiate ambiguities when assessing the extent of intermediary liability in intellectual property issues.

Despite providing a strong basis for intellectual property protection, these laws were not written with cyberspace or e-commerce in mind. For example, the Patents Act does not contain explicit rules on safeguarding technological innovations used in e-commerce ecosystems, while the Copyright Act does not specifically address digital infringement through online platforms. In a similar vein, the Trade Marks Act is not well-suited to address cross-border mark misuse in online marketplaces, because vendors usually come from other countries.

3.2 Judicial Engagement

Indian courts have started modifying current laws to take into account the realities of online shopping. The Delhi High Court acknowledged the necessity for efficient remedies against infringement in online marketplaces when it addressed patent enforcement in the context of mobile technology sales on digital platforms in Telefonaktiebolaget LM Ericsson v. Xiaomi Technology.[31]

The Delhi High Court took a strong stand against intermediary platforms that host counterfeit goods in L'Oréal SA v. ShopClues.com, stating that e-commerce companies could not avoid punishment by claiming mere facilitation. The court underlined that middlemen have an

[30] The Information Technology Act, No. 21 of 2000, § 79, India Code (2009).
[31] *Telefonaktiebolaget LM Ericsson v. Xiaomi Technology & Ors.*, (2017) 69 PTC 1 (Del. HC)

obligation to take reasonable precautions to stop the selling of fake goods. Similarly, the court determined that platforms offering value-added services could be regarded as active participants and, as such, be held accountable for trademark infringement in Christian Louboutin SAS v. Nakul Bajaj.[32]

These rulings show a slow judicial trend towards increasing intermediaries' liability in online transactions. However, ambiguity persists due to inconsistent rulings and the lack of a unified statutory standard.

3.3 Intermediary Liability and Safe Harbour

In the event that intermediaries operate as conduits and undertake due diligence, they are free from liability for third-party material under Section 79 of the IT operate. Indian courts, however, have given this clause varying interpretations. Some rulings have maintained substantial safeguards for intermediaries, while others have limited safe harbour in favour of rightsholders.[33]

This conflict illustrates how difficult it is to strike a balance between intellectual property protection and innovation and the commerce. Excessive responsibility may hinder digital trade, while overly expansive safe harbour regulations run the danger of permitting infringement. A balanced and unified framework can only be provided by legislative reform.

A judicial division can be seen in the interpretation of Section 79 of the IT Act. In order to protect themselves from widespread liability, certain rules highlight that intermediaries should only take action following judicial notification. Others, like L'Oréal v. ShopClues, demand proactive monitoring, especially when platforms make money off of infringement. This discrepancy emphasises the necessity of statutory clarification. In order to bring Indian legislation into line with global best practices, the Draft Digital India Bill, 2023, which aims to replace the IT Act, suggests stronger due diligence requirements and may reinterpret intermediary liability.

3.4 Challenges In Enforcement

India's IPR enforcement in internet commerce confronts numerous obstacles despite court

[32] *Christian Louboutin SAS v. Nakul Bajaj & Ors.*, 2018 SCC OnLine Del 12915
[33] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (clarifying limits of intermediary liability in the free speech context)

efforts:

I. **Complexities of Jurisdiction:** Since infringers frequently operate from outside, domestic law enforcement is challenging.[34]

II. **Resource Limitations:** Courts and regulatory organisations do not have enough resources to effectively monitor and decide cases involving internet infringement.

III. **Technological Gaps:** The sophisticated AI techniques utilised by international platforms are not readily available to enforcement agencies.

IV. **Fragmented Judicial Interpretation:** Enforcement results are unpredictable due to conflicting court decisions regarding intermediary liability.

These problems highlight the need for India to implement a hybrid enforcement paradigm that incorporates the AI technologies, clarifies intermediary liability, and harmonises judicial procedures in order to successfully safeguard IPR in the digital marketplace.

CONCLUSION

Global trade has been transformed by the exponential expansion of digital commerce, but it has also increased the scope and complexity of intellectual property rights (IPR) violations. Online marketplaces are fuelled by low entry barriers, seller anonymity, and cross-border accessibility, all of which support legal trade while also making it easier for counterfeit goods, piracy, and trademark abuse to occur.[35]

Although the TRIPS Agreement created a uniform standard for IPR enforcement, its technology-neutral clauses have not been sufficient to handle the particular difficulties presented by cyberspace.[36] The Anti-Counterfeiting Trade Agreement (ACTA) sought to modernise enforcement, especially in the digital realm, but its efficacy as a worldwide remedy was compromised by its rejection by important jurisdictions like the European Union.[37] As a

[34] Shamnad Basheer, The Enforcement of IPR in India's Digital Economy, 4 *Indian J. L. & Tech.* 1, 21–23 (2010).
[35] OECD, *Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact* (2016).
[36] Agreement on Trade-Related Aspects of Intellectual Property Rights arts. 41–61, Apr. 15, 1994, 1869 U.N.T.S. 299.
[37] Eur. Parl. Deb. (July 4, 2012), rejection of ACTA, available at https://www.europarl.europa.eu.

result, domestic legal innovation is necessary because the international system is still fractured.

Artificial intelligence (AI) in particular has become a potent ally in the fight for intellectual property rights. AI can lower enforcement costs, monitor millions of web listings in real time, and identify patterns of infringement. Its drawbacks include unsolved liability issues, false positives, and a lack of nuance in intricate legal decisions.[38] Therefore, without an institutional and legal structure to support it, a simply technological solution is insufficient.

The legal framework in India, which includes the Information Technology Act of 2000, the Trade Marks Act of 1999, the Patents Act of 1970, and the Copyright Act of 1957, was created before the advent of the internet and does not contain extensive provisions for cyberspace. Although Indian courts have started to broaden intermediary liability in instances like L'Oréal v. ShopClues[39] and Christian Louboutin v. Nakul Bajaj[40] enforcement is still dispersed because of jurisdictional issues, resource limitations, and differing interpretations of safe harbour under the IT Act.[41]

One fact is highlighted by the analysis from domestic, international, and technology viewpoints: a hybrid approach combining institutional capacity-building, technological innovation, and legal change is necessary for effective IPR enforcement in digital commerce.

SUGGESTION

Refining Legal Frameworks

- Add specific clauses addressing digital infringement to the copyright, patent, and trademark statutes.

- To guarantee clarity and predictability, harmonise the IT Act's intermediary responsibility rules.

Increasing Intermediary Accountability:

- Provide e-commerce platforms with legal obligations to actively monitor and stop

[38] A.V. Pokrovskaya, *Intellectual Property Rights Infringement on E-commerce Marketplaces: Application of AI Technologies, New Challenges*, E3S Web Conf. (2024)
[39] *L'Oréal SA v. ShopClues.com & Ors.*, 2018 SCC OnLine Del 9340.
[40] *Christian Louboutin SAS v. Nakul Bajaj & Ors.*, 2018 SCC OnLine Del 12915.
[41] The Information Technology Act, No. 21 of 2000, § 79, India Code (2009); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

fraudulent sales.

- Follow international best practices when implementing due diligence requirements that strike a balance between accountability and safe harbour.

Including AI in Law Enforcement:

- Promote platforms' use of AI monitoring tools while imposing obligatory reporting and transparency requirements.

- To reduce false positives and avoid over-enforcement that can impede legal digital liberties, establish regulatory rules.

Increasing Enforcement Agencies' Capacity:

- Give the judiciary and other enforcement agencies the tools and training they need to deal with AI evidence and cross-border infringement concerns.

- Create specialised cyber-IPR units in law enforcement.

International Cooperation

- Encourage bilateral and regional agreements that are specific to the enforcement of digital IPR, especially between poor nations.

- Encourage the creation of a new international framework that protects knowledge access while fusing the universality of TRIPS with the digital-specific elements of ACTA.