WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Liability of E-Commerce Platforms for Online Counterfeit Goods: A Legal Analysis under Indian Trademark Law

Priyanka Tanwar[1], Dr. Chandra Parkash[2]

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Assistant Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

ABSTRACT

The subject under examination studies the liability of e-commerce platforms for online counterfeit goods in India by situating the problem within the existing structure of Indian trademark protection, intermediary immunity, consumer protection rules, and the newer criminal procedure and evidentiary codes. The inquiry moves from the core rights under the "Trade Marks Act, 1999" to the layered protections conferred on intermediaries by "Section 79 of the Information Technology Act, 2000" and the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" as amended on 6 April 2023, which together make safe harbour conditional on demonstrable due diligence and a responsive notice and takedown regime. The study asks whether a marketplace that curates, promotes, fulfils, or guarantees goods continues to be a passive intermediary or becomes an actor in the infringing transaction, and it evaluates this question against the position that trademark law is directed primarily at those who apply a mark or deal in goods, while the IT regime is directed at conduits. The method adopted is doctrinal, drawing on statutory text, executive rules, and binding Delhi High Court decisions from 2017 to 2025, which have supplied the most detailed reasoning on digital marketplace activity. The study finds that Indian law does not yet impose an absolute duty on platforms to screen every listing ex ante, but it does require them to act after being put to specific knowledge, and it removes the shield when platforms move from mere hosting to active facilitation, as seen in cases that dealt with luxury resale, direct selling networks, and origin mislabelling. The analysis also records how the "Consumer Protection (E-Commerce) Rules, 2020" and the "Digital Personal Data Protection Act, 2023" tighten the compliance perimeter by demanding seller verification, data governance, and transparent disclosures that can be used by trademark proprietors to trace infringers and by authorities to pursue criminal remedies under the "Bharatiya Nyaya Sanhita, 2023" for counterfeit property marks. The implications in the Indian context are threefold. First, safe harbour is secure only when the platform can prove procedural discipline. Second, trademark proprietors must align their enforcement strategies with the IT route and not rely solely on the trade mark statute. Third, the new criminal and evidentiary codes, especially "BNSS, 2023" on electronic search recording and "BSA, 2023" on admissibility of electronic records, provide a sharper public law pathway against repeat counterfeiters operating through e-commerce channels.

Keywords: E-commerce, intermediary liability, counterfeit goods, trademark infringement, Section 79 IT Act, Consumer Protection E-Commerce Rules, safe harbor, due diligence, notice and takedown, comparative law

Introduction

The rapid expansion of Indian e-commerce since about 2014 has produced a complex transactional environment in which brand owners, platforms, and consumers meet on digital infrastructure that operates at a national scale but serves highly fragmented seller groups. This expansion has been supported by mobile internet, Unified Payments Interface (UPI), aggressive marketplace discounting, and the entry of foreign capital, each of which has encouraged individual sellers to list goods without the kind of licensing control that brick-and-mortar distribution requires. The same features have also created fertile ground for counterfeiters, parallel importers, and grey-market operators who are able to reach a large audience quickly, hide behind weak disclosures, and disappear after a take-down. The policy challenge for Indian law is that it must at once reward digital trade, protect consumers from substandard or unsafe goods, and secure the statutory exclusivity that registered proprietors enjoy under the "Trade Marks Act, 1999".[1]

The tension between market growth and intellectual property enforcement is sharpened by the design of the intermediary safe harbour in "Section 79 of the Information Technology Act, 2000", which was designed at a time when platforms were expected to be passive conduits and not hybrid retailers that advertise, fulfil, warehouse, and rate goods. When a platform merely provides access, Indian law is willing to place all trademark liability on the actual seller or manufacturer. When a platform chooses to rank products, create premium storefronts, or extend authenticity guarantees, the assumption that it is a passive carrier begins to fail, and courts start to import trademark obligations into the platform's conduct.[2] The Delhi High Court decisions between

[1] Aaron Kamath, Abhishek Senthilnathan, et.al., "Intermediaries Under The Indian Information Technology Law Can Breathe A Sigh Of Relief", *available at:* https://nishithdesai.com/default.aspx?id=5027 (last visited on October 28, 2025).
[2] E-Commerce Platforms As An Intermediary Under The IT Act, 2000, *available at:* https://ksandk.com/information-technology/intermediary-under-the-it-act/ (last visited on October 27, 2025).

2017 and 2025 show a gradual movement from a model based on notice-and-takedown to a model that measures the character of the platform's intervention in the transaction, especially where luxury goods, direct selling products, or food and drug items are involved, and where consumer risk is high.

An added complexity comes from the co-existence of sectoral rules. The "Consumer Protection (E-Commerce) Rules, 2020" divide platforms into marketplace and inventory e-commerce entities and assign verification, disclosure, and grievance redressal duties that are independent of trademark complaints. At the same time, the 2023 update to the IT Rules has made safe harbour expressly conditional on compliance with due diligence, user identification, and traceability requirements, which means that every failure to collect seller data or to respond to rights-holder complaints can now be read against the platform when it seeks immunity. The present study argues that because counterfeit goods are by definition intended to deceive, Indian trademark law alone cannot deliver complete relief unless it is read together with the evolving intermediary regime, the new criminal codes, and data protection provisions that compel platforms to preserve and share identity trails of infringing sellers.[3]

Research Questions

The research proceeds on the premise that the key controversy is whether Indian law at present creates primary liability for an online marketplace when a third-party seller lists counterfeit goods or whether such liability is only secondary, triggered by knowledge, control, or profit participation. The first question asks whether the combined effect of "Sections 27 to 29 of the Trade Marks Act, 1999" and "Section 79 of the Information Technology Act, 2000" is to treat the marketplace as a principal infringer or as a contributory actor once it has been notified of the infringing listing. The second question tests if the safe harbour continues to apply when the marketplace abandons neutrality and becomes an organiser of the sale by warehousing, packaging, advertising, and sometimes even issuing invoices in its own name, which is a pattern now common in fulfilment models and in hybrid inventory models in India. These questions are meant to clarify for rights holders, platforms, and regulators the precise moment when safe harbour ends and trademark exposure begins.[4]

Problem Statement

Platform liability for online counterfeits in India is still uncertain because trademark law speaks in terms of persons who apply or falsify marks, while the IT regime speaks of entities that host third-party information, and neither statute, read alone, squarely answers who bears responsibility when a counterfeit handbag or cosmetic is sold through a curated marketplace. Enforcement practice shows gaps in seller traceability, in consistency of takedown timelines, and in the articulation of due diligence across the "IT Rules 2021" and the "Consumer Protection (E-Commerce) Rules 2020", which results in uneven remedies for brand owners and confusion for platforms that operate multiple business models.[5]

Objectives of the Study

The first objective is to construct a map of the statutory, regulatory, and judicial sources that presently govern the liability of e-commerce platforms in India for counterfeit and look-alike goods, with particular attention to "Sections 27, 28, 29, 101, 102, 103 and 135 of the Trade Marks Act, 1999", "Section 79 of the Information Technology Act, 2000", the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" as updated in 2023, and the "Consumer Protection (E-Commerce) Rules, 2020". The second objective is to suggest a compliance and enforcement model that makes use of statutory notice-and-takedown, contractual seller onboarding, and, where necessary, recourse to criminal provisions on counterfeit property marks under the "Bharatiya Nyaya Sanhita, 2023", together with the evidentiary presumptions for electronic records in the "Bharatiya Sakshya Adhiniyam, 2023", so that rights owners can secure both private and public law remedies.[6]

Research Methodology

The study employs doctrinal legal research based on close reading of statutes, rules, notifications, and reported Delhi High Court and Supreme Court decisions on intermediary liability and counterfeit trade as available up to November 2025, with particular emphasis on cases concerning luxury brands, direct selling products, and platform criminal exposure. Comparative references are drawn from European Union online intermediary rules and from the approach to marketplace counterfeit liability in the United States, but only as contextual material and not as controlling authority. The analysis is qualitative and source-driven, with no empirical survey component.[7]

[3] P. Narayanan, *Law of Trade Marks and Passing Off* 142 (Eastern Law House, Kolkata, 1st edn., 2018).
[4] Christian Louboutin SAS v. Nakul Bajaj And Ors., *available at:* https://sflc.in/policies-and-cases/christian-louboutin-sas-v-nakul-bajaj-and-ors/ (last visited on October 26, 2025).
[5] Avtar Singh, *Consumer Protection Law and Practice* 167 (Eastern Book Company, Lucknow, 1st edn., 2019).
[6] The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited on October 25, 2025).
[7] Pavan Duggal, *Cyber Law: An Exhaustive Section-Wise Commentary on the Information Technology Act* 93 (LexisNexis, New Delhi, 1st edn., 2023).

Statutory Framework in India

The liability of e-commerce platforms for counterfeit goods in India cannot be located in a single enactment, because the Trade Marks Act creates substantive civil and criminal remedies for infringement and falsification, while the IT Act and its rules create conditional immunity for hosts of third-party information, and consumer rules create authenticity and disclosure duties that indirectly reinforce trademark interests. The framework is further strengthened by the new criminal codes that replaced the IPC and CrPC from 1 July 2024, so that offences about false property marks now fall under the "Bharatiya Nyaya Sanhita, 2023" and investigative and search procedures fall under the "Bharatiya Nagarik Suraksha Sanhita, 2023".[8] Since counterfeit listings often require the production and preservation of electronic evidence, the "Bharatiya Sakshya Adhiniyam, 2023" becomes relevant for admitting screenshots, metadata, and platform logs, and the "Digital Personal Data Protection Act, 2023" is relevant to the extent platforms collect, process, and share seller identity data with brand owners or enforcement agencies.[9] This mix of IP, IT, consumer, criminal, evidence, and data-protection norms means that platforms must satisfy several parallel duties before they can safely plead intermediary status.

Trade Marks Act 1999

The "Trade Marks Act, 1999" grants to a registered proprietor the exclusive right to use the mark in relation to goods or services and to seek relief against infringement under "Section 28" and "Section 29". In the context of e-commerce, the mischief normally falls under "Section 29(1)" and "Section 29(2)" because counterfeiters tend to use identical or deceptively similar marks on identical or similar goods, which creates a clear likelihood of confusion. The Act preserves passing off actions for unregistered marks through "Section 27(2)", which is valuable in digital marketplaces where unregistered brands also face copycat listings. Civil remedies of injunction, account of profits, damages, delivery up, and such incidental reliefs are provided under "Section 135", and these are the primary civil tools that brand owners invoke when they seek takedown directions and information disclosure against a platform. Counterfeiting in the criminal sense is addressed through "Section 102", which targets falsifying and falsely applying a trade mark to goods or services, and this is supplemented by punitive provisions in "Sections 103 to 105" imposing imprisonment and fines. These provisions continue to be the first statutory port of call when sellers on e-commerce portals are found manufacturing or distributing spurious goods, and the Delhi High Court has not read them as ousting civil remedies merely because the sale occurred online.[10]

Information Technology Act 2000

The "Information Technology Act, 2000" defines an intermediary in "Section 2(1)(w)" to mean any person who on behalf of another person receives, stores, or transmits a message or provides any service with respect to that message, and this broad definition easily captures marketplace e-commerce entities that host seller-generated listings. Safe harbour is provided by "Section 79", which exempts intermediaries from liability for third-party information, data, or communication links made available or hosted by them, provided that the intermediary's function is limited to such enabling and it observes due diligence and complies with government or court directions for takedown on obtaining actual knowledge. This protection is withdrawn under "Section 79(3)" where the intermediary has conspired, abetted, or aided or induced the commission of an unlawful act, or upon receiving actual knowledge fails to expeditiously remove or disable access to the material. The difficulty with counterfeit goods is that brand owners often discover infringing listings through their own market watch and not through government or court orders, leading to the question whether such private notice amounts to actual knowledge. After "*Shreya Singhal v. Union of India*[11], read down the concept of actual knowledge to require government or court directives for generic speech takedowns, platforms argued that they were not bound to respond to every IP complaint. The Delhi High Court in IP and e-commerce disputes has tended to read "Section 79" contextually and has treated specific, URL-based counterfeiting complaints as sufficient to trigger platform action, especially where the complaint is supported by proof of registration. This approach marks a move away from a rigid, order-based knowledge standard.[12]

Intermediary Due Diligence Rules

The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", as updated on 28 October 2022 and on 6 April 2023, make the enjoyment of safe harbour under "Section 79" conditional on compliance with due diligence obligations, such as publishing rules and privacy policies, removing content on actual knowledge, enabling identification of first originator in specified cases, and running a responsive grievance mechanism. For e-commerce platforms, the most relevant requirements are the obligation to inform users not to host or share material that infringes patents, trademarks, or other proprietary rights, to remove such material on actual knowledge, and to retain and furnish registration or identification records to lawful authorities. Rule changes of 2023 make it clear that intermediaries must act on grievances in a time-bound manner and that failure to do so leads to loss of safe harbour. Because counterfeit goods usually involve repeat or related sellers, these rules provide a statutory path for brand

[8] Police 'Pathshalas' To Explain Legal Reforms, *available at:* https://maharashtratimes.com/e-paper/2025/nov/1-november-2025/police-pathshalas-to-explain-legal-reforms/articleshow/125004923.cms (last visited on October 24, 2025).
[9] The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on November 2, 2025).
[10] Venkateswaran, *Trade Marks and Passing-Off* 201 (LexisNexis, Gurgaon, 1st edn., 2019).
[11] (2015) 5 SCC 1.
[12] Flipkart Internet Private Limited v. State Of NCT Of Delhi And Anr, *available at:* https://globalfreedomofexpression.columbia.edu/cases/flipkart-internet-private-limited-v-state-of-nct-of-delhi-and-anr/ (last visited on November 1, 2025).

owners to demand IP-specific action and for governmental authorities to require disclosure of seller identities for prosecution under the "Bharatiya Nyaya Sanhita, 2023".

Consumer Protection E-Commerce Rules 2020

The "Consumer Protection (E-Commerce) Rules, 2020" apply to all e-commerce entities offering goods or services to consumers in India, and they distinguish clearly between marketplace and inventory models. Marketplace e-commerce entities must, among other duties, display details about sellers, ensure that information relating to return, refund, warranty, delivery, and grievance redressal is clear, and require sellers to guarantee that descriptions and images are not misleading. Inventory e-commerce entities that own the inventory and sell directly to consumers bear direct responsibility for authenticity and quality and are treated in effect like ordinary sellers. The rules require that the platform's name and contact detail of the grievance officer be displayed and that grievances be resolved within one month, giving trademark proprietors an additional procedural forum when a counterfeit listing harms consumer interest. Since many counterfeits in India involve misdeclaration of origin or health compliance, these rules, when read with the 2025 proposal to make country-of-origin filters mandatory, increase the disclosure burden that e-commerce platforms must shoulder.[13]

Marketplace e-commerce entity (Rules 5 and 6)[14]	Must provide accurate seller details, ensure contract between seller and consumer is clear, display information on return/refund/warranty, establish grievance redressal, and take down goods where seller information is incomplete or misleading.
Inventory e-commerce entity (Rule 7)	Treated as seller for all purposes, must not list counterfeit or unsafe goods, must honour warranties and guarantees, and is directly liable for authenticity, misdescription, and non-compliance with Indian law.

Table 1: Marketplace vs Inventory E-Commerce Obligations under "Consumer Protection (E-Commerce) Rules, 2020"

Intermediary Liability Tests under Indian Law

Indian courts, particularly the Delhi High Court, have developed a set of tests to decide whether an e-commerce platform in a trademark dispute is entitled to safe harbour or has crossed into the zone of primary liability. These tests are grounded in statutory language but shaped by fact patterns in the digital marketplace. They consider, first, whether the platform had actual or specific knowledge of a counterfeit listing and, second, whether the platform played an active role in the transaction. A third dimension is the tension between the need for proactive filtering and the statutory assurance in "Section 79" that intermediaries will not be forced to carry out general monitoring. Finally, courts also evaluate whether the facts justify criminal process or whether safe harbour should protect the intermediary from FIRs for trademark offences, particularly those now falling under the "Bharatiya Nyaya Sanhita, 2023".

Actual or Specific Knowledge

"*Shreya Singhal v. Union of India*[15], confined actual knowledge for speech takedowns to government or court orders, but trademark disputes presented a more concrete problem, because platforms regularly receive rights-holder notices that identify exact URLs and trademark numbers and the infringing goods are identifiable at sight. Delhi High Court copyright jurisprudence, especially "*MySpace Inc. v. Super Cassettes Industries Ltd*[16], moved towards a specific knowledge standard, holding that an intermediary that is given a detailed notice of infringing content and the means to locate it cannot claim ignorance and must disable access within a reasonable time. This logic has been extended in e-commerce disputes: where the trademark owner has provided registration details, screenshots, and seller names, platforms are expected to act even in the absence of a court order, and failure to act exposes them to loss of safe harbour under "Section 79(3)". This position aligns with the 2021 and 2023 IT Rules, which require intermediaries to act on user grievances within fixed timelines, making specific knowledge a workable trigger for action.

Active vs Passive Role

A key determinant for liability is whether the platform has remained passive or has engaged in conduct that shows control over the manner in which the goods are displayed, priced, sold, or delivered. Where the platform merely hosts listings and passes buyer details to sellers, courts have leaned towards preserving safe harbour. Where the platform selects and onboards sellers, advertises the goods using the trademark, offers authenticity guarantees, warehouses the goods under a fulfilment service, ships in its own packaging, or receives payment before remitting to the seller, courts have inferred an active role and treated the platform as more than a conduit, which raises the platform's exposure under both the Trade Marks Act and the Consumer Protection E-Commerce Rules. This was the reasoning that animated the decision in "*Christian Louboutin SAS v. Nakul Bajaj*[17], which held that a luxury reseller that promoted branded goods, charged a commission, and offered to authenticate could not hide behind "Section 79".

---

[13] Dipak K Dash, "Centre Proposes 'Country Of Origin' Filter On E-Commerce Sites", *available at:* https://timesofindia.indiatimes.com/business/india-business/centre-proposes-country-of-origin-filter-on-e-commerce-sites/articleshow/124854628.cms (last visited on October 31, 2025).
[14] B. L. Wadhera, *Law Relating to Intellectual Property* 154 (Universal Law Publishing, Delhi, 1st edn., 2014).
[15] *Supra* note 11.
[16] 2017 SCC OnLine Del 10749.
[17] AIRONLINE 2018 DEL 1962.

Proactive Filtering vs No General Monitoring

Indian courts have been cautious not to impose a general monitoring obligation on intermediaries, recognising that such a duty would make online trade unworkable and would conflict with the legislative intent behind "Section 79". The Delhi High Court in "*Kent RO Systems Ltd v. Amit Kotak*[18], rejected the plea that e-commerce platforms must screen every product for IP infringement before displaying it, holding that intermediaries cannot be expected to police all content in advance and that their primary duty is to act once they gain specific knowledge of infringing listings.[19] At the same time, Indian courts have not hesitated to direct proactive steps in narrow statutory settings, such as in "*Sabu Mathew George v. Union of India*[20], on advertisements violating the Pre-Conception and Pre-Natal Diagnostic Techniques Act, where monitoring was justified by an overriding public interest. The result is a balanced position: e-commerce platforms selling ordinary goods are not subject to general monitoring, but when the goods are sensitive or when the platform has repeatedly allowed infringing sellers to reappear, courts can insist on keyword blocks, seller verification, or tighter onboarding even without express statutory text.

Criminal Exposure

Criminal complaints have been filed against e-commerce platforms for alleged sale of counterfeit or misdeclared goods, often invoking the penal sections of the Trade Marks Act alongside cheating or fraud provisions, which after July 2024 require reference to the "Bharatiya Nyaya Sanhita, 2023". Courts have applied "Section 79" to such criminal allegations as well, holding that where the platform has played no active role and has acted promptly on takedown requests, criminal investigation or prosecution would result in injustice. The Delhi High Court order in "*Flipkart Internet Pvt Ltd v. State of NCT of Delhi*[21], quashed the FIR that alleged offences under "Sections 103 and 104 of the Trade Marks Act, 1999" and under copyright law, noting that Flipkart was an intermediary entitled to safe harbour and that the complaint did not show conspiracy or inducement. After the coming into force of the "BNS, 2023", similar conduct would be examined under provisions on counterfeit property marks such as "Section 349 of the Bharatiya Nyaya Sanhita, 2023" read with BNSS search and seizure rules, but the underlying logic remains the same: without active participation or specific knowledge, criminal liability should not attach to the platform.[22]

Indian Case Law on Platform Liability for Counterfeits

Indian jurisprudence on platform liability has been shaped largely by Delhi High Court decisions because most major e-commerce operators and brand owners litigate in Delhi. The decisions discussed below mark the key stages of doctrinal development: recognition of active-role liability in luxury resale, affirmation of non-mandatory ex ante screening, reassertion of safe harbour in criminal matters, clarification of the non-binding character of sectoral executive guidelines, and, finally, the 2025 litigation on Beverly Hills Polo Club that signalled the scale of damages that large platforms could face when courts find infringement. Together, these rulings show that while safe harbour remains central, it is not unconditional, and it yields in the face of platform conduct that imitates that of a seller.[23]

Christian Louboutin Sas v. Nakul Bajaj (Darveys)

"*Christian Louboutin SAS v. Nakul Bajaj*[24], arose from a suit filed by the proprietor of the well-known luxury brand against an online platform, Darveys.com, which styled itself as a facilitator for the sale of premium goods sourced from abroad and delivered to Indian customers. The plaintiff's case was that its registered trademarks, including the word mark and the famous red sole, were being used on the defendant's website without authorisation to promote products that were either counterfeit or were not authorised for distribution in India. The defendant contended that it was only an intermediary that connected members to foreign boutiques, and that it did not itself sell or warehouse the goods, and for this reason it claimed protection under "Section 79 of the Information Technology Act, 2000". The court noted that the website did not function like a neutral notice board but carried elaborate descriptions, images, and meta tags of the plaintiff's marks and offered Indian consumers the comfort of a localised interface.

The court examined the actual operations of Darveys.com and found that the platform was not a passive facilitator. It charged membership fees, it advertised that it could procure goods from abroad, it represented that the goods were genuine, and it used the plaintiff's trademarks not only for identifying goods but also for attracting consumers to the site. It also handled customer queries and complaints, and in some instances was involved in delivery. These features convinced the court that the defendant was playing an active role in enabling the sale of the allegedly infringing goods and was, therefore, not entitled to claim the benefit of safe harbour that is available only to intermediaries who perform a technical, automatic, and passive role. The court stressed that once a platform projects itself as a trusted source for branded luxury products and offers value-added services, it assumes a duty to verify the authenticity of the goods and to disclose the identity of the sellers from whom the goods are sourced.

---

[18] 2017 SCC OnLine Del 7201.
[19] Case Analysis : Kent RO Systems Ltd. & Anr. v. Amit Kotak & Ors, *available at:* https://blog.ipleaders.in/case-analysis-kent-ro-systems-ltd-anr-v-amit-kotak-ors/ (last visited on October 30, 2025).
[20] (2016) 14 SCC 434.
[21] WP(Crl) 1376 of 2020, 17 Aug 2022.
[22] Arrangement Of Sections—Chapter XVIII Of Property Marks: Section 349, *available at:* https://kanoongpt.in/bare-acts/the-bharatiya-nyaya-sanhita-2023/arrangement-of-sections-chapter-xviii-of-property-marks-section-349-38ee139d21a6567e (last visited on October 29, 2025).
[23] P. Narayanan, *Law of Trade Marks and Passing Off* 176 (Eastern Law House, Kolkata, 1st edn., 2018).
[24] *Supra* note 17.

In assessing liability, the court referred to the scheme of the "Trade Marks Act, 1999", especially "Sections 101 and 102" on the meaning of applying trademarks and on falsifying marks. It observed that whoever sells, offers or exposes for sale, or has in possession for sale, goods or things to which a false trade mark or false trade description is applied, is deemed to apply such mark or description and is therefore within the mischief of the Act. Since the defendant's site was the point of sale from the consumer's viewpoint and the defendant gained commercially from each sale, the court treated it as a seller for the purposes of the Act even if the physical goods moved from a third-party source. It directed the platform to take down infringing listings, to obtain guarantees of authenticity from sellers, and to disclose complete seller details to the plaintiff. This set of directions was aimed at making the platform more accountable and at creating a trail for enforcement under both civil and criminal law.

The judgment is notable for refusing to shield the platform behind the argument that monitoring every luxury good would be impossible. The court accepted that intermediaries cannot be compelled to screen all content in every circumstance but pointed out that when a platform decides to operate in a high-value, high-risk segment such as luxury fashion, it must raise its due diligence standards accordingly and must not wait for repeated complaints. The court also approved a set of due diligence measures, such as requiring sellers to enter into proper agreements, obtaining invoices and certificates of authenticity, providing details of sellers on the platform, and allowing trademark owners to flag infringing products, measures that have since been treated as a kind of compliance checklist for e-commerce operators dealing in branded goods. In effect, the court read trademark obligations into the operations of a commercial e-commerce site and limited the scope of "Section 79" in the presence of an active role.

The Darveys ruling therefore brought Indian law closer to the view that safe harbour is not a blanket immunity but a conditional protection that depends on the actual functions performed by the online intermediary. For the present study, this case is critical because it supplies the analytical bridge between the statutory text of "Section 79" and the business realities of platform commerce, and it demonstrates that courts are willing to pierce platform design and commercial arrangements to determine liability.

Kent Ro Systems Ltd v. Amit Kotak, and Kent Ro v. eBay India

"*Kent RO Systems Ltd v. Amit Kotak*[25], concerned the sale of spare parts and cartridges bearing the plaintiff's mark on online platforms, including eBay, without the plaintiff's authorisation. The plaintiff argued that the intermediaries were obliged to verify each and every listing before allowing it to go live, because counterfeit or substandard water purifier parts could cause consumer harm and dilute the brand. The intermediaries responded that they were entitled to the protection of "Section 79 of the Information Technology Act, 2000", that it was technologically and commercially infeasible to pre-screen every product description, and that their obligation, if any, arose only when the plaintiff notified them of a specific infringing listing. The court accepted the intermediary position and framed the issue as one of specific knowledge rather than general duty.

The court held that the IT Act read with the then applicable "Information Technology (Intermediaries Guidelines) Rules, 2011" did not cast an obligation on intermediaries to monitor, screen, or verify the legitimacy of every item that a third party wished to list on the platform. It referred to "Section 79(2)(c)" to observe that intermediaries are required to remove or disable access to content only on receiving actual knowledge or on being notified by the appropriate government agency or by an order of a court. It emphasised that imposing a pre-screening obligation would defeat the very objective of the Act, which was to promote the growth of e-commerce. At the same time, the court clarified that once an intermediary is informed about a specific instance of infringement and is given the exact URL or listing details, it is duty-bound to take down the content within the time prescribed under the rules, failing which it may lose the benefit of safe harbour.[26]

The judgment also addressed the plaintiff's reliance on foreign precedents and on the argument of contributory infringement. The court noted that an intermediary could be said to have abetted or induced infringement only if there was material to show active participation, knowledge of infringing activity, or financial interest in the infringement beyond ordinary commission. Since the plaintiffs had not pleaded conspiracy or specific inducement on the part of the intermediaries, the court found no ground to deny them safe harbour at the interim stage. It therefore refused to grant a blanket injunction compelling e-commerce platform to remove all listings of Kent RO products and left the question of knowledge and participation to be examined at trial on the basis of evidence.[27]

This ruling created a counterweight to Darveys by reaffirming that ordinary marketplaces, which do not project themselves as authenticators and which act promptly on takedown requests, should not be forced into the role of trademark police. It also established the template for URL-specific notices, which has since become standard practice in IP enforcement against platforms. The court's approach anticipated the specific knowledge standard later discussed in MySpace and showed that Indian courts were willing to differentiate between high-involvement luxury platforms and high-volume general platforms. The case therefore remains important for establishing that ex ante screening is not a default obligation for e-commerce intermediaries.[28]

[25] *Supra* note 18.
[26] Kent RO Ltd & Anr. v. Amit Kotak & Ors., *available at:* https://sflc.in/policies-and-cases/kent-ro-ltd-anr-v-amit-kotak-ors/ (last visited on October 28, 2025).
[27] Kent RO System Ltd. v. Amit Kotak, *available at:* https://lawbhoomi.com/kent-ro-system-ltd-v-amit-kotak/ (last visited on October 27, 2025).
[28] E-Commerce Websites Are Not Bound To Keep A Check On Products For IP Infringement Before Advertising On Their Website, *available at:* https://www.scconline.com/blog/post/2017/03/04/e-commerce-websites-are-not-bound-to-keep-a-check-on-products-for-ip-infringement-before-advertising-on-their-website/ (last visited on October 26, 2025).

Amazon Seller Services v. Amway India Enterprises

"*Amazon Seller Services Pvt. Ltd v. Amway India Enterprises Pvt. Ltd*[29], came to the Delhi High Court as an appeal from a single judge order that had effectively restrained online platforms from listing products of direct selling entities such as Amway, Oriflame, and Modicare without the express consent of those entities. The direct selling entities relied on the Direct Selling Guidelines, 2016 issued by the Department of Consumer Affairs and argued that their business model depended on a closed network of authorised distributors and that unauthorised online sale violated their contractual and trademark rights. The platforms contended that the guidelines were advisory, not statutory, and that goods which were lawfully purchased could be resold online in the absence of a specific statutory prohibition. The division bench framed the central question as whether executive guidelines could be enforced against platforms so as to restrict their ability to host third party listings.[30]

The court held that the Direct Selling Guidelines were not law and did not have binding effect on e-commerce platforms. It observed that in the absence of a statutory embargo on resale, the mere fact that the direct selling entities had chosen a particular distribution model could not prevent buyers or even distributors from reselling genuine products on online marketplaces. To that extent, the court set aside the single judge's directions and clarified that platforms were entitled to host such listings subject to other applicable laws. This finding was important for trademark law because it made it clear that control over distribution channels cannot by itself be equated with trademark infringement when the goods being sold are genuine and are not materially altered. The court did, however, direct platforms to maintain robust disclosure and grievance redressal systems so that complaints of counterfeit or tampered products could be addressed quickly.[31]

In its reasoning, the division bench also referred to "Section 79 of the Information Technology Act, 2000" and noted that so long as platforms remain neutral and act on specific complaints, they continue to enjoy safe harbour. It took note of the fact that Amazon and other appellants were large marketplaces operating on the marketplace model prescribed under the "Consumer Protection (E-Commerce) Rules, 2020", which emphasise disclosure and due diligence rather than pre-clearance of every listing. In view of this regulatory scheme, the court saw no justification for imposing a prior-consent requirement flowing from non-binding executive guidelines. This approach avoided stretching trademark rights to cover all forms of unauthorised online resale and preserved the distinction between counterfeit and grey-market goods. The decision therefore marked an important moment in keeping platform liability within statutory boundaries.[32]

Hamdard National Foundation v. Amazon

"Hamdard National Foundation (India) v. Amazon India"[33] concerned the listing on Amazon's Indian platform of Rooh Afza products that originated from Pakistan and were not manufactured by the Indian plaintiffs who owned the "ROOH AFZA" trademark in India. The plaintiffs contended that the listings created confusion in the market, violated their trademark rights, and raised public health concerns because the imported products did not comply with Indian regulatory standards. Amazon argued that it was an intermediary, that the products were listed by third-party sellers, and that it had taken down specific URLs when notified. The Delhi High Court, per Prathiba M. Singh J., took a strict view, noting that the platform was dealing with food products consumed widely in India and that confusion about source and regulatory clearance could not be permitted. It therefore granted a permanent injunction restraining the listings of products not originating from the plaintiffs and directed Amazon to take down all such listings.[34]

The court reasoned that when a platform is informed that certain goods bearing a registered trademark are not originating from the registered proprietor and may not be meeting Indian standards, the platform is bound to act with greater care than it would in the case of an ordinary IP complaint. It placed reliance on the platform's own policies, which required sellers to comply with Indian law and to provide accurate information about country of origin. Since the platform had the technical ability to de-list specific sellers and to prevent re-listing of the same goods under different seller names, the court required it to do so. The order demonstrates a situation where even a marketplace that is otherwise entitled to safe harbour can be directed to act proactively to prevent future infringements once the court is satisfied that there is a risk of recurring infringement that affects consumers directly.[35]

This decision is significant because it connects trademark enforcement with consumer protection and regulatory compliance. The court's directions ensured not only that the plaintiffs' trademark rights were protected, but also that Indian consumers would not buy a food product that had not been cleared for sale in India. The logic of the case aligns with the "Consumer Protection (E-Commerce) Rules, 2020" which require e-commerce entities to provide accurate information and to take down goods that are offered by sellers who do not meet statutory requirements. It also illustrates that in goods

[29] FAO(OS) 133, 134, 135 of 2019, order dated 31 Jan 2020.
[30] Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors., *available at:* https://cyberblogindia.in/amazon-seller-services-pvt-ltd-v-amway-india-enterprises-pvt-ltd-ors/ (last visited on October 25, 2025).
[31] Delhi High Court: Direct Selling Guidelines Advisory In Nature And Not Binding As A Law, *available at:* https://www.agarwaljetley.com/delhi-high-court-direct-selling-guidelines-advisory-in-nature-and-not-binding-as-a-law.html (last visited on October 24, 2025).
[32] Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors., *available at:* https://taxguru.in/wp-content/uploads/2020/02/Amazon-Seller-Services-Pvt.-Ltd.-Vs-Amway-India-Enterprises-Pvt.-Ltd.-Ors.-Delhi-High-Court.pdf (last visited on November 2, 2025).
[33] 2022 SCC OnLine Del 4807 (Delhi H.C.).
[34] Hamdard National Foundation (India) & Anr v. Amazon India Ltd. & Anr., *available at:* https://lexmantis.com/2022/11/30/hamdard-national-foundation-in-anr-v-s-amazon-india-ltd-anr/ (last visited on November 1, 2025).
[35] High Court: Amazon Directed To Remove ROOH AFZA Branded Products Not Originating From Hamdard India, *available at:* https://www.candcip.com/single-post/high-court-amazon-directed-to-remove-rooh-afza-branded-products-not-originating-from-hamdard-india (last visited on October 31, 2025).

affecting health or public faith, courts are prepared to treat platforms as active participants once they are put to notice, and they may order ongoing vigilance even though "Section 79" does not create a general monitoring duty.

Flipkart Internet Pvt Ltd v. State of NCT of Delhi

"*Flipkart Internet Pvt Ltd v. State of NCT of Delhi*[36], involved an FIR lodged against Flipkart for alleged sale of counterfeit cosmetics through its platform, invoking, among other provisions, the penal provisions of the Trade Marks Act. Flipkart approached the Delhi High Court seeking quashing of the FIR on the ground that it was an intermediary entitled to the protection of "Section 79 of the Information Technology Act, 2000" and that it had a proper policy of seller onboarding, terms of use, and takedown. The respondent argued that the platform had promoted the impugned products and had therefore taken an active role. The court examined the operational model of Flipkart and found that the impugned goods were listed by third-party sellers, that Flipkart did not claim the goods to be genuine or to be supplied by it, and that on receiving a complaint Flipkart had removed the listings. It therefore held that continuation of criminal proceedings would result in abuse of the process of law.

The court reiterated that "Section 79" extends to criminal liability as well, and that an intermediary should not be subjected to prosecution merely because an infringing or counterfeit product was found to have been listed on its platform, unless there is material to show that the intermediary had conspired in the act or had failed to act after receiving actual knowledge. It observed that e-commerce platforms are facilitators that provide their digital space to numerous sellers and that some instances of infringement or violation may occur despite reasonable diligence. To hold the intermediary criminally liable in every such case would have a chilling effect on e-commerce. The court, therefore, quashed the FIR. This decision strengthens the proposition that loss of safe harbour is an exception, not the rule, and that courts will look carefully for evidence of active role before allowing the criminal law to proceed.[37]

The ruling is important for the present analysis because it confirms that when platforms have framed and enforced terms that prohibit infringement, have systems to receive and process complaints, and have responded to complaints in good time, they are entitled to claim statutory protection even against offences that have migrated to the "Bharatiya Nyaya Sanhita, 2023". It signals to enforcement agencies that criminal process should be directed primarily at the sellers who actually trade in counterfeit goods and not at the platforms, unless the platform's conduct shows collusion or wilful blindness.

Lifestyle Equities C.V. v. Amazon Technologies Inc.

"*Lifestyle Equities C.V. v. Amazon Technologies Inc.*[38], represents the most recent and commercially weighty dispute on platform liability. The plaintiffs, owners and licensees of the "Beverly Hills Polo Club (BHPC)" trademark, sued Amazon Technologies Inc. and related entities alleging large-scale infringement of their registered marks on the Amazon platform, claiming that the defendants had allowed sellers to offer BHPC-branded goods that were not authorised by the plaintiffs and that the platform's own algorithms and storefronts promoted these products to Indian consumers. The single judge of the Delhi High Court accepted several of the plaintiffs' contentions, found infringement, and awarded damages and costs of about Rs 339 crore, reflecting the scale of the alleged infringing business.[39]

The judgment signalled a strong judicial willingness to impose substantial monetary consequences on a global platform where evidence shows that infringing goods were widely available and that the platform's systems had materially contributed to their sale. The court took into account not only the presence of infringing listings but also the duration for which they remained online, the revenues generated, and the role of Amazon's fulfilment and promotional tools in lending visibility and credibility to the goods. In doing so, the court effectively treated Amazon as an entity that had crossed the line from passive intermediary to active participant, thereby forfeiting the benefit of "Section 79 of the Information Technology Act, 2000". The order resonated across the e-commerce sector because it demonstrated that Indian courts were prepared to assess and award very high damages where trademarks of well-known brands were repeatedly infringed on a platform.[40]

Amazon appealed, and on 1 July 2025 a division bench of the Delhi High Court stayed the operation of the damages order, noting that several questions required closer scrutiny, including the attribution of liability among various Amazon entities, the method of computing damages, and the extent to which platform-level tools could be equated with endorsement or sale of infringing goods.[41] The matter ultimately travelled to the Supreme Court, which on 24 September 2025 declined to interfere with the stay, which meant that Amazon was not required to pay the Rs 340 crore at that stage.[42] Even with the stay, the case is illustrative of the trajectory of Indian law: platforms can face massive financial exposure when they host counterfeit or unauthorised branded

[36] *Supra* note 21.
[37] Delhi High Court Judgment: 2022 DHC 3072, *available at:* https://supremetoday.ai/doc/judgement/IND_Delhi_2022_DHC_003072 (last visited on October 30, 2025).
[38] CS(COMM) 443/2020, order dated 25 Feb 2025, DB stay 1 Jul 2025.
[39] Lifestyle Equities CV & Anr. vs Amazon Technologies, Inc. on 25 February, 2025, *available at:* https://indiankanoon.org/doc/38072391/ (last visited on October 29, 2025).
[40] Procedure, Pleadings And Platforms: DHC's Stay In Amazon v. Lifestyle, *available at:* https://spicyip.com/2025/07/procedure-pleadings-and-platforms-dhcs-stay-in-amazon-v-lifestyle.html (last visited on October 28, 2025).
[41] Ritu Yadav, "Delhi HC Stays Rs 339 Cr Damages Order Against Amazon In Beverly Hills Polo Club Trademark Row", *available at:* https://lawbeat.in/news-updates/delhi-hc-stays-rs-339-cr-damages-order-against-amazon-in-beverly-hills-polo-club-trademark-row-1500462 (last visited on October 27, 2025).
[42] Indu Bhan, "Supreme Court Dismisses Lifestyle Equities' Appeal, Amazon Freed From Rs 340 Cr Trademark Penalty", *available at:* https://m.economictimes.com/news/company/corporate-trends/sc-rejects-lifestyle-equities-plea-amazon-technologies-escapes-rs-340-cr-trademark-damages/articleshow/124093635.cms (last visited on October 26, 2025).

goods at scale, when their business model involves curation and fulfilment, and when they fail to show rigorous compliance with the IT Rules and consumer rules.

For practitioners and scholars, the Lifestyle Equities litigation is important because it sits at the intersection of trademark law, intermediary safe harbour, and consumer-facing platform design. It shows that statutory compliance alone may not be enough if, on facts, the platform's conduct appears to promote or regularise infringing activity. It also shows that in the presence of detailed electronic evidence, which under the "Bharatiya Sakshya Adhiniyam, 2023" enjoys the status of primary evidence, courts are now able to quantify the economic effect of marketplace infringement with greater precision.[43]

Counterfeits vs Grey Market Goods

The emergence of e-commerce has exposed trademark law to two very different patterns of market behaviour that often get conflated in platform governance. One involves goods that never originated from the trademark proprietor or a licensee, on which a spurious mark has been applied, or an authentic mark has been falsified or falsely applied, bringing the matter squarely within "Section 29 read with Sections 101 to 105 of the Trade Marks Act, 1999" and, on the criminal side, within property-mark offences in "Sections 347 and 349 of the Bharatiya Nyaya Sanhita, 2023" for sale of goods bearing counterfeit property marks. Such goods break the chain of title at the very start and damage the indicator function of the mark. The other pattern involves genuine products that were first put on the market abroad with the trade mark owner's consent and then imported into India without local channel permission. That second situation is not about deception at origin and, as the Delhi High Court explained in "*Kapil Wadhwa v. Samsung Electronics Co. Ltd*[44], it travels through the doctrine of international exhaustion, subject to packaging, disclosure and warranty conditions. Platforms that collapse these two categories into one risk over-takedown, exposure to seller claims, and inconsistency with "Rule 5(5) and 5(6) of the Consumer Protection (E-Commerce) Rules, 2020" which expects record-keeping on repeat infringers but not an embargo on lawful trade. A careful legal analysis of listings, product identifiers, images, and seller declarations therefore becomes essential for an e-commerce marketplace that seeks to retain "Section 79 of the Information Technology Act, 2000" safe harbour while honouring trademark exclusivity.[45]

International Exhaustion and Parallel Imports

International exhaustion accepts that once a trademarked good is lawfully put in the market anywhere in the world by or with the consent of the proprietor, the trademark right in relation to that particular article is exhausted, subject to limited grounds of opposition such as impairment or legitimate reasons under "Section 30(4) of the Trade Marks Act, 1999". The Delhi High Court in "*Kapil Wadhwa v. Samsung Electronics Co. Ltd*[46], treated India as following international, not national, exhaustion, which means that parallel importers of genuine Samsung printers could not be stopped merely because the manufacturer operated an exclusive distributor model in India, though the court insisted on clear disclosure that the goods were imported, that Samsung India warranties might not apply, and that after-sales service terms could differ. This is a fundamentally different legal posture from counterfeiting, since the imported good physically embodies the proprietor's goodwill and quality control; the complaint, if any, is about circumvention of territorial segmentation, not consumer deception. A marketplace that receives a takedown notice from a brand for parallel imports must therefore test the assertion against "Section 30 of the Trade Marks Act, 1999" and against the user's right to resell lawfully acquired goods, instead of granting automatic removal. When the listing truthfully states country of origin, warranty status, and condition, and the packaging has not been materially altered, the platform can treat the listing as presumptively legitimate while still offering the brand a fraud-reporting channel. This approach stays aligned with "Rule 4 and Rule 6 of the Consumer Protection (E-Commerce) Rules, 2020" on transparent disclosures, now read together with the grievance and data-retention requirements in "Sections 12 to 16 of the Digital Personal Data Protection Act, 2023" which require that personal and transactional data used to verify seller identity or to respond to a future complaint be processed lawfully and stored only as long as required.[47]

Practical Distinction for Platforms

Operationally, a marketplace must separate investigations into spurious goods that infringe "Section 102 read with Sections 103 to 105 of the Trade Marks Act, 1999" from routine checks on genuine parallel imports that turn on exhaustion, labelling and warranty disclosure. A counterfeit investigation begins by matching the listing's mark, images and packaging to genuine SKUs, checking for obvious price anomalies, querying seller invoices, and looking for serial-number duplication. A parallel-import investigation begins by asking whether the goods were first put in the market with the proprietor's consent, whether the seller can show a legitimate supply chain, and whether repackaging or removal of quality-control codes has impaired the condition of the goods. Platforms need not monitor every listing in real time because "Section 79 of the Information Technology Act, 2000" together with "Rule 3 and Rule 7 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" permits reliance on notice-and-takedown, yet once credible notice is received the platform must act quickly or the safe harbour falls away. Where the platform records country-of-origin and warranty fields at the time of listing, the distinction becomes audit-friendly. Where the platform collects KYC and seller location under "Rule 5 of

[43] The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 25, 2025).
[44] FAO(OS) 93/2012, decided on 27 April 2012 (Del HC).
[45] The Trade Marks Act, 1999, *available at:* https://www.indiacode.nic.in/bitstream/123456789/15427/1/the_trade_marks_act%2C_1999.pdf (last visited on October 24, 2025).
[46] *Supra* note 44.
[47] Kapil Wadhwa & Ors. vs. Samsung Electronics Co. Ltd.: Legal Case Overview, *available at:* https://brieflaws.com/case-briefs/kapil-wadhwa-and-ors-vs-samsung-electronics-co-ltd (last visited on November 2, 2025).

the Consumer Protection (E-Commerce) Rules, 2020", parallel-import sellers can be tagged as higher risk for repeat disclosures but not treated as infringers unless the brand shows impairment or misrepresentation. In counterfeiting, by contrast, repeat participation is itself a red flag that can justify suspension, data sharing with enforcement under "Section 185 of the Bharatiya Nagarik Suraksha Sanhita, 2023" on search of places suspected to contain forged or counterfeit goods, and preservation of electronic records under "Sections 62 and 63 of the Bharatiya Sakshya Adhiniyam, 2023".[48]

Aspect	**Counterfeit goods**	**Parallel imports (grey market)**	**Platform checks**
Source of goods	Not from proprietor or licensee; mark falsified or falsely applied under "Section 102 TM Act, 1999"	From proprietor or licensee abroad; sale in India after international exhaustion recognised in "*Kapil Wadhwa v. Samsung Electronics Co. Ltd*[49], FAO(OS) 93/2012 (Del HC)"	Capture invoices, serial numbers, packaging photos, and seller KYC
Legal trigger	Infringement under "Section 29" plus criminal exposure under "Sections 103-105 TM Act, 1999" and "Sections 347, 349 BNS, 2023"	Permitted unless condition impaired or disclosure false under "Section 30(4) TM Act, 1999"	Mandatory field for country of origin, warranty disclaimer, alteration report
Platform action	Immediate takedown, evidence preservation, report to enforcement through BNSS procedure	Keep listing live with disclosure; act only on brand-specific proof of damage or misrepresentation	Periodic audit, repeat-infringer flag, DPDP-compliant retention of seller data

Table 2: Counterfeit vs Parallel Import, legal tests and platform checks

Comparative Law

Foreign jurisprudence is persuasive for Indian e-commerce disputes because Indian platforms borrow business models, trust architectures and risk-control designs from global marketplaces, while Indian statutory law still places the main liability trigger inside the Trade Marks Act, 1999 and reserves platform due diligence for the IT and consumer frameworks. United States law entered the scene first with an intermediary defence based on knowledge and control, European Union law followed with a more structured view of active-platform conduct, and India, sitting between these poles, has to decide how much of each model is consistent with "Section 79 of the Information Technology Act, 2000", "Rule 5 of the Consumer Protection (E-Commerce) Rules, 2020" and criminal follow-through under BNS and BNSS. The attraction of comparative analysis is not ornamental here. It enables classification of platform practices into three baskets, namely passive hosting with prompt response, active optimisation that may attract liability, and inventory or fulfilment models that collapse the distance between seller and marketplace. It also makes clear that traditional trademark principles on likelihood of confusion and falsification have had to be re-read to fit user-generated listings. Indian doctrine can therefore take guidance from how foreign courts treated platform advertising, repeat-notice patterns, and bad-faith sellers, while still reserving to itself the power to add statutory clarity on secondary liability.[50]

United States

The United States Court of Appeals for the Second Circuit in "*Tiffany (NJ) Inc. v. eBay Inc.*[51], held that eBay could not be saddled with contributory trademark infringement simply because it knew in a general way that some sellers offered counterfeit Tiffany jewellery on the platform. The court insisted on specific knowledge of particular infringing listings or sellers and on a failure to take reasonable remedial steps after notice. This approach tracks the test in Inwood Laboratories for contributory infringement, even though the user here is a service provider, and it dovetails with a safe-harbour ethos similar to what India adopted in "Section 79 of the Information Technology Act, 2000". For Indian marketplaces the lesson is that general brand alerts or industry reports about the prevalence of fakes do not by themselves defeat safe harbour; the marketplace is expected to operate a notice-and-takedown system, to warn or suspend sellers named in a credible notice, and to keep documentary evidence of the steps taken. The American court also endorsed eBay's use of Tiffany marks to describe the availability of genuine goods, which parallels "Section 30(2)(d) of the Trade Marks Act, 1999" that protects honest use to indicate the kind, quality or other characteristics of goods. In an Indian dispute a platform can therefore argue that keyword advertising, navigation pages, or category names that carry brand names are nominative and do not indicate source, provided the marketplace responds in good faith when a rights owner specifies a counterfeit listing.[52]

[48] V. K. Ahuja, *Law Relating to Intellectual Property Rights* 135 (LexisNexis, Gurgaon, 1st edn., 2017).
[49] *Supra* note 44.
[50] S. K. Verma, "Enforcement of Intellectual Property Rights: TRIPS Procedure & Remedies", 46 *Journal of the Indian Law Institute* 92 (2004).
[51] 600 F.3d 93 (2d Cir. 2010).
[52] Tiffany (NJ) Inc. v. eBay Inc., *available at:* https://en.wikipedia.org/wiki/Tiffany_%28NJ%29_Inc._v._eBay_Inc. (last visited on November 1, 2025).

European Union

The Court of Justice of the European Union in "*L' Oréal SA v. eBay International AG*[53], moved the conversation in a different direction by noting that an online marketplace may lose the status of a neutral host where it plays an active role in optimising the presentation of offers or in promoting them, for instance by assisting with keywords or by featuring preferred sellers. Once the platform moves into this active zone, the E-Commerce Directive safe harbour can be restricted and brand owners can obtain injunctions to prevent future infringements. This stands close to situations in India where a marketplace provides warehousing, packaging, or delivery under an inventory or fulfilment model and is then treated as an e-commerce entity with direct liability under "Rule 7 of the Consumer Protection (E-Commerce) Rules, 2020" rather than as a mere intermediary. The CJEU also placed weight on preventive measures: while the marketplace could not be asked to monitor all listings, it could be asked to put in place systems to identify and block sellers who had been found to infringe. That thinking is mirrored in India in "Rule 5(5)" which requires keeping records of repeat infringers for purposes of deactivation and coordination with law enforcement. The European approach therefore offers Indian regulators a precedent to argue that where the platform materially promotes or optimises infringing offers, the protective cloak of "Section 79 of the IT Act, 2000" may not be available.[54]

Synthesis

When these comparative strands are placed together, a convergence becomes visible around two ideas: there is no obligation of general monitoring over every listing, and liability should begin when the platform has actual or very specific constructive knowledge about an infringing offer and does not react proportionately. Divergence arises on what counts as active participation and on the nature of remedies. The United States leans towards a narrow contributory-liability test tied to specific notice. The European Union recognises injunctions and broader preventive orders once the marketplace departs from a neutral role. India, with its combination of "Section 79 of the IT Act, 2000", "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" and "Consumer Protection (E-Commerce) Rules, 2020", can situate itself between these poles by insisting that once a trademark owner sends a notice with SKU, seller identity, screenshots and date, the marketplace must delist, preserve digital evidence under "Sections 62, 63 and 93 of the Bharatiya Sakshya Adhiniyam, 2023", and, where criminal trade-mark counterfeiting is involved, cooperate with seizure and search under BNSS. Remedies in India can therefore range from permanent injunction under the Trade Marks Act, through dynamic or rolling injunctions against future rogue seller IDs, to administrative action by the Central Consumer Protection Authority for failure to display accurate product information.[55]

Jurisdiction	**Liability trigger**	**Safe harbour or defence**	**Remedies available**
India	Specific notice of counterfeit or repeat infringer; active fulfilment or inventory role; violation of "Rule 5, Consumer Protection (E-Commerce) Rules, 2020"	"Section 79 IT Act, 2000" if due diligence under 2021 Rules and evidence preservation under BSA is shown	Injunction, dynamic blocking of seller IDs, damages or account of profits, CCPA directions
United States	Specific knowledge plus failure to act as in *Tiffany (NJ) Inc. v. eBay Inc.*[56],	Nominative fair use and absence of wilful blindness	Injunction limited to identified sellers, damages against primary infringers
European Union	Active role in optimising or promoting infringing offers as in "*L' Oréal SA v. eBay International AG*[57], Case C-324/09 (CJEU 2011)"	Hosting safe harbour when role is neutral	Injunctions, orders to prevent future infringing use, disclosure of seller data

Table 3: India, US, EU tests for marketplace liability and remedies

Compliance Playbook for Marketplaces

For an Indian marketplace that wants predictable outcomes when counterfeit claims surface, compliance must knit together trademark, IT, consumer and data-protection rules. The Trade Marks Act sets the primary standard by defining infringement and counterfeiting, while "Section 79 of the IT Act, 2000" supplies conditional immunity and the 2021 Rules prescribe what due diligence means in the digital space. Consumer law, through "Rule 5 and Rule 6 of the Consumer Protection (E-Commerce) Rules, 2020", requires up-to-date seller details, customer support contacts, and tracking of repeat offenders. The DPDP Act layers on a privacy obligation for the personal data of sellers, buyers and complainants. A marketplace compliance playbook therefore begins with internal governance, moves to contractual control over sellers, integrates a notice-and-takedown workflow, and ends with proactive tools that

[53] Case C-324/09, judgment of 12 July 2011 (CJEU).
[54] Case C-324/09, *available at:* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A62009CJ0324_SUM (last visited on October 31, 2025).
[55] G. B. Reddy, *Intellectual Property Rights and the Law* 158 (Gogia Law Agency, Hyderabad, 1st edn., 2020).
[56] *Supra* note 51.
[57] *Supra* note 53.

stop short of general monitoring. Every one of these elements strengthens the argument that the platform neither induced infringement nor continued to supply services to a seller it knew was infringing.[58]

Governance and Contracts

Strong governance starts with seller onboarding that collects verified identity, tax details, contact information and where necessary corporate documentation, so that each listing can be mapped to a real-world actor. "Rule 5(1)(d) and 5(5) of the Consumer Protection (E-Commerce) Rules, 2020" already expects marketplaces to keep records of sellers who have repeatedly offered infringing goods or whose listings have previously been disabled under the Trade Marks Act, 1999. This can be built into the seller terms as an authenticity warranty affirming that the seller owns or is authorised to sell the goods, that the goods are genuine and unaltered, and that the seller will indemnify the platform against trademark claims. Contracts can also reserve audit rights, empowering the platform to demand invoices, procurement records or even product samples in high-risk categories such as luxury goods, pharmaceuticals, automobile parts or electronics. Where the platform is large enough to appoint a compliance or grievance officer under the IT Rules, that officer can serve as the nodal point for trade mark owners. Linking these contractual mechanisms to DPDP-compliant notices ensures that personal data collected for KYC and audit is processed only for the stated purpose and retained for the period needed to meet "Section 17 of the DPDP Act, 2023" on storage limitation. This package of contracts, notices and audits proves to courts that the marketplace discharged the greater diligence expected from entities that profit from third-party sales.[59]

Notice and Takedown

A reliable notice-and-takedown system is the centrepiece of safe-harbour defence. The IT Rules require that on receiving actual knowledge through a court order or through a notification from the appropriate government, the intermediary must take down the impugned content expeditiously, failing which "Section 79(1) of the IT Act, 2000" will cease to protect it. Marketplaces can extend this logic to private notices from trademark owners, especially when the notice carries the registration number, photographs of the genuine product, screenshots of the infringing listing, and a declaration of good faith. The marketplace then delists the product, informs the seller, preserves listing data, transaction logs and communications for evidentiary purposes under "Sections 62, 63 and 93 of the Bharatiya Sakshya Adhiniyam, 2023", and offers the seller a counter-notice channel. BNSS search-and-seizure provisions permit the police to obtain these records, and platforms should be ready to supply them through audio-video recorded procedures referenced in "Section 105 and Section 185 of the BNSS, 2023". A clear SLA-driven workflow also helps the marketplace show consumer regulators that dispute resolution was timely, which is material in view of the CCPA's recent advisory on self-audit of dark patterns and disclosure practices.[60]

Proactive Risk Controls

Proactive controls are an area where Indian platforms can borrow from the notice-and-stay-down conversations in Europe without adopting general monitoring. Platforms can run brand registry or rights owner programmes in which trademark proprietors upload their registered marks, distinctive images, and typical infringement markers. Automated tools can screen new listings for high-risk combinations such as extreme price deviation, absence of serial numbers, or use of known counterfeit keywords. Where listings are flagged, human review can seek invoices or demand better photographs. Such measures sit comfortably with "Rule 4(1)" and "Rule 5(2)" of the Consumer Protection (E-Commerce) Rules, 2020 which call for accurate description and transparency, and they can be framed as privacy-respecting data processing under the DPDP Act because the purpose is fraud prevention and legal compliance. This approach helps the marketplace demonstrate to courts that it does not turn a blind eye to counterfeiting, which is relevant when a brand later seeks dynamic injunctions or argues that the platform was wilfully supplying services to known infringers. At the same time, by stopping short of platform-wide surveillance and by giving sellers a channel to prove authenticity, the marketplace keeps faith with the principle in "*Tiffany (NJ) Inc. v. eBay Inc.*[61], that general knowledge of infringement does not equate to liability.[62]

Fulfilment and Authenticity Claims

The riskiest zone is where the marketplace itself stores, packs, ships or even promises authenticity through a guarantee badge. In such cases the platform steps into the shoes of a seller and courts are unlikely to treat it as a passive intermediary. "Rule 7 of the Consumer Protection (E-Commerce) Rules, 2020" already makes inventory e-commerce entities responsible for warranties and guarantees offered by them, and to that extent a counterfeit found in a fulfilment centre can give rise to direct trademark infringement under "Section 29 of the Trade Marks Act, 1999" and to criminal complaints under "Section 102 read with Sections 103 to 105 of the Trade Marks Act, 1999". Platforms should therefore segregate inventory SKUs from pure marketplace SKUs, put in place stricter vendor due diligence for inventory supply, and run periodic sampling and impairment tests. Where authenticity is guaranteed, the platform must be prepared to compensate consumers and to seek indemnity from the upstream supplier, which requires that the supplier contract be

[58] Debayan Bhattacharya, "Analysing the Liability of Digital Medical Platforms Under Indian Law", 15 *NUJS Law Review* 94 (2022).
[59] Rule 5: Liabilities Of Marketplace E-Commerce Entities, *available at:* https://www.consumerprotection.in/rule-5-liabilities-of-marketplace-e-commerce-entities/ (last visited on October 30, 2025).
[60] Rohini Sinha, "Do E-Commerce Platforms Provide Safety to Trademark Owners Against Infringement", 7 *International Journal of Law, Management & Humanities* 112 (2021).
[61] *Supra* note 51.
[62] Consumer Protection (E-Commerce) Rules, 2020, *available at:* https://www.consumerprotection.in/consumer-protection-e-commerce-rules-2020/ (last visited on October 29, 2025).

DPDP-compliant so that buyer details can be shared for recall or investigation without breaching data-protection obligations. Failure to do so can invite action not only from trademark owners but also from consumer authorities for unfair trade practice and from IT regulators if takedown is delayed.[63]

Enforcement Toolkit for Trademark Owners

Even where platforms are diligent, brand owners will need an enforcement toolkit tuned to online counterfeiting. Civil law under the Trade Marks Act, 1999 continues to offer the primary remedies of injunction, delivery up, damages or account of profits, and these can be adapted to the online environment through dynamic injunctions that capture future URLs or seller IDs selling the same counterfeit goods. Marketplace rules under consumer law make it easier to identify repeat infringers and to press for their deactivation. Criminal law can be invoked when the counterfeit scale is large, when there is risk to health and safety, or when the seller is anonymous and can be unmasked only through BNSS processes that compel platforms to share data. Evidence law under the BSA, 2023 supports this enforcement by granting legal recognition to stored electronic records, screenshots, and platform logs, which is critical when the infringing listing is short-lived.[64]

Civil Remedies

Civil suits for trademark infringement under "Section 134 of the Trade Marks Act, 1999" can be filed in a forum where the plaintiff carries on business, which makes it easier for brand owners to sue in their commercial hubs even if the infringing seller sits elsewhere and operates through an e-commerce site. Reliefs can include permanent injunction restraining the seller and, in appropriate cases, the marketplace from displaying the infringing listing; delivery up or destruction of counterfeit goods; damages or account of profits; and more recently dynamic injunctions where the court authorises the plaintiff to notify future URLs or seller IDs to the platform for immediate blocking. Courts can also appoint local commissioners to visit fulfilment centres, which will operate under the search and seizure procedure of the BNSS, 2023 and will have to record proceedings by audio-video means. To support these suits, marketplaces must preserve transactional and KYC records in line with BSA presumptions for electronic records and DPDP retention rules. Where the marketplace has already taken down the listing on notice, it can place the takedown logs, communications and seller responses before the court to demonstrate good faith and to seek a direction against the primary infringer only.[65]

Forum	**Reliefs**	**Notes for online counterfeits**
Civil court under "Section 134 TM Act, 1999"	Permanent/dynamic injunction, delivery up, damages/accounts	Platform can be directed to disclose seller identity and to disable future listings
Criminal court invoking "Section 102 read with 103-105 TM Act, 1999" and "Sections 347, 349 BNS, 2023"	Search, seizure, imprisonment and fine for falsifying marks	Marketplace data assists in identifying physical stock points
CCPA or consumer authority under "Consumer Protection (E-Commerce) Rules, 2020"	Directions to correct disclosures, de-list non-compliant sellers, penalty for unfair trade practices	Useful where counterfeit overlaps with misleading country-of-origin or warranty claims

Table 4: Remedies matrix by forum and relief

Criminal Complaints for Counterfeiting

Criminal law becomes relevant when counterfeit goods enter the market on a commercial scale or where the goods affect public health, and the Trade Marks Act, 1999 offers a clear path through "Section 102 (falsifying and falsely applying trademarks)" read with "Sections 103 to 105" on penalties and procedure. These offences are cognisable and give the police authority under the BNSS, 2023 to conduct searches of warehouses, residential premises or fulfilment centres that may contain the fake goods, to seize articles, and to record the entire operation through audio-video means as required by "Section 105 and Section 185 of the BNSS, 2023". Where the platform has identified a repeat infringer and preserved electronic records of listings, chats and payments, these records can be produced as electronic evidence under "Sections 62, 63 and 93 of the Bharatiya Sakshya Adhiniyam, 2023" to connect the online persona to the seized goods. The BNS, 2023 also makes sale of goods bearing counterfeit property marks punishable, giving prosecutors an additional handle where the goods do not fall squarely under the Trade Marks Act but still mislead consumers. E-commerce platforms that cooperate with these investigations improve their chances of retaining safe harbour for the listings they host.[66]

[63] Prachi Kumari, "Legal Mechanisms for Addressing IP Theft and Counterfeiting in E-Commerce Platforms", 4 *Journal of Legal Research and Juridical Sciences* 146 (2024).
[64] V. J. Taraporevala, *Law of Intellectual Property* 188 (Thomson Reuters, New Delhi, 1st edn., 2019).
[65] S. K. Verma, "Enforcement of Intellectual Property Rights: TRIPS Procedure & Remedies", 46 *Journal of the Indian Law Institute* 104 (2004).
[66] The Trade Marks Act, *available at:* https://www.bananaip.com/acts-rules/the-trade-marks-act/ (last visited on October 28, 2025).

Platform Escalations

Before or alongside formal proceedings, trademark owners can escalate within the platform's own governance structure. Many large marketplaces now appoint grievance officers and nodal officers under the IT Rules, 2021, and a trusted-notifier programme can be negotiated with them so that verified trademark owners' complaints move faster through the takedown pipeline. Where a platform fails to display mandatory seller information, contact details, or country-of-origin data, the brand can approach the Central Consumer Protection Authority under "Rule 4, Rule 5 and Rule 8 of the Consumer Protection (E-Commerce) Rules, 2020" to seek directions. Where personal data of buyers is needed to pursue a civil or criminal remedy, the brand can make a lawful request that the platform can honour under the DPDP Act's clauses on disclosure for legal purposes. These routes create pressure on non-compliant sellers without immediately engaging the court system and they help create a track record of brand vigilance, which can later persuade a civil court to grant rolling or dynamic injunctions.[67]

Policy and Reform

Indian trademark law was drafted for a world in which infringement usually occurred through physical distribution networks, but online marketplaces have introduced anonymous sellers, cross-border sourcing, flash listings and AI-generated product descriptions. The Trade Marks Act, 1999 still works as the core statute, yet much of the present discipline of e-commerce platforms comes from the IT Act, the Intermediary Rules, the Consumer Protection (E-Commerce) Rules and now the DPDP Act. None of these statutes says in express terms when a marketplace becomes secondarily liable for trademark infringement, nor how fast it must act on a brand's complaint. Policy reform can therefore focus on three tracks: clarifying secondary liability standards for e-commerce, creating sectoral SOPs for authenticity verification in high-risk categories, and issuing coordinated guidance between MeitY and the Department of Consumer Affairs so that platforms receive a coherent message. Such reform would protect consumers from fakes while giving online sellers and marketplaces predictability.[68]

Clarify Secondary Liability in Trademark Law

One approach would be to add an explicit provision in the Trade Marks Act, 1999 stating that an online marketplace or e-commerce intermediary that (a) receives specific written notice from a proprietor about an infringing listing identified by URL, seller name or order ID, and (b) fails to remove or disable access within a reasonable time, shall be deemed to have permitted the use of the trademark in the course of trade and shall be jointly and severally liable with the primary infringer. The same provision can clarify that marketplaces that act within time, preserve records, share data through BNSS procedure, and maintain a repeat-infringer policy, will retain the benefit of "Section 79 of the IT Act, 2000", creating harmony between trademark, IT and consumer frameworks. This legislative clarity would reduce conflicting High Court decisions and give platforms a statutory basis for insisting on complete, verified notices from brand owners. It would also help translate international learning from "*Tiffany (NJ) Inc. v. eBay Inc.*[69], and "*L' Oréal SA v. eBay International AG*[70], Case C-324/09 (CJEU 2011)" into Indian statutory text without undermining the exhaustion doctrine explained in "*Kapil Wadhwa v. Samsung Electronics Co. Ltd*[71], FAO(OS) 93/2012 (Del HC)".[72]

Standard Operating Procedures

A second reform track would be to encourage industry-wide, perhaps BIS-style, standard operating procedures for authenticity verification in categories where counterfeiting is prevalent, such as cosmetics, automotive spares, luxury fashion, mobile accessories and educational books. These SOPs can prescribe what documents a seller must upload, what images a platform must collect, what impairment tests should be run, and how long the platform must retain related data in a DPDP-compliant vault. They can also include templates for courtroom-ready affidavits under the BSA, 2023 setting out the platform's logs, timestamps, and algorithmic flags. Since "Rule 5(5) of the Consumer Protection (E-Commerce) Rules, 2020" already tells platforms to keep records of repeat infringers, formalising SOPs will not add a new duty but will make compliance more uniform and auditable. Public availability of annual counterfeit-takedown reports, modelled on transparency reports that social-media intermediaries already publish under the IT Rules, would strengthen deterrence.[73]

Coordinated Guidance

The third reform track should come through joint advisories from MeitY, which oversees intermediaries under the IT Act, and from the Department of Consumer Affairs, which enforces the Consumer Protection (E-Commerce) Rules, 2020. These advisories can specify standard counterfeit-reporting formats, evidentiary thresholds for takedown, time limits for response, and data-sharing channels with law-enforcement agencies operating under the

[67] Vanshita Mehra, "Legal Challenges and Regulations for E-Commerce Companies", 6 *International Journal of Law, Management & Humanities* 121 (2020).
[68] V. K. Ahuja, *Law Relating to Intellectual Property Rights* 242 (LexisNexis, Gurgaon, 1st edn., 2017).
[69] *Supra* note 51.
[70] *Supra* note 53.
[71] *Supra* note 44.
[72] Safe Harbour Provisions For Intermediaries In India And US, *available at:* https://blog.ipleaders.in/safe-harbour-provisions-for-intermediaries-in-india-and-us/ (last visited on October 27, 2025).
[73] V. J. Taraporevala, *Law of Intellectual Property* 231 (Thomson Reuters, Mumbai, 1st edn., 2019).

BNSS, 2023. They can also explain how platforms should treat parallel imports so that legitimate grey-market trade is not chilled. With the DPDP Act now in force, the same advisories can lay down model consent notices for sellers and buyers, retention schedules for KYC and transaction data, and security safeguards that platforms must adopt to avoid the steep penalties in "Section 33 and Schedule 1 of the Digital Personal Data Protection Act, 2023". A coordinated approach will give Indian e-commerce a single, hierarchical compliance map that courts can refer to when deciding if a platform has acted diligently in a counterfeit dispute.[74]

Conclusion

Indian law on platform liability for online counterfeits has matured from a blunt, conduit-versus-publisher debate into a fact-sensitive assessment of role and response. Courts preserve Section 79 safe harbour for marketplaces that remain technologically neutral and act promptly on specific, URL-based notices, as seen in Kent RO and the Flipkart FIR-quashing decision, while refusing to impose a general duty to pre-screen every listing. Conversely, when a platform curates, advertises, warehouses, "fulfils", invoices, or offers authenticity guarantees, judges tend to treat it as an active participant-narrowing or negating safe harbour-as in Christian Louboutin (Darveys) and in the BHPC/Amazon single-judge ruling that awarded headline damages before being stayed on appeal (the stay later left undisturbed by the Supreme Court). This trajectory fits the legislative architecture: Section 79 offers conditional immunity; the Intermediary Rules (2021/2023) convert that condition into due-diligence choreography (policies, grievance handling, time-bound action); and the Consumer Protection (E-Commerce) Rules impose seller-verification and disclosure duties that make marketplace governance auditable. For high-risk categories (foods, cosmetics, health products), Hamdard v. Amazon shows courts will demand heightened vigilance and proactive measures after notice, without collapsing into general monitoring. Put simply, Indian doctrine now hinges on three triggers: (1) specific knowledge of a counterfeit offer; (2) active platform conduct approximating a seller; and (3) repeat-infringer patterns that justify tighter onboarding and stay-down steps. 75

At the same time, the system recognizes limits and safeguards. The Amazon v. Amway division bench resists using non-statutory executive circulars to throttle lawful trade, preserving room for genuine resale and parallel imports-doctrinally distinct from counterfeits-provided that disclosures are accurate and condition is unimpaired. The BNSS/BNS/BSA triad modernizes enforcement: police can search/seize counterfeit stock with audio-video recording; platforms can lawfully preserve and furnish KYC, logs, and transaction trails; and courts can rely on electronic records as primary evidence, enabling dynamic injunctions and calibrated criminal process against repeat offenders. When combined with DPDP-compliant data governance and SLA-driven takedown, marketplaces can prove diligence rather than merely assert it-a decisive factor in retaining safe harbour in criminal as well as civil contexts. The policy arc therefore supports a balanced model: no ex-ante universal screening, but mandatory, rapid, and well-documented ex-post response; no blanket liability for marketplaces, but significant exposure when platform design and commercial incentives blur the line between host and seller. The practical message is clear for all actors: platforms must operationalize traceability and response; brand owners should pair Trade Marks Act actions with IT/consumer-rule levers; and regulators can align MeitY and Consumer Affairs guidance to create predictable standards without chilling legitimate e-commerce. [76]

Suggestions

Building on this legal analysis under Indian trademark law, the following targeted steps translate doctrine into day-to-day platform and enforcement practice.[77]

1. Adopt a two-track triage (counterfeit vs. parallel import). Require every IP notice to specify "counterfeit" or "parallel import" with supporting documents (registration number, SKU photos, invoices). Route "counterfeit" to immediate de-listing, evidence preservation, and repeat-infringer checks. Route "parallel import" to disclosure/warranty-status verification instead of default takedown. Document all actions in a tamper-evident log to substantiate safe-harbour diligence.[78]

2. Codify a URL-specific notice standard and SLA. Publish a one-page online form capturing URL(s), seller ID, mark/registration, screenshots, and a good-faith declaration. Commit to de-listing within 24–48 hours for prima facie counterfeits; acknowledge and explain if more time is needed for authenticity review. Send contemporaneous notices to the seller with a time-bound counter-notice window. Auto-generate a case number and exportable report for court filing and police requests.[79]

3. Build a DPDP-compliant evidence vault. On every counterfeit takedown, auto-snapshot listing pages, seller metadata, chat logs, fulfilment scans, and payment tokens. Hash and timestamp artifacts; store retention schedules aligned to litigation and BNSS demands. Restrict access via role-based controls and log every retrieval for chain-of-custody integrity. Provide one-click affidavits that cite hash values and system

[74] Ishita Gupta, "Evolving Scope of Intermediary Liability in India", 27 *International Review of Law, Computers & Technology* 79 (2023).
[75] Kent Ro Systems Ltd. v. Amit Kotak, *available at:* https://www.casemine.com/judgement/in/58be65654a9326199e6aac23 (last visited on November 2, 2025).
[76] Adarsh Saxena, Mitakshi Lakhani, "'Buy Now' or 'Remove From Cart'?: Delhi HC Allows E-Commerce Platforms to List Products of Direct Selling Entities Without Their Consent", *available at:* https://corporate.cyrilamarchandblogs.com/2020/02/delhi-hc-allows-ecommerce-platforms-to-list-products-of-direct-selling-entities-without-their-consent/ (last visited on October 31, 2025).
[77] Shiv Kumar Verma, "Enforcement of Intellectual Property Rights: TRIPS Procedure & Remedies", 46 *Journal of the Indian Law Institute* 116 (2004).
[78] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on November 2, 2025).
[79] *Supra* note 75.

times for BSA admissibility.[80]

4. Tighten high-risk category onboarding. For cosmetics, health foods, auto spares, luxury fashion, and electronics, require enhanced KYC (GST, BIS/FDCA licenses, import documents, batch/lot data). Mandate sample invoices and high-resolution packaging photos before first listing. Run serial-number or GTIN validation where feasible; flag extreme price deviations for manual review. Refuse "authenticity guarantee" badges unless upstream provenance audits are passed.[81]

5. Segment fulfilment and inventory risk. Maintain hard separation between marketplace SKUs and platform-owned or fulfilled SKUs in systems, warehouses, and packaging. Apply heightened sampling and AQL testing to inventory/fulfilled SKUs; quarantine suspect batches automatically. Display supply-chain disclosure on product pages where the platform touched storage or packaging. If a counterfeit is found in platform custody, process immediate consumer redress and supplier chargebacks.

6. Use "trusted notifier" programs with escalation ladders. Invite rights-holders with a proved track record to a higher-priority queue that triggers near-instant de-listing on prima facie proof. Require reciprocal commitments: accurate notices, periodic registry updates, and withdrawal when error is shown. Set a graduated response for sellers: warning → listing suspension → account termination → marketplace-wide block upon repeat counterfeit findings. Publish quarterly metrics on notices, turnaround times, and outcomes.[82]

7. Deploy narrow, non-general monitoring tools. Configure rules for only high-signal patterns: seller-ID recycling, banned keywords, duplicate imagery, and serial-number anomalies. When a flag fires, pause the listing and request invoices or better images rather than mass removals. Allow brand APIs to push signature assets (logos, holograms) for machine checks under agreed false-positive thresholds. Continuously A/B test thresholds to minimize lawful-trade friction.[83]

8. Institute a country-of-origin and warranty disclosure checklist. Make origin and warranty fields mandatory and validated (dropdowns, not free text). Auto-warn consumers when manufacturer warranty does not apply; require sellers to state equivalent seller warranty terms. Reject listings with mismatched origin indicators across title, bullets, and images. Export non-compliance reports to the Grievance Officer and, if unresolved, to the Central Consumer Protection Authority channel.[84]

9. Standardize litigation-ready playbooks with law-enforcement. Pre-agree BNSS search/seizure SOPs with local cyber cells, including data-request formats, service levels, and AV-recording compatibility. Train a small incident-response cell to produce certified electronic records and witness statements within 72 hours. Maintain a roster of local commissioners for rapid civil raids where courts so order. After each incident, run a post-mortem to update keyword blocks, seller-onboarding controls, and repeat-offender maps.[85]

10. Clarify internal red lines for "active role". Create a checklist that must be cleared before marketing programs roll out: use of brand marks in ads, ranking boosts, storefront curation, bundling, and guarantees. Require Legal to sign off when programs could re-characterize the platform as an inventory seller or promoter in the eyes of a court. If a program crosses red lines, add compensating controls (enhanced audits, seller indemnities, visible disclosures) or confine it to vetted brands. Review this checklist quarterly against new case-law and regulatory advisories[86].

Bibliography

Books:

- Avtar Singh, *Consumer Protection Law and Practice* (Eastern Book Company, Lucknow, 1st edn., 2019).
- B. L. Wadhera, *Law Relating to Intellectual Property* (Universal Law Publishing, Delhi, 1st edn., 2014).
- G. B. Reddy, *Intellectual Property Rights and the Law* (Gogia Law Agency, Hyderabad, 1st edn., 2020).
- P. Narayanan, *Law of Trade Marks and Passing Off* (Eastern Law House, Kolkata, 1st edn., 2018).
- Pavan Duggal, *Cyber Law: An Exhaustive Section-Wise Commentary on the Information Technology Act* (LexisNexis, New Delhi, 1st edn., 2023).
- V. J. Taraporevala, *Law of Intellectual Property* (Thomson Reuters, New Delhi, 1st edn., 2019).

[80] Adarsh Saxena, Mitakshi Lakhani, "'Buy Now' or 'Remove From Cart'?: Delhi HC Allows E-Commerce Platforms to List Products of Direct Selling Entities Without Their Consent", *available at:* https://corporate.cyrilamarchandblogs.com/2020/02/delhi-hc-allows-ecommerce-platforms-to-list-products-of-direct-selling-entities-without-their-consent/ (last visited on October 31, 2025).

[81] Christian Louboutin Sas vs Nakul Bajaj & Ors on 2 November, 2018, *available at:* https://indiankanoon.org/doc/99622088/ (last visited on November 1, 2025).

[82] Delhi High Court Examines Intermediary Liability For Trademark Infringement: Part I, *available at:* https://spicyip.com/2018/11/delhi-high-court-examines-intermediary-liability-for-trademark-infringement-part-i.html (last visited on October 31, 2025).

[83] Consumer Protection (E-Commerce) Rules, 2020, *available at:* https://thc.nic.in/Central%20Governmental%20Rules/Consumer%20Protection%20%28E-Commerce%29%20Rules%2C%202020.pdf (last visited on October 30, 2025).

[84] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 29, 2025).

[85] *Supra* note 1.

[86] *Supra* note 2.

- V. K. Ahuja, *Law Relating to Intellectual Property Rights* (LexisNexis, Gurgaon, 1st edn., 2017).
- Venkateswaran, *Trade Marks and Passing-Off* (LexisNexis, Gurgaon, 1st edn., 2019).

Statutes:

- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)
- The Consumer Protection (E-Commerce) Rules, 2020 (Notified under the Consumer Protection Act, 2019)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Notified under Section 87 of the Information Technology Act, 2000)
- The Trade Marks Act, 1999 (Act No. 47 of 1999)

Articles:

- Debayan Bhattacharya, "Analysing the Liability of Digital Medical Platforms Under Indian Law", 15 *NUJS Law Review* 94 (2022).
- Ishita Gupta, "Evolving Scope of Intermediary Liability in India", 27 *International Review of Law, Computers & Technology* 79 (2023).
- Prachi Kumari, "Legal Mechanisms for Addressing IP Theft and Counterfeiting in E-Commerce Platforms", 4 *Journal of Legal Research and Juridical Sciences* 146 (2024).
- Rohini Sinha, "Do E-Commerce Platforms Provide Safety to Trademark Owners Against Infringement", 7 *International Journal of Law, Management & Humanities* 112 (2021).
- S. K. Verma, "Enforcement of Intellectual Property Rights: TRIPS Procedure & Remedies", 46 *Journal of the Indian Law Institute* 92 (2004).
- Vanshita Mehra, "Legal Challenges and Regulations for E-Commerce Companies", 6 *International Journal of Law, Management & Humanities* 121 (2020).

Websites:

- Aaron Kamath, Abhishek Senthilnathan, et.al., "Intermediaries Under The Indian Information Technology Law Can Breathe A Sigh Of Relief", *available at:* https://nishithdesai.com/default.aspx?id=5027 (last visited on October 28, 2025).
- Adarsh Saxena, Mitakshi Lakhani, "'Buy Now' or 'Remove From Cart'?: Delhi HC Allows E-Commerce Platforms to List Products of Direct Selling Entities Without Their Consent", *available at:* https://corporate.cyrilamarchandblogs.com/2020/02/delhi-hc-allows-ecommerce-platforms-to-list-products-of-direct-selling-entities-without-their-consent/ (last visited on October 31, 2025).
- Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors., *available at:* https://cyberblogindia.in/amazon-seller-services-pvt-ltd-v-amway-india-enterprises-pvt-ltd-ors/ (last visited on October 25, 2025).
- Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd. & Ors., *available at:* https://taxguru.in/wp-content/uploads/2020/02/Amazon-Seller-Services-Pvt.-Ltd.-Vs-Amway-India-Enterprises-Pvt.-Ltd.-Ors.-Delhi-High-Court.pdf (last visited on November 2, 2025).
- Arrangement Of Sections-Chapter XVIII Of Property Marks: Section 349, *available at:* https://kanoongpt.in/bare-acts/the-bharatiya-nyaya-sanhita-2023/arrangement-of-sections-chapter-xviii-of-property-marks-section-349-38ee139d21a6567e (last visited on October 29, 2025).
- Case Analysis : Kent RO Systems Ltd. & Anr. v. Amit Kotak & Ors, *available at:* https://blog.ipleaders.in/case-analysis-kent-ro-systems-ltd-anr-v-amit-kotak-ors/ (last visited on October 30, 2025).
- Case C-324/09, *available at:* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A62009CJ0324_SUM (last visited on October 31, 2025).
- Christian Louboutin SAS v. Nakul Bajaj And Ors., *available at:* https://sflc.in/policies-and-cases/christian-louboutin-sas-v-nakul-bajaj-and-ors/ (last visited on October 26, 2025).
- Christian Louboutin Sas vs Nakul Bajaj & Ors on 2 November, 2018, *available at:* https://indiankanoon.org/doc/99622088/ (last visited on November 1, 2025).
- Consumer Protection (E-Commerce) Rules, 2020, *available at:* https://thc.nic.in/Central%20Governmental%20Rules/Consumer%20Protection%20%28E-Commerce%29%20Rules%2C%202020.pdf (last visited on October 30, 2025).

- Consumer Protection (E-Commerce) Rules, 2020, *available at:* https://www.consumerprotection.in/consumer-protection-e-commerce-rules-2020/ (last visited on October 29, 2025).
- Delhi High Court Examines Intermediary Liability For Trademark Infringement: Part I, *available at:* https://spicyip.com/2018/11/delhi-high-court-examines-intermediary-liability-for-trademark-infringement-part-i.html (last visited on October 31, 2025).
- Delhi High Court Judgment: 2022 DHC 3072, *available at:* https://supremetoday.ai/doc/judgement/IND_Delhi_2022_DHC_003072 (last visited on October 30, 2025).
- Delhi High Court: Direct Selling Guidelines Advisory In Nature And Not Binding As A Law, *available at:* https://www.agarwaljetley.com/delhi-high-court-direct-selling-guidelines-advisory-in-nature-and-not-binding-as-a-law.html (last visited on October 24, 2025).
- Dipak K Dash, "Centre Proposes 'Country Of Origin' Filter On E-Commerce Sites", *available at:* https://timesofindia.indiatimes.com/business/india-business/centre-proposes-country-of-origin-filter-on-e-commerce-sites/articleshow/124854628.cms (last visited on October 31, 2025).
- E-Commerce Platforms As An Intermediary Under The IT Act, 2000, *available at:* https://ksandk.com/information-technology/intermediary-under-the-it-act/ (last visited on October 27, 2025).
- E-Commerce Websites Are Not Bound To Keep A Check On Products For IP Infringement Before Advertising On Their Website, *available at:* https://www.scconline.com/blog/post/2017/03/04/e-commerce-websites-are-not-bound-to-keep-a-check-on-products-for-ip-infringement-before-advertising-on-their-website/ (last visited on October 26, 2025).
- Flipkart Internet Private Limited v. State Of NCT Of Delhi And Anr, *available at:* https://globalfreedomofexpression.columbia.edu/cases/flipkart-internet-private-limited-v-state-of-nct-of-delhi-and-anr/ (last visited on November 1, 2025).
- Hamdard National Foundation (India) & Anr v. Amazon India Ltd. & Anr., *available at:* https://lexmantis.com/2022/11/30/hamdard-national-foundation-in-anr-v-s-amazon-india-ltd-anr/ (last visited on November 1, 2025).
- High Court: Amazon Directed To Remove ROOH AFZA Branded Products Not Originating From Hamdard India, *available at:* https://www.candcip.com/single-post/high-court-amazon-directed-to-remove-rooh-afza-branded-products-not-originating-from-hamdard-india (last visited on October 31, 2025).
- Indu Bhan, "Supreme Court Dismisses Lifestyle Equities' Appeal, Amazon Freed From Rs 340 Cr Trademark Penalty", *available at:* https://m.economictimes.com/news/company/corporate-trends/sc-rejects-lifestyle-equities-plea-amazon-technologies-escapes-rs-340-cr-trademark-damages/articleshow/124093635.cms (last visited on October 26, 2025).
- Kapil Wadhwa & Ors. vs. Samsung Electronics Co. Ltd.: Legal Case Overview, *available at:* https://brieflaws.com/case-briefs/kapil-wadhwa-and-ors-vs-samsung-electronics-co-ltd (last visited on November 2, 2025).
- Kent RO Ltd & Anr. v. Amit Kotak & Ors., *available at:* https://sflc.in/policies-and-cases/kent-ro-ltd-anr-v-amit-kotak-ors/ (last visited on October 28, 2025).
- Kent RO System Ltd. v. Amit Kotak, *available at:* https://lawbhoomi.com/kent-ro-system-ltd-v-amit-kotak/ (last visited on October 27, 2025).
- Kent Ro Systems Ltd. v. Amit Kotak, *available at:* https://www.casemine.com/judgement/in/58be65654a9326199e6aac23 (last visited on November 2, 2025).
- Lifestyle Equities CV & Anr. vs Amazon Technologies, Inc. on 25 February, 2025, *available at:* https://indiankanoon.org/doc/38072391/ (last visited on October 29, 2025).
- Police ‘Pathshalas' To Explain Legal Reforms, *available at:* https://maharashtratimes.com/e-paper/2025/nov/1-november-2025/police-pathshalas-to-explain-legal-reforms/articleshow/125004923.cms (last visited on October 24, 2025).
- Procedure, Pleadings And Platforms: DHC's Stay In Amazon v. Lifestyle, *available at:* https://spicyip.com/2025/07/procedure-pleadings-and-platforms-dhcs-stay-in-amazon-v-lifestyle.html (last visited on October 28, 2025).
- Ritu Yadav, "Delhi HC Stays Rs 339 Cr Damages Order Against Amazon In Beverly Hills Polo Club Trademark Row", *available at:* https://lawbeat.in/news-updates/delhi-hc-stays-rs-339-cr-damages-order-against-amazon-in-beverly-hills-polo-club-trademark-row-1500462 (last visited on October 27, 2025).
- Rule 5: Liabilities Of Marketplace E-Commerce Entities, *available at:* https://www.consumerprotection.in/rule-5-liabilities-of-marketplace-e-commerce-entities/ (last visited on October 30, 2025).
- Safe Harbour Provisions For Intermediaries In India And US, *available at:* https://blog.ipleaders.in/safe-harbour-provisions-for-intermediaries-in-india-and-us/ (last visited on October 27, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 29, 2025).

- The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf (last visited on October 25, 2025).
- The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 25, 2025).
- The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on November 2, 2025).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on November 2, 2025).
- The Trade Marks Act, 1999, *available at:* https://www.indiacode.nic.in/bitstream/123456789/15427/1/the_trade_marks_act%2C_1999.pdf (last visited on October 24, 2025).
- The Trade Marks Act, *available at:* https://www.bananaip.com/acts-rules/the-trade-marks-act/ (last visited on October 28, 2025).
- Tiffany (NJ) Inc. v. eBay Inc., *available at:* https://en.wikipedia.org/wiki/Tiffany_%28NJ%29_Inc._v._eBay_Inc. (last visited on November 1, 2025).