

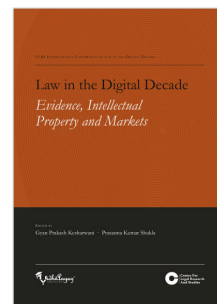
CHAPTER 12

Protecting Trademark in the Metaverse: The Emerging Threat of AI-Generated Counterfeits

A. Vedha Valli

in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 123–138

DOI <https://doi.org/10.63108/VAB.LDD.2.12>



CITATIONS

BLUEBOOK (21ST ED.)

A. Vedha Valli, *Protecting Trademark in the Metaverse: The Emerging Threat of AI-Generated Counterfeits*, in *LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS* 123 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)

A. Vedha Valli, ‘Protecting Trademark in the Metaverse: The Emerging Threat of AI-Generated Counterfeits’ in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 123.

CHICAGO (17TH ED.)

Valli, A. Vedha. “Protecting Trademark in the Metaverse: The Emerging Threat of AI-Generated Counterfeits.” In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 123–138. Maihar: VidhiAagaz, 2026. <https://doi.org/10.63108/VAB.LDD.2.12>.

APA (7TH ED.)

Valli, A. V. (2026). Protecting trademark in the metaverse: The emerging threat of AI-generated counterfeits. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 123–138). VidhiAagaz. <https://doi.org/10.63108/VAB.LDD.2.12>

SOURCE

<https://doi.org/10.63108/VAB.LDD.2.12>

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

CHAPTER 12

Protecting Trademark in the Metaverse: The Emerging Threat of AI-Generated Counterfeits

A. VEDHA VALLI*

Generative artificial intelligence tools allow metaverse users to generate virtual wearables, avatar accessories and other branded goods, which often infringe upon trademark rights. These infringing goods, however, are not static counterfeits but dynamically generated knockoffs that rarely explicitly name the trademark owner and take place in novel digital environments. This paper analyses whether and how Indian trademark laws can tackle such emerging forms of infringement based on the doctrine of “use in the course of trade”, the “identical or similar goods” jurisdictional anchor and the “likelihood of confusion” standard. It argues that the ability of Indian trademark law to address these concerns is limited by the very existence of doctrines and tests that seek to make sense of trademark infringement in virtual settings, as well as the lack of a holistic regulatory approach to the liability of metaverse platforms under the Trade Marks Act, 1999 and the Information Technology Act, 2000. By relying on recent Indian, EU, US and UK jurisprudence and early cases on trademarks and AI-generated counterfeits, the paper highlights the jurisdictional fragmentation in addressing generative AI infringement in India and proposes a unified approach to enforcing trademark rights against dynamically generated virtual counterfeits.

Keywords: trademark infringement, generative AI, metaverse, intermediary liability, virtual counterfeiting

1 INTRODUCTION

The term “metaverse” refers to an immersive, digital environment, where users can interact in real time through avatars, engaging in social, commercial and creative activity that imitates the real-world experience. Unlike the previous virtual platforms, the metaverse consists of technologies such as augmented and virtual reality, blockchain, Gen AI etc., allowing users to create, own, and transact within it. Platforms like Roblox, Decentraland, and The Sandbox exemplify this shift. It creates spaces where users can build, buy, and sell virtual goods, effectively imitating the real world commerce in a decentralised, user generated economy.¹

It is this dual character of the metaverse which acts as both a social space and an economic market, that has drawn many luxury and fashion brands to venture out in virtual reality shops and it is precisely this same openness and user generative capability that has made the metaverse equally vulnerable to infringement.²

* Assistant Professor at Department of Intellectual Property Law, The Tamil Nadu Dr. Ambedkar Law University, Chennai, Tamil Nadu, India.

¹ Tambiama Madiega, Polona Car and Maria Niestadt, ‘Metaverse: Opportunities, Risks and Policy Implications’ (European Parliamentary Research Service Briefing PE 733.557, June 2022) [https://www.europarl.europa.eu/Reg-DATA/etudes/BRIE/2022/733557/EPRS_BRI\(2022\)733557_EN.pdf](https://www.europarl.europa.eu/Reg-DATA/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf) accessed 10 September 2026.

² Prada Group, LVMH, Prada Group and Cartier Come Together to Form the Aura Blockchain Consortium Supporting the First Global Blockchain Dedicated to the Luxury Industry’ (Press release, 20 April 2021) <https://www.pradagroup.com/en/news-media/press-releases-documents/2021/21-04-20-aura-blockchain-consortium.html> accessed 10 September 2026.

Metaverse platforms embed generative artificial intelligence tools that let users create wearables, avatar skins, and branded accessories through natural language prompts. Many brands are launching their own metaverse stores, expanding the brand in the virtual world. To name a prominent one, Gucci, one of the most famous names in high end fashion, didn't want to miss the opportunity of being an innovator in the fashion industry by investing in the metaverse. They began their investment in May 2021 when they opened Gucci Garden on Roblox, celebrating their 100th anniversary. During this event, users could purchase NFT collectibles. Later that year, they sold their Dionysus bag for 350,000 Robux, which equals about \$4,115.³ Their next step was investing in land on The Sandbox to expand its Gucci Vault, an online store. This virtual store will give shoppers a more immersive experience and develop their NFT market further. If they continue to gain popularity, their NFTs could become a \$56 billion market by 2030.⁴

As official virtual storefronts demonstrated that branded digital wearables and accessories could command real economic value, the same open-platform tools that let Gucci and other houses build immersive stores also made it just as easy for anyone, without permission or licensing, to model, mint, and sell near identical virtual imitations of those goods, so counterfeiting migrated into the metaverse as a natural extension of its legitimate luxury market. Where conventional counterfeiting involves a fixed infringing product, manufactured once and distributed many times, generative virtual counterfeiting is produced anew at each point of use, frequently without the user ever naming the brand being copied.⁵

This generative shift in metaverse counterfeiting operates through two distinct pathways of infringement. In the first, a deliberate infringer, whether an individual creator or an operator of a virtual storefront, consciously designs and lists a virtual good that reproduces a brand's logo, trade dress, or distinctive product silhouette, mirroring the intent driven infringement familiar from conventional counterfeiting, only executed through 3D modelling or NFT-minting tools rather than physical manufacture.⁶

In the second, and more novel, pathway, the infringement is generated automatically by the platform itself in response to an ordinary user's natural language prompt, where a user asking a generative AI tool for "a designer style handbag" or "a luxury monogrammed jacket" may receive an output that reproduces protected trade dress or a recognisable brand aesthetic without the user ever naming, intending to copy, or even being aware of the brand being emulated. This second pathway unsettles the doctrinal assumptions on which trademark and design law were built, both of which presuppose an identifiable infringing actor who has made a deliberate choice to copy. Where the copying is instead a byproduct of a generative model's training data and the platform's own output design, liability becomes difficult to locate in either the prompting user or a single authorial infringer, raising the question of whether responsibility should

³ 'Gucci Hosts Virtual Exhibition in Online Game Roblox to Mark Centenary' (*Dezeen*, 20 May 2021)

<https://www.dezeen.com/2021/05/20/gucci-garden-roblox-virtual-exhibition/> accessed 23 September 2026.

⁴ Barton Goldenberg, 'Gucci's Metaverse Makeover: A Case Study in Fashion Innovation' (*ISM*, 19 December 2023)

<https://ismguide.com/gucci-xr-metaverse-case-study/> accessed 23 September 2026.

⁵ Bernard Marr, 'How Luxury Brands Are Making Money in the Metaverse' *Forbes* (19 January 2022)

<https://www.forbes.com/sites/bernardmarr/2022/01/19/how-luxury-brands-are-making-money-in-the-metaverse/> accessed 23 September 2026.

⁶ Sneha Madan, 'The Palika Bazaar of the Metaverse: Is the Trade Marks Act, 1999 Equipped to Regulate Digital Counterfeits?' (*Khurana & Khurana*, 11 July 2026) <https://www.khuranaandkhurana.com/the-palika-bazaar-of-the-metaverse-is-the-trade-marks-act-1999> accessed 23 September 2026.

shift toward the platform or the AI tool provider that shaped the generative output in the first place. These unintentional creations by generative AI could result in licensing market dilution.⁷

This shift is no longer speculative. In November 2023, the UK High Court delivered the first judgment anywhere to find trademark infringement arising from an AI model's own generative output, when Stable Diffusion was shown to reproduce Getty Images' watermark in synthetic images it had never been directly instructed to create.⁸

This paper asks whether India's trademark and intermediary liability framework, designed around a stable, identifiable act of "use" by a defendant, can respond to infringement that is generative, ephemeral, and machine scaled. It begins by tracing the shift from static, listing based counterfeiting to on demand virtual generation, grounded in a concrete scenario and in the scale of the market now at stake, and situating itself against the small but growing foreign scholarship already engaged with the problem. It proceeds to work through Indian trademark doctrine strain by strain, analysing the threshold requirement of "use," the tests for similarity and confusion, the separate doctrine of dilution, and design law as a further, equally insufficient regime, pointing out that each was built around a discrete, comparably fixed act of infringement that generative output does not supply. The analysis proceeds to address platform accountability under Section 79 of the Information Technology Act, including India's own recent executive advisories on generative AI, before setting this domestic picture against comparable developments in the European Union, United States, United Kingdom, and Singapore. Drawing upon this doctrinal and comparative foundation, the paper proposes a coordinated enforcement framework for India, outlines what that would mean in practice for rights holders, platforms, and regulators even before any reform, and concludes by acknowledging the limits of a doctrinal and comparative analysis of this kind.

2 METHODOLOGY

The methodology deployed in this research is doctrinal and comparative. The relevant statutes, namely the Trade Marks Act, 1999 and the Information Technology Act, 2000 are examined alongside the leading Indian authorities interpreting the same. These are then placed in comparative perspective with a set of carefully chosen foreign precedents from the jurisdictions of the European Union, the United States and the United Kingdom. The choice of these jurisdictions is informed by the fact that these have provided the most detailed engagement with the issue of liability for AI generated or platform mediated virtual content thus far. The comparison is made in order to single out nuances, such as the EU's approach to the use of virtual counterfeits based on their perceived impact on the consumer, which may have a degree of applicability in the Indian context. Finally, since the Indian case law remains entirely silent on the issue of generative virtual counterfeits, the paper extrapolates from the existing Indian case law on keyword and marketplace liability and dilution, identifying the point at which such reasoning breaks down in the face of generative content.

⁷ Reinhard Oertli, 'Trademark Disputes in the Metaverse and Enforcement Challenges' (WIPO Webinar, Trademark Enforcement Issues in the Metaverse, WIPO/WEBINAR/RESPECTFOR IP/2023/1, 26 January 2023) https://www.wipo.int/meetings/en/details.jsp?meeting_id=75574 accessed 23 September 2026.

⁸ Getty Images (US) Inc & Ors v Stability AI Ltd [2023] EWHC 2863 (Ch).

3 THE GENERATIVE SHIFT

3.1 From Static Knock-Offs to On Demand Generation

The metaverse, understood as a persistent and interconnected network of 3D environments navigated by avatars, has evolved from a niche gaming concept to a commercial space in which branded virtual goods, digital fashion and NFT backed assets hold real economic value. Counterfeiting in this environment takes several forms distinct from physical world infringement. First, unauthorized replication occurs when third parties replicate and sell virtual wearables, skins or accessories which copy registered trademarks or trade dress of established brands, often offered on in-platform marketplaces or third party NFT exchanges without any licensing arrangement. Second, “asset spoofing” includes minting NFTs visually replicating the metadata or imagery of a genuine branded item, exploiting the lack of verification by many marketplaces of the authenticity of the underlying intellectual property before listing. Third, avatar and storefront impersonation enables bad actors to erect stores which closely mimic a brand’s presence, deceiving users into purchasing counterfeit digital goods or providing payment credentials in what amounts to a metaverse native phishing scheme. These practices are compounded by the pseudonymity of underlying blockchain transactions in many metaverse platforms, which defeats traditional enforcement mechanisms which rely on identifying an infringer’s physical location or corporate identity, and by the jurisdictional ambiguity of platforms whose servers, users, and hosting entities may be distributed across multiple countries simultaneously.

Online counterfeiting, as documented in Indian enforcement literature, has largely concerned fixed listings. A seller uploads a product description and image, and that listing persists until removed. Generative virtual counterfeiting inverts this structure. The infringing asset does not exist until a user’s prompt calls it into being, and no two generations need be identical. This defeats the assumption, implicit throughout trademark doctrine, that an infringing article is a discrete, comparably fixed thing that can be seized, delisted, or compared side-by-side with the registered mark.

Three episodes illustrate this trajectory. First, *Hermès International v Rothschild*⁹, the first NFT trademark trial in the United States, found that a digital artist’s “MetaBirkin” NFTs, AI assisted digital images evoking Hermès Birkin trade dress, infringed and diluted Hermès marks, with the jury rejecting a First Amendment defence because use was found explicitly misleading rather than genuine artistic commentary. Second, *Nike Inc v StockX LLC*¹⁰, concerning NFTs marketed as “Vault” tokens bearing Nike’s marks, settled in August 2025 before trial, leaving unresolved whether such tokens are themselves infringing “goods” or merely digital receipts for physical products. Third, and most significantly, *Getty Images v Stability AI* confirms that a generative model itself can be the direct source of trademark infringing output independent of any human curation of a specific listing.

The scale at which this problem is emerging is not trivial. Industry estimates put the global virtual goods market at approximately USD 132–150 billion in 2025–26, with virtual goods and NFTs identified as among the fastest growing revenue segments in the broader metaverse economy that itself is projected to grow at a compound annual rate in excess of 40 per cent through the remainder of the decade.¹¹

⁹ *Hermès International v. Rothschild*, No. 22-cv-384 (JSR), 2022 WL 4671520 (S.D.N.Y. Sept. 30, 2022)

¹⁰ *Nike, Inc. v. StockX LLC*, No. 22-cv-983 (VEC) (S.D.N.Y., filed Feb. 3, 2022)

¹¹ Global Growth Insights, ‘Virtual Goods Market Size, Share, Growth, and Industry Analysis’ (updated 5 February 2026) <https://www.globalgrowthinsights.com/market-reports/virtual-goods-market-116419>; Mordor Intelligence, ‘Virtual Goods Market Size, Forecast Report, Drivers & Opportunities 2031’ <https://www.mordorintelligence.com/industry-reports/virtual-goods-market>;

Separately, the OECD and the European Union Intellectual Property Office estimate that counterfeit and pirated goods accounted for approximately USD 467 billion in global trade in 2021.¹² These two curves are converging. The same brand equity that drives physical counterfeiting is now a generation prompt away from being reproduced in virtual form that no manual takedown process was designed to absorb. For India, this convergence arrives alongside the continuing challenge of counterfeit enforcement in physical markets, making early attention to the generative dimension a matter of pre-empting a known failure pattern rather than responding to an entirely novel one.

Consider a metaverse platform with a built-in generative wardrobe tool. A user, without naming any brand, prompts the tool for “a luxury quilted handbag in black leather with a gold chain strap for my avatar.” The tool, trained on a large corpus of fashion imagery, returns an asset that closely tracks the trade dress of a specific well-known handbag. The user did not intend to infringe and may not even recognise the resemblance. The platform did not curate or list or advertise any specific infringing item and the asset itself may never be generated in exactly that form again. Yet the output is, on any ordinary understanding, a virtual counterfeit of a real brand’s protected trade dress. None of Sections 29(1), (2), or (4) of the Trade Marks Act was drafted with this fact-pattern in mind, and none of the twenty-six Louboutin factors squarely focuses on a platform whose only “act” was to build and operate the generative tool itself.

The problem is even more acute for trade dresses and get-up marks than word-marks. A user would not have to type in the name “Hermes” or “Louboutin” to generate an image that incorporates elements of the plaintiff’s protected trade dress; a prompt of the type “quilted flap handbag with an interlocking-C clasp” or “stiletto with a glossy red sole” or a combination of the two would be sufficient, given that the diffusion style image generating models learn associations between concepts and visual appearances. Not that this is merely a theoretical problem. It was precisely the red sole that the CJEU was asked to consider in the *Louboutin v Amazon* case when ruling on the scope of the “marketplace” liability, and the word based approach to infringement, ubiquitous in the Indian jurisprudence on keyword and meta tag use, would be entirely unhelpful in a case concerning visual similarity that never invokes brand names.

4 RELATED WORK

The scholarship on trademark liability for generative AI output is only just beginning to emerge, and is almost entirely outside of India. UK practitioner commentary published ahead of INTA 2026¹³ (and therefore presumably in advance of key developments in the law) has flagged that Section 10(4) of the UK Trade Marks Act 1994 provides no scenario that cleanly describes an AI generated output, and frames it as an “underappreciated risk” for AI platforms and intermediaries. Speaking of EU law, the question is how the concept of “use” under European trademark law should be interpreted for AI generated signs and how liability could be allocated between the user, the model developer, and the platform. US practitioner literature has separately observed that generative tools can produce brand confusing content

Technavio, ‘Metaverse Market Analysis, Size, and Forecast 2026-2030’ (April 2026) <https://www.technavio.com/report/metaverse-market-industry-analysis> accessed 2 October 2026.

¹² OECD and EUIPO, ‘Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges’ (OECD Publishing, May 2025) https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/05/mapping-global-trade-in-fakes-2025_5c812e3c/94d3b29f-en.pdf accessed 2 October 2026.

¹³ Oliver Fairhurst and Victoria Owrid, ‘Trade mark liability in the age of Generative AI’ (Lewis Silkin, 6 March 2026) <https://www.lewissilkin.com/en/insights/2026/03/06/trade-mark-liability-in-the-age-of-generative-ai> accessed 2 October 2026.

“without any human intent to infringe” and that prompt filtering safeguards are emerging as an industry response despite the lack of a settled doctrine requiring them.¹⁴ None of this speaks to the Indian position, and none situates the problem within a jurisdiction where trademark and intermediary liability are governed by two separate and uncoordinated statutes rather than a single trademark code.

5 DOCTRINAL STRAIN: THE “USE” REQUIREMENT

Section 29 of the Trade Marks Act, 1999 conditions infringement on use, in the course of trade, of a mark identical or similar to a registered mark in relation to identical or similar goods or services, in a manner likely to cause confusion. Each element presupposes an identifiable actor whose conduct constitutes the “use.”

The Delhi High Court’s Division Bench, in *Google LLC v DRS Logistics (P) Ltd*¹⁵ and the subsequent *Google LLC v MakeMyTrip India Pvt Ltd*¹⁶ appeal, held that the invisible use of a registered mark as a keyword in a paid advertising programme constitutes “use in advertising” under the Trade Marks Act, extending the concept beyond visual display on a webpage. Crucially, however, the Court’s reasoning still anchored liability to Google’s own commercial conduct in selling and prioritising the keyword which is an identifiable, repeatable business practice, not a one-off machine generated output. A subsequent contempt proceeding in 2026 in *DRS Logistics (P) Ltd. & Anr. v. Google India Pvt. Ltd. & Ors*¹⁷ confirmed that even this expanded “use” doctrine is read narrowly by the courts. Google was held not to be under a general obligation to proactively monitor all future advertisements for a plaintiff’s marks, only to act on specific complaints, underscoring how far Indian doctrine remains from any duty to police continuously generated content.

Where a metaverse platform’s generative tool produces a virtual item that incorporates a registered brand (having learned the pattern during the training phase), there is no act of reproduction, since no human being has deliberately sought to copy the plaintiff’s mark. This, therefore, goes beyond the “use” of a registered trademark as provided under Section 10(4) of the UK Trade Marks Act, 1994, and Section 29(6) of the Indian Trade Marks Act. Both of these statutes list down the various acts which constitute the “use” of a registered trademark; however, they fail to address situations where an AI system independently “learns” patterns and subsequently produces items that bear a striking resemblance to a registered trademark. It may be argued that Section 10(4) of the UK Trade Marks Act, 1994, and its Indian counterpart, Section 29(6), were drawn with the mindset of a deliberate human act in view. However, even that is not explicitly provided for in either statute. Put another way, there is no provision in either statute that speaks of a scenario where the “user” of the mark is not a natural or artificial person.

¹⁴ Brian M Wheeler, “Trademarks in the Age of AI: The Emerging Legal Battlefield for Brand Owners and Users of Generative AI” (Atkinson, Andelson, Loya, Ruud & Romo, Business Law Journal, 23 June 2025) <https://www.aalrr.com/Business-Law-Journal/trademarks-in-the-age-of-ai-the-emerging-legal-battlefield-for-brand-owners-and-users-of-generative-ai> accessed 2 October 2026; see also Dominique E Smith and Daniel P Mullarkey, “Trademark Risks in the AI Age: Navigating Infringement, Dilution and Genericness” (Polsinelli, 29 October 2025) <https://www.polsinelli.com/publications/trademark-risks-ai-age-navigating-infringement-dilution-genericness> accessed 2 October 2026.

¹⁵ *Google LLC v. DRS Logistics (P) Ltd.*, 2023 SCC OnLine Del 4809

¹⁶ *Google LLC v. MakeMyTrip (India) Private Limited & Ors.*, 2023 SCC OnLine Del 7965.

¹⁷ *DRS Logistics (P) Ltd. & Anr. v. Google India Pvt. Ltd. & Ors*, CS(COMM) 1/2017 (Delhi HC, 15 June 2026), 2026:DHC:5102

5.1 The Cross-Border Nature of the Metaverse and the Problem of Jurisdiction

The metaverse poses a particular challenge to the policing of counterfeit goods, precisely because it erodes the territorial anchors upon which trademark and IP enforcement typically rely: a counterfeit virtual sneaker or handbag ‘sold’ on a metaverse platform may have been minted by a developer in one jurisdiction, hosted on servers in another, paid for in a wallet registered in a third, and ‘worn’ by an avatar accessible to the users everywhere simultaneously. Unlike the physical world, the metaverse provides no fixed location for the infringement to have occurred, because every point of access is effectively a point of sale. Consequently, the threshold question predating the emergence of the metaverse but sharpened by it is which court has jurisdiction over the infringement claim, and against whom?

Courts confronting internet based infringement have historically resolved this via a graduated inquiry into the ‘interactivity’ of the online conduct: the foundational articulation is the sliding-scale test from *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*¹⁸, which allocated websites onto a spectrum of websites, ranging from ‘passive’ websites that simply provide information and support no personal jurisdiction, through those which are ‘interactive’ in the middle, where jurisdiction turns on the level of exchange of commercial information, to sites where defendant knowingly and repeatedly transmits files or carries out transactions with forum residents. A metaverse storefront which allows avatars to browse, customise, and purchase counterfeit virtual goods sits squarely at the interactive-to-active end of the spectrum, making the Zippo framework a natural starting point, but exposing its limits, since it was designed for a different context of static websites.

A second, complementary line of authority is the ‘effects test’ from *Calder v. Jones*¹⁹, where the US Supreme Court held that a forum may exercise personal jurisdiction over a non-resident defendant where the defendant’s conduct is expressly aimed at the forum and causes harm that the defendant knew would be suffered there. Applied to the metaverse, this recasts the inquiry from the mechanics of the platform to the foreseeable locus of injury: if a counterfeit selling avatar or platform knowingly targets consumers or a brand owner’s reputation in a particular jurisdiction, then the effects test allows that forum to assert authority, even without a physical or server based presence there.

Indian courts have had to reconcile both approaches, and the leading authority is *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy*²⁰. There, the Delhi High Court held that mere accessibility of an allegedly infringing website within the forum (Delhi) is not sufficient to establish jurisdiction under Section 20 of the CPC in a passing off or trademark action: the plaintiff must show that the defendant ‘purposefully availed’ itself of the jurisdiction of the forum and that this targeting caused actual injury, either commercial or reputational, within that forum. The Court expressly warned against uncritical importation of the Zippo scale, noting that interactivity alone, without demonstrable targeting and effect, cannot found jurisdiction, particularly at the pre-trial injunction stage, where the plaintiff bears the burden of a *prima facie* showing of both purposeful availment and resultant harm.

Read together, these three authorities frame the jurisdictional problem the paper must confront: the metaverse is, by definition, the most ‘interactive’ and ‘targeting capable’ environment yet devised, satisfying Zippo’s active end and *Calder*’s foreseeability prong comfortably. The avatar economy is constructed purely on real-time, individualised commercial exchange. Yet Banyan Tree’s insistence on

¹⁸ *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997)

¹⁹ *Calder v. Jones*, 465 U.S. 783 (1984)

²⁰ *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy*, CS(OS) 894/2008 (Delhi HC, 2009)

purposeful availment and demonstrable in-forum injury demands more than platform-wide interactivity: it is asking for evidence that a particular counterfeiting actor targeted a particular market. This is exactly where enforcement stalls in practice: metaverse platforms are architecturally borderless but IP remedies are doggedly territorial, forcing brand owners to a fragmented, jurisdiction-by-jurisdiction pursuit of infringers who don't reside in any jurisdiction at all.

5.2 Similarity and Confusion at Machine Scale

In *Cadila Health Care Ltd v Cadila Pharmaceuticals*²¹ the Supreme Court outlined seven factors for assessing deceptive similarity, which include the nature of the marks, the degree of resemblance, the nature of the goods, the similarity of the goods' character and purpose, the class of purchasers, the mode of purchasing and other surrounding circumstances. The test is based on a comparison between two comparably fixed marks and the Court's own emphasis on protecting consumers from confusion which is heightened in that case by the public health stakes of pharmaceutical mislabelling, is reflective of a paradigm of one product measured against one mark.

A generative model can produce thousands of subtly distinct renderings of a branded good from a single prompt, none identical to any prior output and none identical to the registered mark, yet all individually capable of evoking the brand's trade dress. Applying Cadila's factor-by-factor comparison to a single generated instance may yield a finding of no deceptive similarity even where the pattern of generation, taken as a whole, systematically trades on a brand's goodwill. The seven factor test was not built to assess a generative pattern; it was built to assess a discrete pair of marks.

Getty Images v Stability AI is instructive here as well. The UK High Court's finding of infringement was expressly described as "historic and extremely limited," confined to particular instances where the model reproduced Getty's watermark in a manner capable of causing confusion. The judgment did not, and on the pleadings before it could not, address the systemic pattern of generation. This is precisely the limitation that a Cadila style, instance-by-instance test would replicate if applied to Indian virtual counterfeiting disputes.

A further Cadila factor, the nature and similarity of the goods themselves, assumes that both the registered mark and the impugned use attach to comparable categories of goods or services. A generated avatar skin or virtual handbag is not, in any conventional sense, in the same category of goods as the physical product the registered mark denotes. It is a rendering, often free or nearly costless to produce, with no supply chain, no manufacturing cost and no physical scarcity. Indian courts have not yet had occasion to decide whether a virtual asset is a "similar good" to its physical counterpart for infringement purposes, and the *Nike v StockX* litigation's unresolved "digital good versus digital receipt" debate shows that even well resourced foreign litigants have not settled the point.

5.3 Dilution Without Confusion

Because generated virtual assets frequently fail the "similar goods" threshold, a confusion based cause of action under Section 29(1) or (2) may simply not be available. However, Section 29(4) of the Trade Marks Act protects marks with an established reputation in India against use on dissimilar goods or services where that use takes unfair advantage of, or is detrimental to, the distinctive character or repute of the

²¹ *Cadila Health Care Ltd v Cadila Pharmaceuticals Ltd* (2001) 5 SCC 73

mark, without requiring proof of consumer confusion at all. On its face, this is a better doctrinal fit for virtual counterfeiting. A luxury handbag brand's reputation can be diluted by a flood of near identical AI-generated virtual renderings even if no metaverse user is actually confused into thinking the platform is the brand's authorised seller.

In *Rolex SA v Alex Jewellery Pvt Ltd*²² the Delhi High Court granted interlocutory relief under Section 29(4) of the Trade Marks Act, holding that a mark's established reputation in India evidenced through long use, extensive advertising and international registration sufficed to trigger dilution protection even outside the mark's registered goods category, without any need for the mark to first be listed as "well-known" by the Registrar under Section 11. This built on the Supreme Court's earlier recognition, in *N.R. Dongre v Whirlpool Corporation*²³, of transborder reputation as a basis for protecting a foreign mark even before extensive use within India. Together, these cases show Indian courts willing to protect brand distinctiveness across dissimilar goods categories without insisting on confusion. This can be considered as a doctrinal posture well suited, in principle, to virtual assets that resemble a brand's trade dress without competing in the same market.

Dilution doctrine still requires a court to identify the impugned "use" and to assess "unfair advantage" or "detriment" against a specific instance of that use. It therefore inherits the instance-by-instance limitation. A court can find dilution in one generated output, or a documented pattern of outputs put before it as evidence, but has no existing mechanism to address the platform's generative capacity as such, independent of specific instances a plaintiff happens to capture and plead. Reframing the cause of action from confusion to dilution therefore removes one obstacle, the similar goods requirement, without removing the deeper one, the need for a discrete, provable act of use.

5.4 Design Law as a Parallel and Also Insufficient Regime

A brand's protected trade dress is often, or sometimes alternatively, protectable as a registered design. Section 2(d) of the Designs Act, 2000 protects the features of shape, configuration, pattern, ornament, or composition of lines or colours applied to an article, judged solely by the eye but expressly excludes anything that is itself a trademark. In principle, a metaverse platform's generative reproduction of a handbag's distinctive silhouette could trigger a similar protection as a registered design as readily as it could trade dress under the Trade Marks Act, giving a rights holder a second statutory route into the same underlying problem.

Indian courts have held that design and trademark protection for the same feature are not mutually exclusive. In *Mohan Lal v Sona Paint & Hardware*²⁴, a Full Bench of the Delhi High Court held that registering a feature as a design places no limitation on its use as a trademark by the registrant, so that a passing off action lies once that use has generated goodwill. Composite suits for design infringement and passing off for the same trade dress are not uncommon, as the Delhi High Court's own jurisprudence in *Crocs Inc USA v Bata India Ltd & Ors*²⁵ shows, but they are limited to elements beyond the registered design. Design registration also has a scale problem. Infringement under the Designs Act also requires a comparison between the infringing article and the registered design, which involves the same sort of

²² *Rolex SA v Alex Jewellery Pvt Ltd* 2009 (41) PTC 284 (Del)

²³ *N.R. Dongre v Whirlpool Corporation* AIR 1995 Del 300, 1995 (34) DRJ 109, affirmed (1996) 5 SCC 714

²⁴ *Mohan Lal v Sona Paint & Hardware* (AIR 2013 Delhi 143)

²⁵ *Crocs Inc. USA v. Bata India Ltd. & Ors.*, 2019 (78) PTC 1 (Del), decided 18/24 January 2019

discrete comparison issue that the Cadila and Louboutin tests grapple with. Adding a third statutory regime only adds a third forum for litigation without resolving the underlying issue that none were designed to handle continuously generated articles rather than discretely manufactured ones.

6 PLATFORM ACCOUNTABILITY UNDER SECTION 79

6.1 The Safe Harbour and the Active-Participant Test

Section 79 of the Information Technology Act, 2000, which provides a safe harbour for intermediaries, was also engaged in *Christian Louboutin SAS v Nakul Bajaj & Ors*²⁶. The Delhi High Court found that an e-commerce portal was not insulated by Section 79's safe harbour when it went beyond a mere directory function by guaranteeing authenticity, utilising the plaintiff's trademarks in its meta tags, or exercising control over fulfilment, all of which constituted "active participation" in the infringement. The Court provided an extensive but non-exhaustive list of activities that could be indicative of such participation.

A platform that makes use of its own generative tool to produce an infringing asset in response to a user's query arguably goes beyond even the conduct outlined in the Louboutin test. The platform does not merely facilitate a transaction between a buyer and seller, it actively creates the infringing content through its own tool, which is then profited from by the platform. This appears to place it even further up the slope towards "active participation" than even a curating marketplace would, since the tool itself, not an independent seller, is the source of the infringement.

The Louboutin test was framed in terms of actions that a company could take to facilitate or benefit from infringement, each of which involved some exercise of discretion on the part of the curator. Generative AI infringement, on the other hand, arises from a model's statistical propensities, which may not be the result of any particular intention on the part of the curator. Courts evaluating a Section 79 claim in the context of a generative AI dispute would have to determine whether the mere operation of a system that regularly produces infringing content constitutes "active participation" in infringement, which the Louboutin jurisprudence did not directly address.

Section 79(3)(b) of the IT Act, which governs the safe harbour, mandates that an intermediary must expeditiously remove unlawful content upon receiving actual knowledge or awareness of its existence. In *Shreya Singhal v Union of India*²⁷, the Supreme Court directed that the "expeditious" removal of unlawful content would normally entail taking action upon receipt of a court order or a government directive; a private complaint would not be sufficient to satisfy the requirements of Section 79(3)(b). This places the onus of detecting unlawful content on the complainant rather than the intermediary, which has to remove it only once it receives such an order or directive. The notice and takedown regime which forms the basis of Section 79 does not seem to apply as directly to a generative programme as it does to a human moderator. If a trademark owner were to notify a generative programme operator that a certain output infringes upon their mark, the operator would be entitled to remove that particular output, but the mere removal of that output would not necessarily be sufficient to prevent future infringing outputs, since those would constitute separately infringing acts by the operator. The next infringing output could be completely different from the first one, and the trademark owner's knowledge of the first output would

²⁶ *Christian Louboutin SAS v Nakul Bajaj & Ors* (2018 SCC OnLine Del 12215)

²⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1

not be sufficient for them to be entitled to remove the second one. In short, the notice and takedown regime leaves trademark owners in a weaker position than they would like; they cannot simply rely on Section 79 to prevent a continuous stream of infringing outputs so long as those are not specifically notified to the programme operator.

6.2 India's Emerging Regulatory Response to Generative AI

India has been quick to respond to the phenomenon of generative AI, even if not specifically in the context of IP, in its own way. The Ministry of Electronics and Information Technology issued advisory guidelines on 1 March 2024 for intermediaries and platforms that use AI, generative AI, or algorithms. These guidelines stated that such entities must ensure that their computer resources do not permit any bias or discrimination or threaten the integrity of the electoral process, and that under-tested or unreliable AI models be made available only with the explicit permission of the Government and after labelling the possible fallibility or unreliability of their output. Further, the advisories indicated that such platforms must label, or embed with permanent unique metadata or an identifier, synthetically created content that could be used as misinformation or a deepfake. Industry concern led to a revised advisory on 15 March 2024, which replaced the obligation to obtain prior government permission with a labelling requirement, although it remained anchored to Rule 3 of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Both built on an earlier advisory of 26 December 2023 on misinformation and deepfakes.²⁸ All in all, these advisories make it clear that MeitY views generative AI deployment as involving enhanced due diligence obligations under the current Intermediary Guidelines but have so far focused on issues related to electoral integrity, bias, and unlawful content, leaving open the regulatory space for trademark and trade-dress reproduction.

7 COMPARATIVE PERSPECTIVES

7.1 European Union

In the joined references *Louboutin v Amazon*²⁹, the CJEU ruled that an online marketplace may be held liable for trademark infringement by third-party sellers if an average, reasonably informed consumer may believe that the marketplace itself is the source of the goods on its site, such as where the marketplace prominently displays its own trademarks alongside listings and offers its own delivery services for the goods. A similar “average consumer” test appears in the EU’s Digital Services Act (Regulation 2022/2065)³⁰, which in Art 6(3) withdraws the hosting exemption for consumer protection liability where a platform’s presentation “would lead an average consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.” This consumer perception based test is potentially more directly applicable to the liability of Gen AI platforms than India’s “conduct based

²⁸ Ministry of Electronics and Information Technology, Advisory No. eNo.2(4)/2023-CyberLaws-3 (1 March 2024), superseded by Advisory No. eNo.2(4)/2023-CyberLaws-3 (15 March 2024); Ministry of Electronics and Information Technology, Advisory No. eNo.2(4)/2023-CyberLaws-2 (26 December 2023); Press Information Bureau, ‘MeitY issues advisory to all intermediaries to comply with existing IT rules’ (26 December 2023) <https://pib.gov.in/PressReleaseDetail.aspx?PRID=1990542> accessed 2 October 2026.

²⁹ *Louboutin v Amazon* (Cases C-148/21 and C-184/21, CJEU, 22 December 2022)

³⁰ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

active participant” test, as it focuses on the impression created by the former’s presentation rather than actions.

7.2 United States

The MetaBirkins case illustrates the US courts’ approach to trademark infringement of expressive digital works, which is governed by the Rogers test³¹, under which artistic use of a trademark is permissible if it has artistic relevance and is not explicitly deceptive. Nike v StockX, which was settled without a ruling on the NFT specific claims, raises more foundational issues about whether an AI or blockchain mediated representation of a branded good constitutes a “good” for trademark law purposes, and if so, what constitutes “use” of the mark.

7.3 United Kingdom

Getty Images v Stability AI³² is the closest analogy to the situation raised by Nike and MetaBirkins in UK law. The narrow finding of infringement in Getty Images v Stability AI highlights the limited ways in which current trademark law can address AI training data and output, focusing as it did on the reproduction of watermark content, a fortuitous fact particular to the case. The UK courts have yet to grapple directly with the issue of trade dress reproduction by generative AI.

7.4 Singapore: A Soft-Law Comparator

A fifth jurisdiction merits brief discussion as it takes a significantly different approach to the issue: Singapore. Unlike the US, EU, UK, and India, which have grappled with the issue in courts, Singapore has thus far responded to the threats to IP posed by generative AI at the policy level. In particular, the Infocomm Media Development Authority and the AI Verify Foundation have issued a Model AI Governance Framework for Generative AI on 30 May 2024³³, after a public consultation begun in January 2024.

The framework contains nine pillars for trustworthy AI, among which are intellectual property and content provenance risk management measures, including recommendations for content watermarking and provenance tracking rather than liability defaulting. Although Singapore’s courts have not yet addressed the issue, its approach of developing a voluntary, advisory framework for content provenance risk-management for generative AI offers useful insight nonetheless. It demonstrates that a soft law approach, of the type that India’s Ministry of Electronics and Information Technology has begun to develop for other AI risks, may serve as an effective starting point for addressing trademark and content provenance concerns without waiting for court cases to intervene.

None of these jurisdictions have developed a comprehensive legal framework for holding platforms liable for their users’ AI driven prompt triggered counterfeits. India is further differentiated within this group by the lack of coherence between TM and IT law, which has complicated enforcement in both physical and digital goods spaces. The EU’s average consumer test, the US’s Rogers test, and the UK’s narrow infringement finding all address some aspects of the liability risk, but none propose a unified solution that incorporates a threshold “use” test, similarity/dilution test, and platform accountability test.

³¹ Rogers v. Grimaldi, 875 F.2d 994 (2d Cir. 1989)

³² Getty Images (US) Inc & Ors v Stability AI Ltd [2025] EWHC 2863 (Ch)

³³ Infocomm Media Development Authority, ‘Artificial Intelligence in Singapore’ (IMDA) <https://www.imda.gov.sg/about-imda/emerging-technologies-and-research/artificial-intelligence> accessed 23 September 2026.

8 TOWARD A COORDINATED ENFORCEMENT FRAMEWORK

8.1 Clarifying “Use” for Generative Output

Section 29 could be clarified to bring it in line with the “invisible keyword” rulings in DRS Logistics and MakeMyTrip, which held that a search engine’s use of a trademarked keyword to improve search results, even when the keyword was not visible to the user, constituted “use” of the mark. Similarly, a platform’s generative reproduction of a registered trademark, including trade dress and getup, should be considered “use” regardless of whether the mark was explicitly named in the user prompt. Such a clarification would be consistent with the generative AI specific amendments made to the IT Rules in 2026, which explicitly require notice and takedown of AI-generated deepfake audiovisual content. It should also extend to include trade dress reproduction, as suggested by the prompt without name problem, and should apply to Section 29(1), 29(2) and 29(4) dilution claims to avoid the similar goods exception.

8.2 A Generative-Active-Participant Test under Section 79

The Louboutin style factors could be supplemented with a presumption of reduced safe harbour for platforms whose users generate infringing content using the platforms’ own tools, as opposed to independently uploaded content, thus recognising the former as the active participants in infringement. This presumption should be rebuttable by evidence of the platforms’ documented filtering safeguards, thus distinguishing between platforms that take reasonable measures to prevent infringement and those that do not. The generative active participant presumption would dovetail with the clarified “use” test to establish direct liability for the platforms that host or distribute infringing AI content. It would also address the knowledge standard by shifting the burden of proof from whether the platform knew of a particular infringing output to whether it took reasonable steps to prevent such outputs.

8.3 Institutional Coordination

A referral mechanism between the Trade Marks Registry, the Central Consumer Protection Authority, and the Ministry of Electronics and Information Technology would allow trademark infringement complaints to be processed once, rather than split between different agencies with differing jurisdictions. This would reduce the burden on trademark owners, who would not have to pursue parallel remedies under the TM Act and the IT Act. In effect, it would allow such complaints to be directed to a single nodal agency.

8.4 Extending MeitY’s Due-Diligence Advisories to Brand Protection

Rather than develop a new legal framework, India could look to extend the due diligence advisories already issued by MeitY for other areas of AI governance to trademark and trade dress protection. Metaverse platforms that employ generative AI tools could be required to adopt brand- and get-up-specific filtering measures comparable to the prompt filtering guidelines already adopted voluntarily by some AI developers to avoid deepfake harms. This would utilise an existing advisory mechanism to establish a minimum standard of liability avoidance for platforms hosting AI generated content, without requiring new legislation. It would also serve as a basis for further clarifications on trademark and trade dress harms

that MeitY may seek to issue separately. This recommendation is potentially the most immediately viable, as MeitY has already issued two advisories concerning generative AI in 2024.

While India's IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026³⁴, represent a major step towards regulating synthetic media and require notice and takedown of AI-generated audiovisual content, the rules are primarily aimed at deepfakes, impersonation, and misinformation, with limited guidance on AI driven trademark infringement. Rule 3(1)(d) and 3(3)(a)(ii) of the amended rules apply primarily to AI generated deepfake content and require traceability, embedded provenance metadata, and a compressed takedown window for such content.

8.5 Verification and Audit

This suggests a system of periodic third-party audits of platform filtering mechanisms, with the ability to rely on actual content rather than self reported compliance. These could be combined with the Trade Marks Registry's own well known marks determinations under Section 11 to create a feedback loop between the Registry and the platforms.

The preceding recommendations are not mutually exclusive; rather, they suggest a potential sequence of reforms that would collectively address the enforcement challenges associated with AI counterfeiting in the metaverse. Statutory clarification of the "use" standard would establish a legal baseline for trademark infringement by AI generated content. The "generative-active-participant" presumption would supplement it by addressing the safe harbour concerns for platforms that host or distribute such content. Institutional coordination would reduce the procedural and jurisdictional barriers for trademark owners seeking remedies, while audit and verification mechanisms would provide a supervisory function over the entire system and inform future policy updates.³⁵

Return to the generative wardrobe tool described earlier in this paper, where a brand-blind prompt resulted in a virtual handbag infringing on a luxury label's trade dress. Under the clarified "use" standard discussed above, the platform's output would constitute "use" of the plaintiff's mark. Under the rebuttable active participant presumption, the platform would be held liable for hosting such content absent documented trade dress filtering, which would be necessary for it to adopt if it wished to continue operating in India, as suggested in Part 8.4 above. The trademark owner, for its part, would have the option to file a consolidated complaint to the single nodal agency suggested in Part 8.3, rather than separately litigating the trademark infringement, passing off, and information technology violations. The scenario described at the beginning of this paper as a doctrinal conundrum is transformed, under these recommendations, into a concrete compliance procedure with predictable consequences for the parties involved.

³⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E) (10 February 2026), amending the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, GSR 139(E) (25 February 2021).

³⁵ Indranath Gupta and Lakshmi Srinivasan, 'Evolving Scope of Intermediary Liability in India' (2023) 37 International Review of Law, Computers & Technology 294.

9 PRACTICAL IMPLICATIONS FOR RIGHTS HOLDERS AND PLATFORMS

9.1 For Brand Owners

Until such statutory and policy clarifications as discussed above are made, brand owners are not without recourse. Trademark portfolios should include registrations of trade dress and getup in addition to word marks, to capture the likelihood of AI driven infringement. Given the prompt without brand name scenario, a trademark registration covering only a brand's word mark leaves its visual elements vulnerable to reproduction by generative tools. Second, brand owners should consider building a paper trail in support of a potential dilution claim under Section 29(4) in anticipation of infringement, as demonstrated by the *Rolex v Alex Jewellery* case, where the court found that the plaintiff's extensive advertising, international sales, and use of trademarks in connection with its goods were relevant to its finding of dilution.

9.2 For Platforms

Platforms that employ generative tools should consider the implications of the new safe harbour rules on their operations. Verifiable trade dress and brand name filtering practice will become a necessity for any platform that wishes to continue operating in India. This is particularly true for multi jurisdictional platforms, which would benefit from adopting the most stringent of the regional standards, such as the EU's average consumer test, to avoid the need to maintain separate compliance practices for each jurisdiction.

9.3 For Regulators

The recommendations for the Trade Marks Registry and the Ministry of Electronics and Information Technology are the most immediately tangible, as they involve no new legislation at all. The regulator could utilise the existing advisory framework to send a message to the industry that trademark and trade dress reproduction fall within the scope of the IT Act's existing obligations. This could be done as early as the next quarter, without requiring any legislative change, by issuing guidelines similar to those issued by Singapore's Infocomm Media Development Authority and AI Verify Foundation in May 2024.

10 LIMITATIONS AND SCOPE

This paper offers recommendations based on a review of doctrinal and policy responses in other jurisdictions. It does not attempt to quantify the scale of the threat to trademarks posed by prompt driven AI counterfeits in the metaverse. An empirical assessment would require the cooperation of the platforms to identify the prevalence of AI generated counterfeits in their domain, something that this author is currently attempting to quantify in her ongoing research. Finally, a word on copyright: while this paper focuses on trademark law, the same AI generated works raise complex questions for copyright law, including the authorship and originality of the output. These questions fall outside of the scope of this paper but will be addressed separately in due course.

11 CONCLUSION

Treating AI-driven virtual counterfeits as a variation of existing online counterfeits understates the shift already underway in the courts in jurisdictions such as the EU, the US, and the UK. Enforcement models

that have been adequate for static, non-generative infringing content, be it “use” in the case of trademarks, “substantial similarity” for copyrights, or the “average consumer” test for passing off, may prove insufficient in the face of prompt driven, generative AI counterfeits at the scale suggested by Nike and the MetaBirkins dispute. The fragmentation of India’s trademark and information-technology law adds to the challenge, making early doctrinal and institutional coordination, rather than waiting for the equivalent of the Getty Images v Stability AI dispute to occur in India, the preferable option. The five part recommendations articulated in this paper seek to contribute to that coordination by building upon the frameworks already available in the Indian law landscape.

* * *