Alliance Journal of Intellectual Property Law (AJIPL)
Volume: 3, Issue: 1, 2025 | e-ISSN: 2584-0363

ARTIFICIAL INTELLIGENCE AND TRADEMARK ENFORCEMENT IN E-COMMERCE: RECONCEPTUALISING PLATFORM GOVERNANCE, ACCOUNTABILITY, AND RIGHTS PROTECTION

Aditya Singh[1] *& Dr.Ujwal Prabhakar Nandekar*[2]

ABSTRACT

The rapid growth of e-commerce has accentuated the challenges that trademark protection faces today, particularly in relation to online counterfeiting, unauthorized use of marks, and trademark dilution on global online market platforms. Empirical research today suggests that international online trade in counterfeit and pirated goods is estimated to amount to trillions of dollars every year, and that online platforms have increasingly become the main conduit of infringement of intellectual property rights of various kinds.[3] The traditional tools of trademark protection today have proved inefficacious in dealing with modern trademark infringements in the digital space.

In this context, the concept of artificial intelligence (AI) has come into the picture as a possible enforcement mechanism that could improve the monitoring of trademarks and quickly respond to violations detected through image recognition algorithms and natural language processing methods. In fact, there has been a recent spate of state-level implementations of AI-based governance platforms in India that emphasize the relevance of technologically supported models

1. Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU) Pune-411014, Maharashtra, India (SIU).
2. Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR), Symbiosis Law School, Pune (SLS-P), Symbiosis International (Deemed University) (SIU) Pune-411014, Maharashtra, India (SIU).
3. Organisation for Economic Co-operation and Development & European Union Intellectual Property Office, Global Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact 11–15 (2023), https://www.oecd.org/gov/global-trade-in-counterfeit-and-pirated-goods-2023.pdf.

of governance. In this context, it becomes clear that there could be legal and ethical implications associated with the use of AI as a mechanism for enforcing trademarks.

This paper critically analyzes the weaknesses of the current frameworks of trademark enforcement from the perspective of e-commerce and explores the potential role of AI technology as a complementary regime rather than a substitute for adjudicative decision-making.

Using a methodology that combines doctrinal research approaches with comparisons and case studies of AI-powered trademark protection mechanisms. The paper critiques the practical advantages as well as the normative challenges of AI-facilitated enforcement. Lastly gave recommendations that seek a balance between the principles of technology and trademark protection will be made.

Keywords: Artificial Intelligence, Trademarks, E-commerce, Intellectual Property, Brand Protection

INTRODUCTION

E-commerce has emerged as one of the key pillars of retailing across the world and has altered the manner in which products and services are promoted, distributed, and consumed. With the advent of internet accessibility at a rapid pace, businesses have found it exceptionally easy to target customers across borders. According to recent estimates, total e-commerce retail sales are anticipated to touch over USD 4.3 trillion in 2025.[4] However, this new reality of retailing across borders has also created new legal concerns with regard to the protection of trademarks, which include cyber counterfeiting.

Unlike the traditional offline market, which is geographically limited by national boundaries and traditional inspection systems, the online market is borderless. This inherent nature has led to the widespread problem of trademark violations in the form of domain name spoofing, keyword advertising, copycat advertising, and deceptive cyber branding. The current framework of enforcing rights to marks in general depends on geographical jurisdiction, litigation after the infringement has occurred, and notice-and-takedown provisions, which have not been very effective in taking on the magnitude and pace associated with cyberspace violations. The time- and cost-associated problems related to litigation make it even more difficult for rights owners in general, especially small- and medium-sized businesses.

The challenges with the conventional regimes have encouraged an increasing concern with technology-intensive approaches for enforcing trademarks. One of these emerging technologies is artificial intelligence (AI), which shows the potential of serving as a regulatory adjunct with the ability to improve trademark monitoring by means of image recognition, machine learning, and natural language processing technologies. Trademark monitoring is supported by enabling automated monitoring of internet marketplaces, social networking sites, and other digital spaces, which provides an effective means of making early identifications or immediate responses to acts of trademark infringement. On the level of regulatory policy, current developments occurring in India, with the adoption of AI-driven regulatory tools by the government of Telangana, demonstrate an underlying movement towards the integration of emerging technologies in regulatory frameworks.[5]

Despite the expanding use of AI-driven brand protection systems by online platforms and IP owners, important legal and social issues remain. AI-powered enforcement systems currently face issues such as bias in algorithms, data protection, fairness in process, and inconsistencies in jurisdiction in various systems of law. Related developments in comparative jurisdictions make it clear that, on the one hand, online platforms

4. United Nations Conference on Trade and Development, Global E-commerce Sales Surpass Trillions Amid Digital Expansion (2024), https://unctad.org/topic/ecommerce-and-digital-economy.
5. Press Information Bureau, Government of India, Telangana Adopts Artificial Intelligence and Emerging Technologies for Governance Reforms (September 4, 2024), https://pib.gov.in/PressReleasePage.aspx?PRID=2054116.

have been mandated to undertake proactive due diligence by systems such as that of the European Union, while on the other hand, most systems of law have been applying or remain dependent on the intermediary immunity approach.[6]

In this context, this research paper fills a considerable gap in the area of research because it has not yet been explored in a coherent and well-articulated legal framework to effectively incorporate AI technology in the enforcement of trade marks in a manner that would improve its effectiveness without diminishing trademarks and fair competition, and due process. The research paper uses a doctrinal research method and a comparative analysis in relation to the legal implications of using AI technology in brand-protection systems in a manner that examines its positive and negative implications in terms of improving its effectiveness in trade mark activities and providing appropriate legislative and strategic proposals in this regard to effectively improve trademark protection in the e-commerce environment based on a balancing of normative provisions in this area.

UNDERSTANDING TRADEMARKS IN THE DIGITAL ENVIRONMENT

The existence of trademarks is essential to market economies in that they enable a consumer to distinguish the commercial origin of a product or service. The classic economic theory of trademarks considers trademarks not only as proprietary signs but also as devices that reduce search costs for consumers and facilitate fair competition.[7] Although these roles have remained valid under the current digital economy scenario, the technology infrastructure of e-commerce sites has drastically altered the display, consumption, as well as misuse of trademarks.

As such, trademark rights are territory-specific on matters such as enforcement, and such enforcement is generally contingent on territory-specific markets, consumer perception, and human intervention sales. Online marketplaces, on the other hand, function on territory-nonspecific seller networks and automated advertising tools, thus largely diminishing the specific nature of the territory.[8] Moreover, with the use of online marketplaces, trademarks are not intuitively seen on packaging and at the point of sales, but on results pages, product pages, advertising links, and other platform-generated suggestions. Thus, trademark infringement on the Internet can actually be heightened not only by an Internet user's actions but also by platform preferences elsewhere on the Internet that aim at visibility, interaction, and convenience.

Such is the transformation that has resulted that the infringement of trademark in the context of e-commerce is now qualitatively different in character when compared with the infringement of trademark in the physical world. For example, the infringement of a trademark is no longer episodic but is now continuous in nature. It is no longer localized; in other words, infringement of trademark in e-commerce is now scalable. It is also often not traceable.[9]

Trademark Infringement in E-Commerce

Online e-commerce sites are middleman platforms that bring together a huge number of sellers as well as consumers, with a massive dependence on automated services for managing listings, advertisements, and content. Although these platforms provide huge benefits of scalability and ease of access as well as operational efficiency, they at the same time provide a huge risk environment when it comes to the enforcement of

6. Council Regulation 2022/2065, articles 26–28, 2022 Official Journal of the European Union (L 277) 1 (Digital Services Act).
7. William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 Journal of Law and Economics 265, 269–72 (1987).
8. Graeme B. Dinwoodie, *Developing a Private International Law of Trademarks*, 24 Berkeley Technology Law Journal 161, 170–73 (2009).
9. Organisation for Economic Co-operation and Development & European Union Intellectual Property Office, Global Trade in Counterfeit and Pirated Goods 45–48 (2023).

trademark rights. The major loophole lies in the fact that there is a lack of screening of vendors and a dependence on "user-generated content" along with algorithm-driven or popular content promotion; henceforth, there is a huge risk of spreading counterfeit merchandise quickly on these sites.[10]

In today's digital or online world, the major methods of counterfeiting or violation of trademark on these sites include counterfeiting, cybersquatting, and misleading keywords.

1. Counterfeit and Unauthorized Products- Online counterfeiting is one of the major challenges faced by trademark protection on e-commerce platforms. Online counterfeits often copy registered trademarks, logos, packaging, and trade dress. This, in turn, meets the legal requirement of the "likelihood of confusion" principle established under trademark law. Contrary to the conventional counterfeiting ring, online counterfeiters utilize the anonymity of platforms, global supply chain disunity, and territorial fragmentation as a means of staying undetected and unenforced.[11] This is because online infringers continue iterating after taking down the domains selling the infringing goods.

In particular, the lack of physical examination in online transactions raises concerns with regard to consumer vulnerability. The purchase decision to a large extent relies upon visual representations of the product in terms of picture and description in cyberspace; hence, the likelihood of mistaken identification based upon visual similarity is considerable. Figure 1 below contrasts a licensed sports jersey with a counterfeit product advertised in cyberspace.

In the example presented in Figure 1, it is quite apparent that the counterfeit product has reproduced the registered trademark and trade dress; however, a difference in quality becomes apparent only upon purchase. Counterfeit goods directly affect the source-indicating function of a trademark.[12]

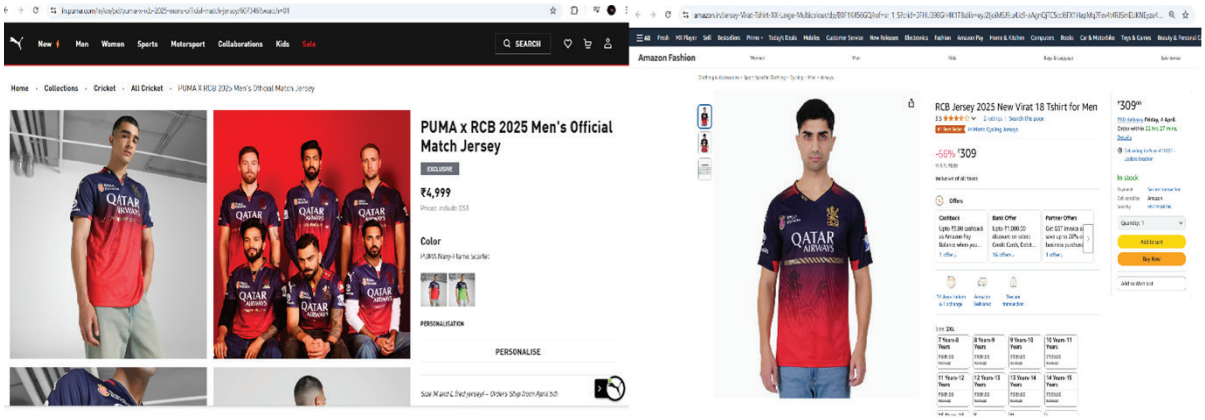


Figure 1: Comparison between original and fake RCB jersey advertisements on an e-commerce website. (Source: Created by the Authors)

2. Cybersquatting & Domain Misappropriation- Cybersquatting refers to the act or process whereby an individual registers or uses domain names identical or confusingly similar to established trademarks, with bad faith intentions.[13] Domain names play vital brand identifiers in the

10. Ariel Ezrachi & Maurice E. Stucke, Virtual Competition 83–87 (2016).
11. World Intellectual Property Organization, Trademark Law and Practice 17–20 (2nd edition 2021).
12. European Union Intellectual Property Office, Online Trade in Counterfeit Goods: Risks and Policy Responses 22–25 (2022).
13. Jonathan Weinberg, *ICANN and the Problem of Cybersquatting*, 50 Duke Law Journal 187, 190–94 (2000) https://scholarship.law.duke.edu/dlj/vol50/iss1/5.

digital economy. Cybersquatters use deceptive domains identical or confusingly similar to established brands, support counterfeiting, phishing scams, and theft of consumer data, consequently resulting in economic losses for brand owners.

Cybersquatting appears to require a response that can be achieved only via greater international cooperation in order to adequately address such issues, rather than simply being dealt with by reactive or remedial measures currently in place, such as cases under the Uniform Domain Name Dispute Resolution Policy or cases based on passing off in domestic trademark law.[14]

3. Keyword Advertising and Trademark Use- The practice of using trademarks in advertising search engines raises complex questions in relation to trademarks and antitrust laws. Even when engaging in comparative advertising through search engine advertising, there might be a misleading of the public through the use of trademarks in a way that attracts the public using deceptive means.[15] The lack of human intervention in advertising makes it difficult to attribute liability when there is infringement in advertising results that are attributed automatically through the search engine. Traditional advertisement infringement laws are difficult in human-controlled advertisement systems are even more difficult in algorithm-driven advertisement systems.[16]

4. Online Imitation and Brand Impersonation- The internet and digital marketplaces have also seen the rise of lookalike sites, fake social media profiles, and deceptive seller pages that mimic well-known brands. This abuse relies upon consumers' reliance upon brand recognition and visual branding in an effort to facilitate fraudulent purchases, counterfeit goods, identity theft, and other illicit activity. The rapidity at which impersonator profiles may be developed underscores the shortcomings of a system of enforcement reliant solely upon notification.[17]

5. Content Regulation and Trademark Protection- The platform economy is built on user-generated content, which is also the origin of difficult trademark problems. On the one hand, a fine balance of protection of trademarks and freedom of expression, in particular, the freedom of parody, political statement, or non-commercial usage needs to be ensured**.** Over-regulation may lead to private censorship; under-regulation facilitates large-scale trademark abuse.[18] Moreover, this dilemma implies, in turn, the increasing use of AI-enhanced trademark enforcement methods, which will be addressed in the following sections.

CURRENT LEGAL POSITION AND ITS LIMITATIONS

Trademark enforcement depends traditionally on a mix of private and public law mechanisms, including cease-and-desist notices, civil litigation, and border enforcement measures. While cease-and-desist letters provide a low-cost opening salvo, their deterrent effect is low when issued against repeat or anonymous online infringers. Civil litigation, doctrinally sound, often proves poorly fitted for the digital context due to high costs, jurisdictional complicating factors, and procedural delays-all issues that disproportionately hit small and medium trademark holders.[19] Customs enforcement mechanisms, which authorities take action to intercept counterfeit goods at the national borders-remain viable in physical trade but cannot meet the challenge of digitally mediated

14. Uniform Domain Name Dispute Resolution Policy paragraph 4(a); The Trade Marks Act, 1999, section 27 (India).
15. Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 Houston Law Review 777, 784–89 (2004) https://scholarship.law.bu.edu/faculty_scholarship/875.
16. Google Inc. v. MakeMyTrip (India) Pvt. Ltd., 2022 SCC OnLine Del 1143.
17. WIPO, *Digital Brand Protection Report* 31–34 (2021).
18. Rebecca Tushnet, *Gone in Sixty Milliseconds: Trademark Law and Cognitive Science*, 86 Texas Law Review 507, 532–35 (2008) https://scholarship.law.georgetown.edu/facpub/792.
19. Irene Calboli & Jane C. Ginsburg, *Trademark Litigation in the Digital Age*, 92 New York University Law Review 1310, 1321–24 (2017) https://scholarship.law.tamu.edu/facscholar/1546.

transactions where goods are portioned, shipped directly to customers, or intermediated through cross-border platforms.[20]

Intermediary Liability and Safe Harbour Regimes

The central legal tension within e-commerce trademark enforcement relates to the regulation of online intermediaries. Trademark infringement primarily falls under Section 29 of the Trade Marks Act, 1999, in terms of Indian law, which presumes a direct infringing actor.[21] E-commerce platforms are not direct sellers but rather intermediaries. Their liability is consequently reviewed through the safe harbour mechanism under Section 79 of the Information Technology Act, 2000, where conditional immunity is accorded to intermediaries functioning as passive conduits with no actual knowledge of unlawful material.[22]

This framework corresponds to a wider trend at the global level. In the United States, for example, Section 230 of the Communications Decency Act, 1996 limits intermediary liability, and in the European Union, the e-Commerce Directive has traditionally relied on a notice-and-takedown model for hosting providers.[23] Such regimes were aimed at allowing innovation and the freedom of expression within the early internet ecosystems. Nonetheless, they have become more and more incongruent in modern e-commerce platforms that operate by actively curating content through the use of algorithms and advertising technologies, as well as through ranking mechanisms.

Evolving Indian Regulatory Obligations in India

Understanding these shortcomings, India has, over the years and as thought is embodied in Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,[24] amended in 2022, extended intermediary due diligence. As an example, the requirements under these rules include content moderation, transparency in grievance redressal, and a time-limited removal of illegal content. Though these reforms are indicators of a change to more platform accountability, they continue to be more of a procedural and responsive aspect. More importantly, they do not put a broad responsibility on proactive measures towards averting trademark infringement, nor do they touch upon the usage of automated systems to aid infringing actions.

Judicial Interpretation: A Pattern of Cautious Deference

The Indian courts have played a pivotal role in setting out the scope of intermediary liability, and they have always adopted a more conservative stance that, in effect, gives benefits to safe harbor protection and shuns any proactive monitoring responsibility.

Delhi High Court ruling in *MySpace Inc. v. Super Cassettes Industries Ltd*.[25] stated that an intermediary would not have the protection of safe harbor in case it does not take a reasonable time to remove infringing content when actual knowledge is given. The ruling only reaffirmed the notice-based enforcement paradigm and made it clear that middlemen are relieved off the duty of actively monitoring the content.

20. Organisation for Economic Co-operation and Development & European Union Intellectual Property Office, Illicit Trade in Counterfeit Goods 61–64 (2022) https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/03/dangerous-fakes_08dedd45/117e352b-en.pdf.
21. The Trade Marks Act, Number 47 of 1999, section 29 (India).
22. The Information Technology Act, Number 21 of 2000, section 79 (India).
23. 47 United States Code section 230 (2018); Council Directive 2000/31/EC, articles 12–15, 2000 Official Journal of the European Union (L 178) 1.
24. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended (India).
25. *MySpace Inc. v. Super Cassettes Indus. Ltd.*, 2017 SCC OnLine Del 6382

Likewise, in the case of *Kent RO Systems Ltd. v. Amit Kotak*,[26] the court stated that the law does not entail intermediaries to decide independently on each listing about an intellectual property violation and only on receiving a particular notification by the right-owner. This stance gives a sense of judicial sensitivity to the over-compliance costs to which platforms were exposed to, yet it also fixes in place a reactionary model of enforcement.

In *Christian Louboutin SAS v. Nakul Bajaj*,[27] the Delhi High Court added a significant qualification that e-commerce platforms taking an active part, warehousing or packaging, and brand promotion will forfeit safe harbor immunity. Even here, the judgment did not go so far as to demand proactive monitoring by the intermediary but rather its participation in the particular transaction.

The doctrinal uncertainty in applying traditional trademark concepts to digital advertising is further manifested in the reasoning of *Google LLC v. MakeMyTrip (India) Pvt. Ltd.*[28] the court's holding that the use of trademarks as keywords does not constitute infringement, absent consumer confusion, was recognition of the insufficiency of existing statutory tests in confronting algorithm-driven advertising systems.

Limitations in the Existing Framework Structure

Collectively, this legal framework, together with the judicial interpretation, has three systemic constraints.

To begin with, still in e-commerce, enforcement of trademarks is largely complaint-based, where the responsibility of detection and enforcement rests with right owners and not the platforms.

Secondly, a current safe harbor policy still sees platforms like passive intermediaries when they intervene in the online market using automated tools.

Third, the current norms of the law are not likely to prevent mass and repeated violations, which are made easy by anonymity, algorithmic amplification, and jurisdictional fragmentation.

These boundaries indicate a regulatory dissonance between conventional trademark philosophy and the technological structure of digital markets. Although the courts have attempted to preserve innovation by limiting the reach of intermediary liability, this too has had the unintended side effect of opening enforcement blind spots that infringers have now exploited more than ever. It is here where AI-enabled enforcement systems are being established as substitutes to the adjudication and justice system, yet rather support systems that can help boost detection, prioritization, and response as part and parcel of the current legal provisions.

LEGAL AND ETHICAL CHALLENGES THAT NEED TO BE TAKEN INTO CONSIDERATION WHILE USING AI FOR PROTECTION

The introduction of trademark protection via the use of artificial intelligence is a paradigm shift in the policing of intellectual property in the online market. As a matter of fact, these AI systems are not only used as ancillary detection systems; rather, they are used as gatekeeping systems to control access, visibility, and viability on e-commerce websites. This, in turn, leads to the basic enforcement operations being shifted out of the courts to private technological infrastructure with extensive legitimacy and rights protection implications.

An example of the implementation of the principles of private regulatory delegation is the enforcement of trademarks by AI, where online platforms assume a non-judicial decision-making role in the court of law in trademark disputes without the due-process safeguards of the decision-making process in adjudication of

26. *Kent RO Sys. Ltd. v. Amit Kotak*, 2017 SCC OnLine Del 8040.
27. *Christian Louboutin SAS v. Nakul Bajaj*, 2018 SCC OnLine Del 12215.
28. *Google LLC v. MakeMyTrip (India) Pvt. Ltd.*, 2022 SCC OnLine Del 1143.

trademarks. This also requires that the resultant trademark enforcement system be evaluated from the perspective of the trademark doctrine, administrative law, constitutional guarantees, and competition policy, in addition to efficiency considerations.

1. Reliability & Accuracy: Moving from Technic Errors to Legal Damages- Precision is not merely an AI-technical action to perform trademark protection; it also impacts the market interaction and property rights in real-life situations. False positives may result in material deletions, sales account suspension, and consumer loss of faith in direct communication, and without prior lack. False negatives, however, enable infringement activity to go on unhindered, thus making trademark protection useless.[29]

The major distinction that exists between AI error and classic human error is the difference in magnitude and speed. The discriminative algorithm classification is capable of replicating an error on thousands of listings in several seconds, therefore guaranteeing a more systemic type of harm than an individual one.

In a doctrinal sense, this raises questions about a 'likelihood of confusion' standard of consumer protection, which, in a human sense, preserves a context-based assessment of consumer confusion rather than a machine-based assessment in a formulaic computation of similarity.

Additionally, trademark laws have provisions to ensure fair use of trademarks in cases such as parody, nominative fair use, or comparative advertising, all of which require interpretation that may be relative or subjective.[30] By design, AI systems are not adept at undertaking such interpretation. Consequently, autonomous enforcement may easily slide into "over-compliance," wherein online platforms may take the precaution of deleting to avoid potential responsibility.[31]

The proper course of law is therefore to embrace AI rather than to exclude it, although it must be kept within bounds. The use of hybrid models of enforcement, whereby AI systems are utilized for detection and triage, with legally trained human decision makers as the final authority, is therefore a best practice, rather it's a necessity for maintaining doctrinal integrity.[32]

2. Algorithmic Bias as Structural Inequality- It is necessary to address algorithmic bias with regard to the enforcement of trademarks through a structural inequality lens rather than a technical glitch lens. AI is based upon predictively powerful datasets that are skewed towards trademarks of more developed markets, mainstream languages, and mainstream trading parties. This creates a situation wherein enforceability is skewed towards world-class trademarks while pushing other trademarks into obscurity.

As far as competition law is concerned, discrimination in enforcement creates an uneven playing field for market access, which mainly affects smaller companies and new entrants. On issues of equality, it perpetuates inequalities, which trademarks law is intended to redress, not entrench. There is a risk that a new system of inequality based on trademarks will be established. That is, a kind of "hierarchy of trademarks."[33]

29. Organisation for Economic Co-operation and Development, Artificial Intelligence and Intellectual Property 33–36 (2021) https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/02/intellectual-property-issues-in-artificial-intelligence-trained-on-scraped-data_a07f010b/d5241a23-en.pdf.

30. WIPO, *Trademark Law and Practice* 18–22 (2d ed. 2021).

31. Rebecca Tushnet, *Trademark Law as Commercial Speech Regulation*, 58 South Carolina Law Review 737, 754–58 (2007) https://scholarship.law.georgetown.edu/facpub/276.

32. Cary Coglianese & David Lehr, *Regulating by Robot*, 105 Georgetown Law Journal 1147, 1185–88 (2017) http://ssrn.com/abstract=2928293.

33. WIPO, *Artificial Intelligence and Intellectual Property Policy* 21–24 (2022) https://www.wipo.int/en/web/frontier-technologies/artificial-intelligence/index.

Bias exists in linguistics as well. When machine learning models are trained mostly in English datasets, they fail to correctly detect symbols that use non-Latin alphabets. Such situations lead to the risk of wrong takedown notices or a lack of enforcement in international markets.[34]

From a legal perspective, a lack of bias in algorithms could be considered a violation of the principles of discrimination and equality enshrined in various constitutional laws and conventions. Thus, bias reduction should be institutional within laws and conventions related to data diversity and the evaluation of algorithms.[35]

3. Data Protection, Trade Secrets, and Informational Power- AI-enforced trademark protection requires the large-scale processing of sensitive business data pertaining to intellectual property enforcement strategies, logos, business behavior patterns, and other business metadata. This kind of intellectual property law confluence poses an array of complicated issues concerning the enforcement of the DPDP, GDPR, and CCPA.[36]

In addition to personal data, trademark enforcement data sets tend to include business-critical data that may be trade secrets. If not managed carefully through regulation and strict confidentiality agreements, the sharing of data among platforms, AI suppliers, and enforcement parties could potentially lead to undermine a competitive advantage.[37] From a regulatory perspective, a double duty of compliance in terms of privacy and trade secret protection is required for AI-enforcement systems.

The privacy by design principle must be extended not only to technical measures of privacy but also to government measures on data access, retention, and secondary use. Obligations with regard to transparency are also paramount. Rightsholders/sellers must be made aware not only of the fact but the manner in which the AI system affects the outcome of an enforcement action. Otherwise, the AI system becomes an opacity system inconsistent with data protection standards.

4. Jurisdictional Fragmentation and the Crisis of Legal Certainty- The territorial basis on which trademark law is founded is fundamentally at variance with the global reach that enforcement systems based on AI must facilitate. AI tools operating on cross-national platforms often apply the same enforcement standards despite differences in trademark law across countries.

For example, the doctrine of prior-use rights in India appears diametrically opposite to that in the European Union's registration-oriented system.[38] An AI system designed in accordance with EU norms may end up enforcing registered trademarks too early in countries where the determining factor is usage, and may under-enforce in others.

From the perspective of private international law, there are unanswered questions about the rules of law that will be applied to the enforcement carried out by AI. This is because the enforcement carried out by AI lacks calibration according to jurisdiction and could become a matter of a private legal order that crosses the boundaries of the national law to which it is subject.

In other words, it becomes imperative to have the jurisdictional legal module in the AI system itself. The thresholds and standards of evidence, and also the remedies, cannot but be dynamically

34. Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition* 109–13 (2016).

35. EUIPO, Artificial Intelligence Bias and Intellectual Property Enforcement 15–18 (2023) https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/2023_IP_Tech_Watch_Discussion_Paper/2023_IP_Infringement_and_Enforcement_Tech_Watch_Discussion_Paper_FullR_en.

36. EU High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI* (2019).

37. Council Regulation 2016/679, articles 4, 6; California Civil Code sections 1798.100–1798.199 https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100.

38. Pamela Samuelson, *Privacy, Trade Secrets, and Data Governance*, 67 University of California Los Angeles Law Review 1124, 1146–50 (2020) https://people.ischool.berkeley.edu/~pam/papers/privasip_draft .

accommodated according to the local jurisdictions themselves.

5. Fairness, Access, and Global Power Asymmetry- AI-based enforcement solutions would work towards decreasing monitoring expenses, although their availability is not equal across all parties. Large companies can either implement sophisticated AI-based solutions or hire experts, whereas smaller companies, as well as rights holders in developing countries, do not have equal opportunities.[39]

From a normative perspective, the aim of the law of trademarks is to facilitate fair competition, not to consolidate monopolies. The equal distribution of access to AI-based enforcement mechanisms thus raises a particular concern for distributive justice. International collaboration via organizations such as WIPO is therefore called for to create a common infrastructure for law enforcement.

6. Automation, Due Process, and Right to Be Heard- Decisions about trademarks, and even more so concerning takedown and suspension of accounts, have direct and immediate effects in the economic sphere. When decisions and procedures initiated with regard to trademarks are also made through AI systems, the role of procedural guarantees becomes essential. The requirement of due process includes notice, justification for a decision, and the possibility of appealing an adverse decision.[40]

AI-enforced systems without human judgment may fail to provide these safeguards in practice, de facto translating trademark enforcement into administrative litigation outside judicial control. For AI-enforced systems to uphold the principles of the rule of law, the following requirements need to be met.

7. Transparency, Accountability, and Democratic Legitimacy- In conclusion, "The use of artificial intelligence in trademark enforcement raises questions about democratic legitimacy." As a consequence of private platforms and algorithms being involved in the definition of the scope of intellectual property rights, the enforcement of these rights becomes "insulated from public view."[41]

Through this aspect, there is a lack of transparency concerning the matter at issue among the affected parties and the impact being generated. Accountability and governance frameworks need to then distribute accountability among platforms, AI providers, and rightsholders. The use of explainable AI, audit trails, and independent supervision is not an add-on or a desirable feature but a mandatory requirement in order to ensure that AI enforcement is compatible with public law values.

CASE STUDIES: AI-ENABLED MODELS OF TRADEMARK ENFORCEMENT

The practical implications of AI-driven trademark enforcement can be better understood through a practical analysis of the different models of enforcement currently deployed by legal and technology service providers. This section examines two widely adopted approaches to AI-assisted brand protection: one based on automation and scale, and the other on hybrid human-AI governance.

Instead of evaluating technological sophistication in isolation, the practically already implemented analysis looks at how the different models operationalize trademark enforcement, allocate decision-making power, and address the legal and ethical risks outlined in the previous section.

39. UNCTAD, *Digital Economy Report* 2023, at 91–95.
40. Jerry L. Mashaw, *Due Process in the Administrative State* 23–27 (1985).
41. Frank Pasquale, *The Black Box Society* 148–53 (2015) .

A. Gowling WLG: Automation-Centric Enforcement Architecture[42]

Gowling WLG has developed an AI-powered brand protection system designed to address the scale and velocity of online trademark infringement. The system deploys machine learning algorithms to continuously monitor e-commerce platforms, social media marketplaces, and domain name registries for indicia of trademark misuse. Image recognition, OCR, and text-matching technologies are used to identify visually similar logos, altered brand names, and deceptive product descriptions that may evade manual review.

Operation efficiency is also perhaps the greatest strength of the system in Gowling WLG as far as enforcement is concerned. With detection being automated, the detection of infringing listings can be achieved at an earlier stage; cases can then be risk-scored, prioritizing on repetition, behavior of the seller, and market reach. This form of triage minimizes the enforcement latency and allocates resources towards brand owners to act on the most impactful infringements.

Notably, automated creation of takedown notices, cease-and-desist communications, and platform-specific enforcement requests is made easier by the system, significantly shortening response time. This construction is innovative and displays some of its structural constraints.

This model, which is effective in counterfeiting of high volumes, is based on similarity measures and behavioral measures, which may not be effective in counterfeiting comparative advertising, parody, or references to descriptions that are not legally illegal. In areas where structural human review occurs at the time of making decisions, over-enforcement is bound to lead to unreasonable takedowns and chilling declarations of lawful commercial expression. The Gowling model displays the trade-off in scale and the subtleties of the doctrine of very automated systems of enforcement.

B. Corsearch: Hybrid Intelligence and Jurisdiction-Sensitive Enforcement.[43]

Corsearch does the latter in a much different way that combines AI-based detection with systematic human supervision by intellectual property experts. The online marketplace, domain names, and online advertising platforms are scanned with machine learning tools that identify possible infringements. These automatic notifications are nonetheless more of a tool to assist in decision-making and not necessarily a driving force to enforce.

Another excellent signature of Corsearch model is the addition of legal knowledge in many bottlenecks of enforcement. Human reviewers scrutinize AI-marked cases with a view to assessing the jurisdictional applicability, the chances of confusion, and potential defenses relating to trademark law. The hybrid architecture is also very applicable in the cross-border enforcement where the various standards of law are divergent; therefore, automated decision-making is challenging. Corsearch reduces the risk of false positives resulting in incorrect enforcement measures, should false positives arise, which would be common under a monolithic algorithm standard across different legal frameworks, through the creation of a jurisdiction-sensitive legal review.

Behavioral and predictive analytics are also used by Corsearch to recognize repeat infringers and newer infringement patterns. Not all reactive systems permit anticipatory enforcement measures, including tracking seller networks and flagging high-risk accounts in advance, which this enables. Governance-wise, the hybrid concept is more appropriate to the principles of due process because it does not eliminate the human judgment in making determinations that have implications for legal rights and market access. This is, however, more operationally expensive and less scalable compared to fully automated systems.

42. Gowling WLG, AI-Powered Brand Protection Services, https://gowlingwlg.com (last visited December 26, 2025).
43. Corsearch, Hybrid Intelligence for Brand Protection, https://corsearch.com (last visited December 26, 2025).

C. Comparative Evaluation and Regulatory Implications.

The AI-enforcement model used in the two firms, Gowling WLG and Corsearch, was comparatively analyzed, thus bringing two highly distinct paradigms of enforcement.

a. It is the model of Gowling that is focused on speed, scalability, and automation; in this model, the counterfeiting on a large scale in quite homogeneous markets is fought.

b. The hybrid model of Corsearch, in which the focus is put on legal accuracy, jurisdictional sensitivity, and procedural fairness, and in which it is more appropriate in the context of complex and high-risk enforcement scenarios or cross-border enforcement.

Regulatory-wise, none of the models is a comprehensive solution. Any strategy that focuses on automation runs the risk of making trademark protection a sort of privatized over-regulation, and any strategy with too much human involvement might be unprepared to address the magnitude of internet-based infringement.

The case studies thus support the main thesis of the paper, AI can be utilized only as an auxiliary tool of enforcement infrastructure that exists within the confines of legal governance as an independent decision maker. The findings hold significant value in terms of how platforms will be regulated and policies will be formulated.

To lawmakers and regulators, architectures that are enforced ought to be encouraged that are both algorithmically efficient and human accountable, transparent, and appeal mechanisms. Lacking such integration, AI-based enforcement is likely to contribute to the doctrinal, ethical, and jurisdictional issues mentioned above.

CONCLUSION

The emergence of the digital space has altered the core of commerce by altering the terms of operation and enforcement of trademarks. The internet has also expanded significantly on the dangers of counterfeiting, trademark watering down, cybersquatting, and deceptive brand practice on a scale that prior machinery of interception could never be created to accommodate. As it has been demonstrated in this paper, trademark law, so deeply entrenched in the territorially bounded and reactive modes of enforcement, cannot meaningfully confront the speed, anonymity, and amplification aspects of the contemporary e-commerce ecosystems. It is against this background that AI has come out as a powerful enforcement platform of trademark monitoring, detection, and response.

The AI-enhanced devices are also able to analyze the waves of online data, detect phenomena of infringement, and decrease the latency of such enforcement in a manner that human-based mechanisms cannot conduct with sacredly. The application of AI to trademark enforcement is not, however, entirely a technical process, as it has been demonstrated critically in this research paper.

It raises deep legal and ethical issues of due process, algorithmic discrimination, protection of information, taking too much power, and over-enforcement via secretive, non-public decision-making algorithms. The fundamental input of this paper is a conceptual redefinition of AI-based trademark enforcement not as a technological neutral application but as a case of delegated regulatory governance. Based on doctrinal discussion, comparative, and case study of existing systems of enforcement, the paper demonstrates how AI can strengthen trademark protection only when it is incorporated within legally responsible rights-conscious structures. The need to automate, thus, must be married with human surveillance, disclosure requirements, avenues of appeal, and jurisdiction-specific calibration with an eye to uniformity with doctrine on trademarks and with fundamental principles of equity and competition.

The paper also highlights that it is important to have concerted regulatory actions against transnational infringement of trademarks. The crossing of national borders by digital marketplaces is facing disjointed legal frameworks with risks of frequently creating enforcement blind spots or inconsistent outcomes. The harmonization processes, driven by international organizations and

informed by comparative regulatory experience, are a crucial tool of legal predictability, and the freedom of national doctrine is safeguarded.

Policy programs that integrate technological innovations with political change accompany closely related policy programs in developing AI governance frameworks in India and the European Union, which serve as worthy benchmarks towards future change. Thus, the meaningful trademark protection of the digital economy basically demands a multidimensional approach that will demand the doctrinal precision of technological capacity and normative protection.

AI should play the role of supplementary enforcement architecture, not a replacement for legal adjudication. If set within a framework of principled governance, AI-assisted enforcement can effectively contribute to heightened brand protection, reduced counterfeiting, and increased consumer trust without compromising procedural justice or market fairness. It is through this balance that trademark law can retain effectiveness, legitimacy, and responsiveness in the face of an increasingly algorithm-driven commercial environment.

RECOMMENDATIONS FOR E-COMMERCE PLATFORMS: A GOVERNANCE-ORIENTED FRAMEWORK

From the above analysis, it is clear that trademark infringement on e-commerce platforms not only represents a scaling issue but also a governance gap between traditional trademark rules and algorithm-driven e-commerce platforms. A practical enforcement strategy would thus need e-commerce platforms to rely on AI not as a technical solution in isolation, but as part of a governance framework for enforcement that is legal and rights-aware. The suggestions below are tailored to take into account the constraints that are identified and analyzed in this paper.

1. Need for Continuous Monitoring and Ad-Hoc Enforcement- E-commerce platforms should opt for AI-based systems that monitor their own marketplaces and social media platforms in relation to their product listings and advertising features on a real-time basis. Unlike the complaint-based approach, real-time monitoring will make it possible to identify violations that would otherwise be removed by the time takedown procedures are initiated.

This will directly mitigate the reactive nature of current legal frameworks and the enforcement lag that has been identified as a weakness in Section III of the paper. This system would focus on the highest risk listings rather than universal surveillance and would still remain within the boundaries of a safe-harbor regime.

2. Need to establish a Context-Sensitive Trademark Detection with Legal Standards as Anchor- AI-based enforcement tools should begin to incorporate greater levels of context assessment that are inclusive of trademark principles of confusion, use of the mark, and commercial activity. It is essential that deep learning models be trained to not only detect counterfeits, but to differentiate between counterfeits and activities that might constitute nominative use, parody, or comparative advertising.

This recommendation goes some way in mitigating risks associated with over-enforcement and chilling effects, which have been recognized in Section IV, since it aligns AI detection logic with substantive law concerning trademarks instead of pattern recognition. This will ensure that AI is not detrimental to doctrinal protections incorporated into trademark jurisprudence.

3. Requirement of a Cross-Platform and Cross-Channel enforcing coordinators- The infringement rings are also getting established in cyberspace and are functioning across the platforms, and the e-commerce platforms are required to make use of the interoperating AI systems capable of establishing connections in the marketplace or other environments within cyberspace to identify any form of infringement activity.

This recommendation will overcome the disjointing challenge of platform-specific

enforcement and better address Repeat Offenders in terms of jurisdictional and platform silos exploitation. Enforcement coordination discourages arbitrage of regulation without holding the same standard to all jurisdictions regardless of diversity.

4. Need to develop an Advanced Image Recognition Technology to Fight Insidious Counterfeit Techniques- The Platforms should install image recognition technology with AI that has capabilities in detecting geometric patterns, feature vectors, and trade dress besides logos. This technology is highly required when there are counterfeits that have been created using different colored logos, half logos, and stylized logos.

This will also improve the enforcement standard by addressing the circumvention of infringement, and thus, the enforcement will be less human-dependent. This solution, combined with human verification, would help increase accuracy and make enforcement a fully automated decision.

5. Remote to create a Behavioral Anomaly Detection to Proactive Seller Control- The solutions that can be employed to detect high-risk sellers before mass trademark or/and copyright infringement are using AI tools to identify the patterns of the behavior exhibited by the seller, such as switching between different accounts regularly, suspicious peaks in sales, and deleting listings repeatedly.

This transforms the enforcement of a post-harm remedy to proactive control to proportions and degrees of infringement that are challenging to control by the courts of law and traditions. Monitoring of conduct is behavior-oriented as opposed to content-only based judgment since it does not use similarity to determine content.

6. Sensitivity to Multilingual and Culturally Adaptive AI Systems- Due to the transnational character of e-commerce, an AI-based enforcement system should be able to detect and interpret multi-linguistically and culturally sensitive trademarks that contain non-Latin scripts and region-specific trademarks.

This recommendation is biased by algorithms and unequal enforcement discussed in Section IV, since it guarantees that the fact that trademarks are not offered protection in churning markets and non-English-speaking nations is not systematic.

7. Need to have a Firewall and Forensically Solid Evidence Recovery system- Enforcement AI should automatically document and hold copies of the evidentiary content, such as screenshots, metadata, and timeline information, in the event of copyright infringement. These materials must be prepared in a way that is in line with the judicial and administrative demands.

The issue of the evidentiary burden that befalls trademark owners, particularly in cases involving cross-border, is resolved in such an extension and enhances the defensibility of take-down notices. In addition, it enhances transparency, as well as accountability, in the sense that audit trails of enforcement decisions are created.

8. Need to have a model which can continuously update its models and adapt to threats- AI-based enforcement tools shall be re-trained frequently to fit changing Tactics of infringing, such as deep fake branding, animations, and false product descriptions. The constant learning will make sure that the AI systems will not grow obsolete and rely less on historic trends of infringement, which in turn will make them relevant in enforcement and reduce the production of false positives caused by obsolete learning information.

9. Requirement of Institutional Cooperation with Regulators and Trademark Agencies- E-commerce applications need to collaborate with trademark offices, customs departments, and regulators so as to develop a standardized AI-based protection system with standard indicators and reporting resources to detect risks. Regardless of such synergic activity bridges the legitimacy gap there is between the regulation of the privatized platforms and the national regulating framework such that the role of enforcement of AI systems does not affect the sovereignty of the law.

10. Installing Ethical AI, Transparency, and Appeal Systems- E-commerce platforms should introduce the rules of ethical AI into their trademark protection systems to involve the explainability of AI results, the ability to monitor questionable situations, and ask the affected traders to file a complaint. The problems of due process, accountability, and legitimacy are particularly covered in this recommendation. Reasonable and revisable enforcement practices would make AI a support system and not an unattractive privatizer of judgment.

REFERENCES

1. Press Information Bureau, Government of India, Telangana Leads Adoption of Artificial Intelligence and Emerging Technologies in Governance (September 4, 2024)
2. United Nations Conference on Trade and Development, Global E-commerce Sales Surpass Trillions Amid Digital Expansion (2024)
3. Press Information Bureau, Government of India, Telangana Adopts Artificial Intelligence and Emerging Technologies for Governance Reforms (September 4, 2024)
4. Council Regulation 2022/2065, articles 26–28, 2022 Official Journal of the European Union (L 277) 1 (Digital Services Act).
5. William M. Landes & Richard A. Posner, *Trademark Law: An Economic Perspective*, 30 Journal of Law and Economics 265, 269–72 (1987).
6. Graeme B. Dinwoodie, *Developing a Private International Law of Trademarks*, 24 Berkeley Technology Law Journal 161, 170–73 (2009).
7. Organisation for Economic Co-operation and Development & European Union Intellectual Property Office, Global Trade in Counterfeit and Pirated Goods 45–48 (2023).
8. Ariel Ezrachi & Maurice E. Stucke, Virtual Competition 83–87 (2016).
9. World Intellectual Property Organization, Trademark Law and Practice 17–20 (2nd edition 2021).
10. European Union Intellectual Property Office, Online Trade in Counterfeit Goods: Risks and Policy Responses 22–25 (2022).
11. Jonathan Weinberg, *ICANN and the Problem of Cybersquatting*, 50 Duke Law Journal 187, 190–94 (2000).
12. Uniform Domain Name Dispute Resolution Policy paragraph 4(a); The Trade Marks Act, 1999, section 27 (India).
13. Stacey L. Dogan & Mark A. Lemley, *Trademarks and Consumer Search Costs on the Internet*, 41 Houston Law Review 777, 784–89 (2004).
14. Google Inc. v. MakeMyTrip (India) Pvt. Ltd., 2022 SCC OnLine Del 1143.
15. WIPO, *Digital Brand Protection Report* 31–34 (2021).
16. Rebecca Tushnet, *Gone in Sixty Milliseconds: Trademark Law and Cognitive Science*, 86 Texas Law Review 507, 532–35 (2008).
17. Irene Calboli & Jane C. Ginsburg, *Trademark Litigation in the Digital Age*, 92 New York University Law Review 1310, 1321–24 (2017).
18. Organisation for Economic Co-operation and Development & European Union Intellectual Property Office, Illicit Trade in Counterfeit Goods 61–64 (2022).
19. The Trade Marks Act, Number 47 of 1999, section 29 (India).
20. The Information Technology Act, Number 21 of 2000, section 79 (India).
21. 47 United States Code section 230 (2018); Council Directive 2000/31/EC, articles 12–15, 2000 Official Journal of the European Union (L 178) 1.
22. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended (India).
23. *MySpace Inc. v. Super Cassettes Indus. Ltd.*, 2017 SCC OnLine Del 6382
24. *Kent RO Sys. Ltd. v. Amit Kotak*, 2017 SCC OnLine Del 8040.

25. *Christian Louboutin SAS v. Nakul Bajaj*, 2018 SCC OnLine Del 12215.
26. *Google LLC v. MakeMyTrip (India) Pvt. Ltd.*, 2022 SCC OnLine Del 1143.
27. Organisation for Economic Co-operation and Development, Artificial Intelligence and Intellectual Property 33–36 (2021).
28. WIPO, *Trademark Law and Practice* 18–22 (2d ed. 2021).
29. Rebecca Tushnet, *Trademark Law as Commercial Speech Regulation*, 58 South Carolina Law Review 737, 754–58 (2007).
30. Cary Coglianese & David Lehr, *Regulating by Robot*, 105 Georgetown Law Journal 1147, 1185–88 (2017).
31. WIPO, *Artificial Intelligence and Intellectual Property Policy 21–24 (2022).*
32. Ariel Ezrachi & Maurice E. Stucke, *Virtual Competition* 109–13 (2016).
33. EUIPO, Artificial Intelligence Bias and Intellectual Property Enforcement 15–18 (2023).
34. EU High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI* (2019).
35. Council Regulation 2016/679, articles 4, 6; California Civil Code sections 1798.100–1798.199.
36. Pamela Samuelson, *Privacy, Trade Secrets, and Data Governance*, 67 University of California Los Angeles Law Review 1124, 1146–50 (2020).
37. UNCTAD, *Digital Economy Report* 2023, at 91–95.
38. Jerry L. Mashaw, *Due Process in the Administrative State* 23–27 (1985).
39. Frank Pasquale, *The Black Box Society* 148–53 (2015).
40. Gowling WLG, AI-Powered Brand Protection Services, https://gowlingwlg.com (last visited December 26, 2025).
41. Corsearch, Hybrid Intelligence for Brand Protection, https://corsearch.com (last visited December 26, 2025).