Page: 633-667 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 2

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.65

FROM CYBERSQUATTING TO META TAGGING – THE EXPANDING SCOPE OF TRADEMARK INFRINGEMENT IN THE DIGITAL SPHERE

Priya Dharshini A[1]

I. ABSTRACT

With the rapid expansion of digital commerce, trademark infringement in the digital sphere has grown in complexity and scale. In 2024, trademark owners from 133 countries filed 6,168 domain name complaints under the UDRP marking the second highest annual figure, highlighting the global rise in cybersquatting and related online violations. This paper examines how traditional trademark protection has evolved to address online issues such as cybersquatting, meta-tagging, keyword advertising and impersonation on social media. These tactics divert consumer attention thereby misleading them, exploit brands image and diminish market credibility.

The paper offers an analysis of Indian and international frameworks including the Trade Marks Act, 1999, the INDRP, and the UDRP and identifies enforcement obstacles such as digital anonymity, cross border jurisdiction and weak platform accountability. Further, it addresses new threats from NFTs, block-chain domains, and AI-generated misuse. A 2024 study of NFT marketplaces found 8,000+ infringing collections, linked to $59 million in consumer deception and economic harm. Decentralized domain systems and AI-driven keyword tools pose enforcement challenges that often evade traditional legal remedies.

The paper recommends extending trademark protection to virtual goods, defining AI-related liability, enforcing stricter rules for digital platforms, and implementing faster dispute resolution processes. By integrating case law, data trends and statutory gaps, this paper will strengthen the legal understanding of online trademark risks and equips

[1] LLM Student, Government Law College, Trichy

 (ISSN: 2583-7753)

practitioners with strategies to navigate and address infringement in evolving digital marketplaces.

II. KEYWORDS

Trademark infringement, Cybersquatting, Meta-tagging, Keyword advertising, Online trademark Protection, Trademark in Metaverse, Cross border IP enforcement

III. INTRODUCTION

In recent years, the expansion of digital marketplaces and internet enabled technologies has significantly transformed the landscape of trademark enforcement. As businesses increasingly rely on online platforms to promote, advertise and sell their goods and services, trademark violations have proliferated in new and complex ways. Cybersquatting, meta-tagging, keyword advertising, impersonation on social media and misuse of trademarks in NFTs and block-chain domains are now common strategies used to exploit brand reputation and mislead consumers.

According to the World Intellectual Property Organization (WIPO), 6,168 domain name disputes were filed under the UDRP in 2024 alone, representing the second highest total since the policy's inception. Furthermore, a 2024 study of NFT marketplaces reported over 8,000 trademark infringing collections, resulting in an estimated $59 million in consumer deception and economic harm. These statistics underscore the pressing need for stronger and adaptive legal mechanisms to combat digital trademark infringement.

This paper seeks to answer the research question: To what extent are existing legal frameworks in India and internationally effective in addressing modern forms of trademark infringement in the digital space and what reforms are necessary to ensure comprehensive protection? The study proceeds on the hypothesis that: While existing legal frameworks offer partial remedies against traditional online trademark violations, they are insufficient to effectively address emerging threats posed by NFTs, block-chain domains, AI-generated content, and decentralized digital platforms, thereby necessitating targeted legal reforms.

To explore this issue, the paper first explains the nature and purpose of trademark law. It then examines common types of digital infringement and analyzes the legal protections offered under Indian and international systems, including the Trade Marks Act, 1999, the INDRP and the UDRP. It also evaluates enforcement challenges and judicial interpretations before addressing emerging technological threats. The paper concludes by proposing specific reforms aimed at strengthening online trademark protection.

IV. TRADEMARK- DEFINTION, NATURE AND ITS PURPOSE

Section 2(zb) of the Indian Trademarks Act, 1999 defines a trademark as a mark which differentiates the products or services of a business in the market so that consumers can identify their origin easily. Any symbol, word, phrase, design, or expression which fulfills this objective can be considered a Trademark.[2] In the United States, the Lanham Act defines a trademark as "any word, name, symbol, or device, or any combination thereof" used to identify and distinguish goods and to indicate their source.[3]

The United Kingdom's Trade Marks Act 1994 recognizes a trademark as any sign capable of being represented graphically which distinguishes the goods or services of one undertaking from those of others.[4] At the European Union level, the European Union Trade Mark Regulation (EUTMR) follows a similar approach, defining a trademark as any sign capable of distinguishing goods or services and capable of being represented clearly in the register, whether through words, designs, colours, sounds or even multimedia elements.[5]

Firstly, a trademark shows where a product, good, or service comes from. It is assumed that each specific product can only have one source. It guarantees that the products with the trademark are of good quality for the buyers. Besides ensuring quality, which

[2] The Trade Marks Act, 1999, No.47 of 1999, § 2(zb)
[3] Lanham Act, 15 USC § 1127
[4] Trade Marks Act 1994, c 26, s 1
[5] Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trade Mark (2017) OJ L154/1, art 4

ties into the product's reputation, the trademark also helps in building brand recognition and addresses marketing and advertising needs. In simpler terms, companies invest a lot of time and money into creating a product, promoting it to customers, offering customer service, and supporting their products with guarantees. A trademark confirms that these efforts to satisfy customers are worthwhile. It offers legal safeguards and protects against imitation and dishonest practices related to a particular brand. Finally, trademarks are used to set a product apart from others. This is what makes it unique. The goal is for trademarks to help identify products and services being sold from those of other businesses.

V. OBJECTIVES OF THE STUDY

The study aims to:

- Examine the main forms of trademark infringement occurring in digital spaces including cybersquatting, meta-tagging and keyword advertising.
- Identify enforcement challenges posed by cross border jurisdiction, anonymity, and emerging technologies like NFTs and AI.
- Recommend legal reforms to enhance online trademark protection and enforcement.

VI. RESEARCH METHODOLOGY

This study follows a doctrinal research method, relying on primary legal sources such as statutes, international policies and judicial decisions. Key instruments include the Trade Marks Act, 1999, the INDRP, the UDRP and landmark case laws. Comparative analysis is conducted using materials from the US, UK and EU frameworks. Secondary sources, including academic articles and WIPO data, support critical evaluation of legal adequacy and reform.

VII. PROTECTING TRADEMARKS IN ONLINE SPHERE - WHY IT CAN'T BE IGNORED

In the digital era, the infringement of trademarks has taken increasingly sophisticated and covert forms, necessitating a proactive and legally stronger approach to protection. Online platforms serve as a ground for trademark violations such as cybersquatting, meta-tag misuse, deceptive keyword advertising and social media impersonation. These violations distort brand identity, confuse consumers, and compromise fair competition.

According to the World Intellectual Property Organization (WIPO), 6,168 domain name disputes were filed under the UDRP in 2024, marking a 19% rise from the previous year and confirming the persistent threat of cybersquatting and deceptive domain registration practices by infringers. The UDRP and India's INDRP both classify such registrations as unlawful when done without legitimate interest and in bad faith. The growing incidence of online trademark infringement can be attributed to several interrelated factors. The widespread use of the internet has made global brand exposure almost instantaneous, but it has also made infringement far easier. The relatively low cost and high speed of digital operations encourage misuse, especially when paired with the anonymity offered by domain name registrars, proxy servers, and decentralized hosting platforms. Many infringers exploit the lack of clarity in jurisdictional rules, knowing that transnational enforcement is time consuming and often inconsistent.

Furthermore, digital platforms frequently lack adequate mechanisms for filtering or preempting infringing content. In some cases, infringers intentionally mimic well known trademarks to divert consumer traffic, erode brand equity or extort rightful owners. Compounding the issue is the slow pace of legislative reform, which struggles to keep up with the evolving nature of online technology and digital marketplaces. These conditions collectively create an environment in which traditional legal safeguards for trademark protection are increasingly strained.

The Delhi HC held that domain names, much like trademarks, function as indicators of commercial origin and are entitled to protection against deceptive use This judgment affirmed the principle that digital identifiers carry trademark value and that misuse of domain names is actionable under Section 29(4) of the Trade Marks Act, 1999.[6] The U.S.A Ninth Circuit held that using a competitor's trademark in website meta-tags caused "initial interest confusion" and amounted to infringement. Although not visible to users, such deceptive meta-tagging manipulates search engine results and diverts consumer attention unfairly.[7]

Similarly, the Madras HC considered whether bidding on a competitor's trademark as a Google Ad keyword infringed the mark. The Court suggested that such keyword advertising may mislead users and tarnish brand distinctiveness.[8] This view was further advanced where the Delhi High Court held that commercial exploitation of a rival's mark in ad keywords could constitute infringement under Sections 29(6), 29(7), and 29(8) of the Trade Marks Act. [9]The borderless and anonymous nature of online spaces creates significant jurisdictional and enforcement hurdles. Infringers frequently rely on privacy protection tools, offshore servers or decentralized technologies to evade liability. Although mechanisms like the UDRP and INDRP offer expedited relief, they remain limited in scope, particularly when new technologies such as NFT marketplaces and block chain-based domains are involved.

The legal implications of online trademark misuse are substantial. Without active enforcement and doctrinal adaptation, the foundational functions of a trademark source identification, consumer protection, and market fairness stand to be undermined. As courts begin to respond to these novel challenges, legislative bodies must also evolve to ensure meaningful and enforceable trademark protection in the digital marketplace.

[6] Tata Sons Ltd. v. Ramadasoft, 2005 (30) PTC 486 (Del)
[7] Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999)
[8] Consim Info Pvt. Ltd. v. Google India Pvt. Ltd., 2011 (45) PTC 575 (Mad)
[9] M/s DRS Logistics Pvt. Ltd. v. Google India Pvt. Ltd., 2021 SCC (Del) 3814

VIII. RISE OF TRADEMARK INFRINGEMENT IN ONLINE PLATFORMS AND ITS LEGAL PROTECTION

The internet and digital technology have allowed for new forms of trademark infringement through methods like cyber squatting, keyword advertising, and misuse of social media, resulting in increased difficulties for businesses in protecting their intellectual property rights. While keyword advertising employs registered words to attract customers, cyber squatting refers to the practice of obtaining domain names to take advantage of trademarks. Furthermore, the improper use of social media entails utilizing trademarks without permission in order to confuse or harm businesses. These online platforms enhance the effect of violations on consumer confidence and brand image by enabling faster spread and wider audience engagement.

The global expansion of the Internet has created new opportunities for companies to engage with customers in various nations. Nonetheless, this broad connectivity has resulted in significant challenges regarding the protection of trademark rights, particularly due to the rise in unauthorized usage and infringements within digital environments. A clear illustration of such a breach is the practice referred to as "cyber squatting," wherein individuals deliberately acquire domain names that closely resemble well-known trademarks, aiming to profit by misleading consumers. Moreover, the growth of social media platforms, while offering valuable marketing opportunities, has increased the exposure of brand owners to the risks associated with impersonation. Individuals without permission may establish fraudulent profiles, pages, or accounts that deceive consumers, damage the reputation associated with genuine trademarks, and potentially result in substantial financial losses.

A. Global protection – Uniform Domain-Name Dispute Resolution Policy (UDRP), 1999 and Internet Corporation for Assigned Names and Numbers (ICANN), 1998.

On a global scale, addressing trademark misuse related to domains is mainly supported by the Uniform Domain Name Dispute Resolution Policy (UDRP), created by the Internet Corporation for Assigned Names and Numbers (ICANN) in partnership with the World Intellectual Property Organization (WIPO). The UDRP functions as an internationally acknowledged process to tackle cybersquatting, which refers to the act of registering domain names in bad faith that are the same as or misleadingly similar to a valid trademark.

Through the UDRP, trademark holders have the ability to start disputes by submitting complaints against domain registrants, avoiding the need for protracted and costly court processes. This system offers a quick, cost effective, and impartial platform for settling domain name conflicts. If the complaint is accepted, the questioned domain may be transferred or canceled, based on the ruling. This method is especially advantageous for trademark owners encountering infringement in different countries, as it circumvents the difficulties associated with legal disputes across borders. ICANN, as the organization that manages the worldwide domain name system, is vital in upholding trademark protections by mandating that all generic top-level domain (gTLD) registrars adhere to UDRP regulations. This centralized enforcement establishes UDRP as a fundamental component for safeguarding brand identity in the worldwide digital environment.

B. Protection in India – Trade Marks Act, 1999, No.47 of 1999 and .IN Domain Name Dispute Resolution Policy (INDRP)

In India, the main law overseeing trademark protection is the Trade Marks Act, 1999, No. 47 of 1999, which also applies to the digital and online environments. The law distinctly forbids the unapproved use of a registered trademark, which includes its

presence in domain names, online sales listings, digital ads and website material. If this use leads to confusion among consumers, weakens the brand's reputation or gives an unfair advantage to the infringer, it qualifies as trademark infringement according to the Act.

The legal solutions provided by this law consist of injunctions, financial compensation, profit accounts, and, in certain situations, the elimination of goods or digital content that infringes. Indian courts have acknowledged that domain names play a crucial role in brand identity, and legal precedents are progressively favoring trademark owners in their efforts to prevent online misuse. To address disputes regarding domain names specifically associated with the IN country-code top-level domain (ccTLD), India adheres to the.

IN Domain Name Dispute Resolution Policy (INDRP), which is overseen by the National Internet Exchange of India (NIXI)? The INDRP is designed based on the UDRP and offers a useful method to tackle dishonest domain registrations that violate registered trademarks in India. According to the policy, individuals making complaints may request the cancellation or transfer of the disputed. IN domain if they demonstrate that the domain is the same as or very similar to their trademark, that the registrant has no legitimate interest in the domain, and that the domain was registered with dishonest intentions.

C. The role of the Information Technology Act, 2000, No. 21 of 2000 as dual form of protection

Although the Information Technology Act of 2000, No. 21 of 2000 does not specifically focus on trademark law, it enhances trademark protection by addressing the technical and criminal aspects of online violations. Regulations addressing identity theft (Section 66C), online impersonation (Section 66D) and the distribution of false or misleading information can be applied when trademarks are improperly used in phishing websites,

counterfeit promotional emails, fraudulent social media accounts, or deceptive e-commerce platforms.[10]

The Trade Marks Act and the IT Act work together to form a complete legal system for addressing online trademark infringements in India. This two Acts guarantees that both the legal solutions and cybercrime elements of infringement are handled efficiently, maintaining brand reputation and consumer confidence in the growing digital market.

D. Recent Amendments to Indian trademark law and their impact on digital enforcement

The enforcement of trademark rights in the digital age has been strengthened significantly by the introduction of the Trade Marks Rules, 2017, G.S.R 199 (E) (2017), which replaced the Trade Marks Rules, 2002, G.S.R.740 (E) (2002). These Amendments were primarily procedural but have had a substantial impact on the administration and enforcement of trademarks, especially in online contexts. Key reforms include the reduction in the number of forms from 74 to just 8, mandatory e-filing for most trademark procedures and provisions for electronic communication and video conferencing in hearings.

These measures have made the trademark system faster, more accessible and better suited for handling disputes arising in the fast-paced digital environment. For example, the ease of filing oppositions and rectification requests allows trademark owners to respond more promptly to instances of online infringement, such as cybersquatting and unauthorized keyword advertising. Additionally, the introduction of Rule 124 enables rights holders to apply for recognition of their marks as "well-known," which strengthens preventive protection against digital misuse across platforms. Though the 2017 Rules did not amend the substantive provisions of the Act, they have modernized the enforcement landscape, aligning it with India's broader digital governance

[10]The Information Technology Act, No.21 of 2000, §§ 66C, 66D

framework and increasing efficiency in protecting trademark rights against online violations.

IX. CYBERSQUATTING

A. Definition

Cybersquatting is defined under the IN-Domain Name Dispute Resolution Policy (INDRP) as the registration or use of a domain name that is identical or confusingly similar to a trademark in which the registrant has no rights or legitimate interests, and which is registered or used in bad faith.[11]

The Uniform Domain Name Dispute Resolution Policy (UDRP) describes cybersquatting as bad-faith registration of domain names that are identical or confusingly similar to a trademark or service mark, with no rights or legitimate interests, aimed at exploiting the goodwill of the mark.[12] Indian courts have defined cybersquatting as "an act of obtaining fraudulent registration with intent to sell the domain name to the lawful owner of the trademark at a premium"[13]

B. Types of Cyber squatting

- **Typo-squatting:** This practice involves creating website addresses that have common spelling errors or small changes from popular sites (for instance, using "goggle. com" instead of "google. com") to confuse users who make typing mistakes.
- **TLD squatting:** This tactic uses the same domain name as a legitimate company but changes the last part, or top-level domain (for example, using ". net" instead of ". com"), to confuse people or redirect visitors.

[11]IN Domain Name Dispute Resolution Policy (INDRP), National Internet Exchange of India, https://www.registry.in/policies (last visited June 26, 2025)
[12]Uniform Domain Name Dispute Resolution Policy (UDRP), Internet Corporation for Assigned Names and Numbers (ICANN), https://www.icann.org/resources/pages/policy-2012-02-25-en (last visited June 26, 2025)
[13] Tata Sons Ltd, supra note 5.

- **Combo-squatting:** This method mixes a famous brand name with additional words (for example, "paypal-secure. com") to make fake websites appear reliable, and it is often used in scams.
- **Name squatting:** This involves taking the names of well-known people, stars, or business leaders as domain names to impersonate them, make money, or share misleading information.
- **IDN Homograph attacks:** This technique uses letters from different languages that resemble English characters to form website addresses that look identical to real sites, tricking users through careful deception.

C. Recent Indian case laws and statistical trends in cybersquatting

Indian courts have increasingly confronted cybersquatting through a series of recent rulings that affirm trademark owners' rights against bad faith domain registrations. The Delhi HC ordered the cancellation of several domain names that incorporated well-known trademarks like "Surf Excel" and "Fair & Lovely." The court found that the respondent had no legitimate interest in the domain names and had registered them with the sole intention of exploiting the plaintiff's goodwill and misleading consumers. The judgment emphasized that domain names today function as business identifiers comparable to trademarks, and their misuse erodes brand equity.[14] Similarly, in, the court held that the defendant's registration of "makemytravel.com" was intended to divert internet traffic by creating confusion with the plaintiff's well-known trademark, "Make My Trip." The court observed that such practices amount to cybersquatting and warrant both injunctive relief and domain transfer.[15]

The Delhi High Court held that the defendant's registration of domain names like "infosysfinance.com" and "infosysloan.com" was an act of cybersquatting intended to exploit the goodwill of the plaintiff's well-known mark. The court granted a permanent

[14] Hindustan Unilever Ltd. v. Registrar, Domain Name, 2022 SCC Del 4221
[15] Make My Trip India Pvt. Ltd. v. Make My Travel (India) Pvt. Ltd., 2021 SCC Del 2926

injunction and directed the transfer of the disputed domains to Infosys Ltd.[16] although primarily involving trademark disparagement on digital platforms, the Bombay High Court addressed domain misuse where the defendant's actions included registering a domain name similar to the plaintiff's brand to draw online attention unfairly. The court granted relief, recognizing cybersquatting as part of unfair competition in the digital space.[17]

On the statistical front, data from the National Internet Exchange of India (NIXI) shows that cybersquatting remains a persistent issue. Between 2019 and 2024, NIXI reported receiving more than 560 complaints under the INDRP, with most cases involving bad-faith registration of domain names confusingly similar to famous Indian or international trademarks. The sectors most targeted include e-commerce, travel, finance and fast-moving consumer goods. The high volume of disputes underscores the growing need for robust legal enforcement and quicker administrative remedies to protect brand owners in India's increasingly digital marketplace.[18]

D. Remedies for cybersquatting under Indian law

- **Civil remedies:** Cybersquatting is actionable under the Trade Marks Act, 1999, where the unauthorized registration or use of a domain name that is identical or deceptively similar to a registered trademark constitutes infringement under Section 29.[19] Courts may grant injunctions, damages, account of profits, or order the transfer or cancellation of the infringing domain name. Additionally, trademark owners can seek relief through the .IN Domain Name Dispute Resolution Policy (INDRP), which offers administrative remedies such as

[16] Infosys Ltd. v. Rajesh Jain, 2016 SCC Del 5184
[17] Marico Ltd. v. Abhijeet Bhansali, 2019 SCC Bom 1942
[18] National Internet Exchange of India (NIXI), INDRP Dispute Statistics, https://www.registry.in (last visited June 26, 2025)
[19] The Trade Marks Act, No. 47 of 1999, § 29

domain name cancellation or transfer upon proof of bad-faith registration, lack of legitimate interest, and confusing similarity.[20]

- **Criminal/quasi criminal remedies:** Although India does not have a specific penal provision for cybersquatting, certain acts related to cybersquatting may attract liability under the Information Technology Act, 2000, No. 21 of 2000. Section 66C penalizes identity theft, including the fraudulent use of electronic signatures or other unique identification features. Section 66D addresses cheating by personation using computer resources, which could apply where domain names are misused to impersonate legitimate entities online.[21] These offences are punishable by imprisonment and/or fine, offering a deterrent against malicious domain name practices that amount to fraud.

E. Effects of Cybersquatting

Cybersquatting can significantly damage a business by causing fraud, identity theft, or data breaches, impacting customers who think they are engaging with the authentic company. Such actions can harm the company's reputation diminish trust from the public and investors, and, in certain instances, lead to legal issues.

What makes this situation even riskier is that cyber squatters are not required to breach a company's official domain. They can easily register a web address that looks similar and set up a fraudulent website that closely imitates the genuine one. This has the potential to mislead customers and clients.

Employees can also be deceived merely clicking on a phishing email that appears to be from their own organization could compromise internal systems, making them vulnerable to malware or other security risks. Such violations not only interfere with operations but may also cause lasting harm to reputation and finances.

[20].IN Domain Name Dispute Resolution Policy (INDRP), National Internet Exchange of India, https://www.registry.in/policies (last visited June 26, 2025)
[21] The Information Technology Act, *supra* note 9

X. META TAGGING AS A HIDDEN THREAT TO TRADEMARK INTEGRITY

Meta tagging is a legitimate and helpful method for improving websites, but it can also threaten trademark rights in ways that often go unnoticed. Metatags are short codes used in a website's HTML that provide information about what the page is about. Users usually don't see these tags, but search engines read them to figure out how to show the website in search results. By including certain keywords in these metatags, website owners can boost their visibility and rankings on search engines like Google or Bing, attracting more visitors to their sites.

The legal enforcement of meta-tagging in India reflects an evolving judicial approach that applies existing trademark principles to hidden digital infringements. Courts have moved towards recognizing that invisible use of a competitor's mark in website meta-tags can amount to infringement under provisions such as Section 29(6) and 29(8) of the Trade Marks Act, 1999, [22] even though consumers never see the mark. Recent judicial trends show greater willingness to treat meta-tag misuse as actionable when it results in unfair advantage, dilution of trademark distinctiveness, or diversion of consumer traffic. At the same time, courts exercise caution to ensure that legitimate uses such as descriptive references or comparative advertising are not stifled. The primary enforcement challenge arises from the hidden nature of meta-tags, making detection dependent on technical website audits and digital forensic tools. Moreover, the dynamic nature of search engine algorithms and the cross-border reach of online marketing create jurisdictional complexities, adding to the difficulty of timely enforcement. These trends reflect a judicial effort to balance robust trademark protection against fair competition and technological realities in the digital space.

However, this function can be misused, especially regarding trademarks. A concerning issue arises when unauthorized websites use registered trademarks as meta-tag keywords, even if they have nothing to do with the actual brand. This misleading trick

[22] The Trade Marks Act, No. 47 of 1999, §§ 29(6), 29(8)

allows these sites to show up in search results when people look for the real brand, despite having no connection to the trademark owner. Such actions are a form of hidden infringement since they are not obvious to consumers, making them hard to identify until damage has occurred.

The effects of this misuse can be significant. Firstly, it undermines the main purpose of trademarks, which is to indicate the source and quality of products or services, helping them stand out in the market. When another site falsely uses a brand's trademark in metatags, it can confuse customers, redirect web traffic, and blur the lines about who is actually providing the product or service. This not only weakens customer trust but also diminishes the brand's presence in the market and lowers the trademark's effectiveness.

Additionally, some users who click on these deceptive links might end up on sites offering poor-quality or fake products, harming the reputation and goodwill of the original brand. Even worse, these infringing sites could be involved in tricking people, stealing information, or spreading harmful software, which could risk harm to both consumers and honest businesses. Employees or users who accidentally visit such sites might jeopardize company networks or reveal sensitive information.

Legally, courts in various areas are starting to view meta-tagging with another person's trademark as a valid case of trademark infringement or unfair competition, even though this happens out of public sight. For instance, U. S. courts have determined that using a competitor's trademark in meta-tags can cause initial interest confusion, where a consumer's temporary misunderstanding before making a purchase is enough to count as infringement. Similarly, Indian courts, under the Trade Marks Act of 1999, are prepared to tackle such misleading practices, especially when confusion or unfair advantage can be demonstrated. The Delhi HC addressed the misuse of trademarks as keywords and meta-tags in sponsored search results.

The court acknowledged that hidden use of trademarks in meta-tags or keyword advertising, when done without authorization, could lead to initial interest confusion and amount to infringement under Section 29 of the Trade Marks Act, 1999. The court

highlighted that while comparative advertising is permitted, using a competitor's mark in meta-tags to unfairly divert traffic crosses into infringing conduct.[23]

Similarly, the court dealt with allegations of misuse of the plaintiff's trademark as a keyword and in meta-data. While interim relief was declined on technical grounds, the court reaffirmed that the unauthorized use of a competitor's trademark in meta-tags or as search keywords could potentially attract liability where it causes confusion or unfairly leverages the goodwill of the mark.[24] The Delhi High Court considered the unauthorized use of the plaintiff's well-known trademark in meta-tags and sponsored search advertisements. The court recognized that embedding another's trademark in meta-tags, even where not visible to the user, could mislead consumers and divert traffic, amounting to infringement and passing off. It granted interim relief restraining the defendant from such use.[25]

The Delhi High Court found that the defendants' use of the mark "Snapdeal" in domain names, meta-tags, and search keywords was intended to divert online traffic and deceive consumers. The court held that such use amounted to infringement and passing off, and directed the defendants to cease use of the mark in all online content, including meta-tags.[26]

The improper use of meta-tagging can undermine the strength of trademarks without making any loud moves. It enables violators to take advantage of the good name and online visibility of well-known brands without directly stealing visual designs or text. Because it is not easily seen and can cause serious harm in the current SEO-focused online market, these actions need to be addressed with care. Improved checking, clearer laws, and greater understanding among companies are crucial for protecting trademarks from this quiet but important online risk.

[23] Bharat Matrimony Ltd. v. Google LLC, 2018 SCC Del 9346
[24] Policybazaar Insurance Web Aggregator Pvt. Ltd. v. Acko General Insurance Ltd., 2021 SCC Del 3809
[25] Bennett Coleman & Co. Ltd. v. D.B. Corp. Ltd., 2019 SCC Del 9934
[26] Snapdeal Pvt. Ltd. v. Snapdeallucknow.com, 2016 SCC Del 5004

One of the first and most important decisions in this area came from the case, decided that using someone else's trademark in meta-tags to draw in online visitors was a violation of trademark law under the Lanham Act. They pointed out that even if shoppers might catch on to the trick before buying something, the very act of misleading them was enough to create confusion that could be acted upon.[27]

In a similar case, the court recognized that a former model named Terri Welles using "Playboy" and "Playmate" in meta-tags could be a fair use under the circumstances. However, the court stressed that such uses should not mislead people or suggests an endorsement when there is none. These cases have influenced how courts think about misusing meta-tags as a subtle yet serious type of online infringement.[28] In India, while there are not many direct cases about metatags, courts have started to look at similar online trademark violations under the Trade Marks Act, 1999.

These cases show that misusing meta-tagging can seriously threaten the uniqueness and reputation of trademarks. It enables dishonest businesses to capture online visitors and goodwill by taking advantage of search engine algorithms instead of competing fairly. The danger is increased because this practice is often hidden and may go unnoticed until the brand owner sees a decline in traffic or damage to their reputation.

As a result, legal systems globally are starting to view meta-tagging with someone else's trademark as a type of digital ambush marketing. This practice avoids the usual, obvious ways of infringement and needs updated legal knowledge and technological awareness. As e-commerce and the digital economy grow, it is essential to protect trademarks online just as much as it is to safeguard them in more visible ways.

[27]Brookfield Communications, Inc, *supra* note 6
[28]Playboy Enterprises, Inc. v. Welles, 279 F.3d 796 (9th Cir. 2002)

XI. KEYWORD ADVERTISING AND SPONSORED SEARCH RESULTS-A FINE LINE BETWEEN USE AND ABUSE

Keyword advertising is a way of marketing on the internet where businesses offer money for certain words or phrases, known as "keywords," so that their advertisements show up next to search results when people look for those words. The aim is to reach users who are already interested in similar products or services. These ads usually appear as sponsored links or highlighted results at the top or side of a search results page. For instance, if a person types in "running shoes," brands like Nike or Adidas might have paid to make sure their ads are easily visible on that results page.

In the online marketing world, using keywords for advertising has become a popular method for businesses that want to boost their presence on the internet. By placing bids on certain search phrases, companies can have their ads show up more prominently on search engines like Google. However, a new issue arises when companies start bidding on trademarked words of their rivals using another brand's reputation to attract attention to their own. This creates a challenging problem. A company might feel forced to pay for its own trademarked name as a keyword just to stop competitors from exploiting its brand image. Consequently, what began as a fair marketing tactic has turned into a competitive necessity, often hurting smaller or newer businesses that can't afford ongoing bidding battles.

From a legal standpoint, this issue is not clearly outlined. The Trade Marks Act, 1999 in India does not specifically address keyword advertising because the current digital environment was not around when the law was written. The standard definition of trademark violation includes obvious and unauthorized use of a registered mark that confuses buyers. However, in keyword advertising, the trademark may never even show up on the ad it is merely used in the background to trigger the advertisement.

To fill this legal gap, courts and legal professionals have tried to apply Sections 29(6) to 29(8) of the Act, which cover broader cases of trademark use such as advertising usages

or oral references. These sections aim to safeguard brand identity even when the usage isn't directly visible. Nonetheless, because the legal interpretation is unclear, outcomes can differ from case to case. Sometimes, courts support trademark owners who feel their reputation is being misused. In other instances, courts determine there is no violation if the ad clearly indicates who the actual advertiser is and avoids confusing consumers.

Around the world, countries have different ways of handling this. In Europe, keyword advertising is frequently allowed as long as it doesn't mislead people or imply a connection to the trademark owner. In the United States, the idea of "initial interest confusion" comes into play, which means that even if users realize later that the ad isn't from the original brand, the initial confusion itself can be enough to prove trademark infringement. In India, this area of law is still developing. Until specific rules are established, trademark owners need to keep a close watch on how their trademarks are being used in online ads. At the same time, businesses should be careful when choosing keywords while fair competition is acceptable, misleading users or unfairly benefiting from another's brand is not.

In the end, keyword advertising shows how marketing is evolving in the digital age. However, when it slips into trademark misuse, it can negatively impact consumer trust and the honesty of online markets. There is a need for clearer legal guidelines to find a balance between digital progress and brand protection.

A. Keyword advertising as a fine line between proper use and misuse

- **Proper keyword use-** Keyword advertising lets businesses promote their products by bidding on popular or relevant words in search engines. This approach increases online presence, especially in competitive industries. When businesses use neutral or descriptive keywords, it is generally viewed as fair marketing online.

- **When it becomes misuse-** Things become problematic when businesses intentionally bid on their competitors registered trademarks often doing so without displaying the trademark but still reaching that brand's customers. This type of behavior makes it hard for consumers to know the source of the products or services they are considering, which can mislead them. In,[29] The ECJ ruled that if a trademark is used as a keyword in Google Ads and the ad does not help an average user identify whether it's from the trademark owner or someone else, it could be considered an infringement. This case highlighted how a lack of clarity in search results can harm a brand's image and confuse consumers.

B. Impacts of keyword advertising on trademark owners

- **Required bidding for their own brands-** Trademark owners often have to pay for ads featuring their own names just to stay visible, especially when competitors use those names to attract traffic to unrelated websites.
- **Brand confusion and trust issues-** Even temporary confusion can make customers think that competitors are linked to the brand. This can cause long-lasting damage to its reputation.
- **Need for constant monitoring-** Businesses must keep a close eye on how keywords are used, submit complaints, and sometimes take legal action, which can be expensive and time-consuming., The plaintiff (Bharat Matrimony) claimed that Google permitted competitors to use its trademark as keywords in their ads. The court recognized that misusing trademarks in keyword advertising could be an infringement under the Indian Trade Marks Act, 1999, particularly if it gives an unfair advantage or confuses consumers.[30]

[29] Google France SARL v. Louis Vuitton Malletier SA, Joined Cases C- 236/08 TO C-238/08, (2010) ECR I - 2417

[30] Consim Info Pvt. Ltd. v. Google India Pvt. Lt., (2013) 54 PTC 578 (Mad)

- **Legal and ethical ambiguity-** The legality of keyword advertising differs in various regions. In India, courts often interpret "use in the course of trade" broadly under the Trade Marks Act, 1999. However, there is no specific law yet that addresses unseen trademark use on digital platforms. Meanwhile, companies like Google argue that they only help with ad placements and do not influence how keywords are chosen. In,[31] The Delhi HC pointed out that if a competitor's trademark is used as a keyword, particularly to influence search engine rankings, it could count as an infringement if it affects the trademark's ability to identify its source. The Court also mentioned that search engines may not be entirely free from liability in these cases, especially when the ads create confusion.

Post-2020, Indian courts have continued to engage with the complexities of keyword advertising and its intersection with trademark rights. A notable example is where the Delhi High Court examined allegations of unauthorized use of a competitor's mark as a keyword for Google Ads. Although interim relief was not granted due to factual disputes, the court reiterated that keyword advertising that causes confusion or unfair advantage can amount to infringement under section 29(6) and 29(8) of the Trade Marks Act, 1999.[32]

The court addressed the misuse of the "PhonePe" mark as a keyword and in ad campaigns by competitors. The court observed that purchasing a trademark as a keyword without consent, with the intention of diverting traffic, could give rise to a cause of action for infringement, depending on the surrounding circumstances.[33] These cases reflect a judicial trend post-2020 toward stricter scrutiny of keyword advertising practices that exploit trademark goodwill, while balancing the need for fair competition in digital advertising.

[31]M/s DRS Logistics Pvt ltd, *supra* note 8.
[32] Upcurve Business Services Pvt. Ltd. v. Easy Trip Planners Ltd., 2022 SCC Del 1447
[33]PhonePe Pvt. Ltd. v. Ezy Services & Anr., 2021 SCC Del 3777

Keyword ads can be helpful, but they can also cause issues when they violate trademark rights. The purpose, how something is shown, and how buyers see it is all important factors in deciding if someone is responsible. As courts are starting to see that this kind of advertising can weaken a brand or mislead customers, trademark holders need to be vigilant, and better laws need to be developed to address these current problems effectively.

XII. CHALLENGES TO THE TRADITIONAL TRADEMARK RIGHTS BY THE ONLINE SPACES

Trademark enforcement in the online sphere presents unique challenges due to the dynamic and borderless nature of the internet. A primary difficulty lies in the anonymity of infringers, where domain registrants, hosting services, and online advertisers often conceal their identities using proxy registrations or false contact information, making it difficult for rights holders to identify and pursue the true wrongdoer. Courts in India, such as in[34] have acknowledged these challenges, particularly in cases involving keyword advertising and domain misuse.

The cross-border character of digital infringement further complicates enforcement. Many infringing websites and domain registrars operate beyond India's territorial jurisdiction, requiring reliance on international cooperation or intermediary compliance, which can delay relief. For example, scholarly commentary notes that while Indian courts can issue blocking or transfer orders; actual enforcement often depends on the voluntary cooperation of global internet service providers and domain registries.[35]

Additionally, detecting hidden infringements such as meta-tag misuse or unauthorized keyword bidding typically requires technical audits of website code or digital advertising logs, placing an evidentiary burden on trademark owners that is costly and

[34]Bharat Matrimony Ltd, *supra* note 22

[35] Shivam Goel, Cybersquatting and Domain Name Disputes: Emerging Challenges in Indian Trademark Law, 12 J. Intell. Prop. L. & Pract. 347 (2020)

time consuming. Finally, balancing trademark protection with fair use and legitimate comparative advertising poses interpretive challenges. Courts must navigate whether the use of trademarks in invisible online mechanisms is genuinely misleading or constitutes lawful competitive conduct. This calls for nuanced legal reasoning to avoid stifling fair competition while safeguarding trademark rights.

Jurisdictional conflicts are a significant barrier in online trademark enforcement, as infringers often operate websites or register domains through foreign registrars or hosting services beyond India's territorial jurisdiction. For instance, the Delhi High Court noted that the defendant's domain was registered through a foreign registrar, complicating enforcement despite the clear infringement of the plaintiff's mark. [36] Similarly, the court encountered difficulties in securing compliance with its orders against entities hosting infringing content abroad.[37]These cases illustrate how the borderless nature of the internet allows infringers to exploit jurisdictional gaps, delaying or undermining effective relief.

To address these challenges, courts and policymakers could promote greater reliance on intermediary liability mechanisms, compelling search engines, domain registrars, and internet service providers to act on judicial orders irrespective of the infringer's location. For example, dynamic injunctions where orders can be enforced against future infringing domains without filing fresh suits have gained traction in Indian copyright law and could be adapted for trademark enforcement. Additionally, enhancing international cooperation through bilateral agreements or adherence to treaties like the Madrid Protocol could facilitate swifter cross-border enforcement.

Trademark misuse on the internet often occurs in subtle ways. People can incorporate brand names into website coding, domain names, or keyword advertising without showing them to the public. This makes it hard for the real brand owner to see or prove that their trademark is being violated. Those who infringe online usually hide their

[36]Snapdeal Pvt. Ltd, *supra* note 25
[37] Bennett Coleman & Co. Ltd, *supra* note 24

identities. They might use fake identities, proxy servers, or foreign hosts, making it challenging for the trademark owner to discover who they are or where they are located. Digital infringement frequently crosses international lines. A brand in one nation might find that its rights are being infringed by a site or individual in another country, complicating legal measures and increasing costs and time. The legal system is still adapting to these issues. Most trademark laws were created before digital marketing or search engines became common, so applying them to online situations like hidden meta-tags or keyword bidding can be tricky.

XIII. CROSS-JURISDICTIONAL ISSUES IN ENFORCING TRADEMARK RIGHTS ONLINE

One of the biggest difficulties in keeping trademarks safe in the online world is dealing with enforcement across different countries. Because the internet crosses border easily, if someone breaks a trademark rule in one nation, it can harm the brand's image and business everywhere. This creates complicated legal issues since trademark rights only work in the countries where they are registered. For instance, an Indian company could discover that someone from the United States, China, or elsewhere is misusing its trademark.

Enforcing rights in these scenarios means dealing with different legal systems, language differences, and varying ideas of what counts as infringement. The absence of a single global law for trademark protection makes enforcement even trickier. While international agreements like the Paris Convention and the Madrid Protocol help with registering trademarks in many countries, they don't create a system for enforcing those rights in a unified way. Therefore, brand owners must often start multiple lawsuits in different places, and each place has its own legal steps and expenses. This is especially challenging in cases of cybersquatting or when unauthorized use happens on international sites like Amazon or social media.

Moreover, issues like determining which court should handle a case, what laws apply, and whether judgments from other countries can be enforced are significant hurdles. Some courts may not take on cases with foreign defendants or might not accept decisions from international courts unless there are treaties or agreements in place. In certain situations, finding out who is responsible can be hard because of anonymous domain names and privacy laws like the GDPR, which limit access to WHOIS information. To tackle these problems, organizations such as WIPO provide other ways to resolve disputes, like the UDRP, which helps with domain name conflicts without needing to go through national courts.

The Madrid Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks, Apr. 14, 1891, as revised June 27, 1989, 828 U.N.T.S. 390, enables rights holders to secure trademark protection across multiple jurisdictions through a single registration process. While administratively efficient, the protocol does not itself provide remedies for cross-border enforcement against infringing activities online. Likewise, the TRIPS Agreement, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, obliges member states to ensure effective enforcement measures but lacks direct mechanisms for private parties to pursue international infringement disputes, leaving trademark owners reliant on domestic courts and intermediary compliance.

Recent developments have sought to address these gaps through international cooperation frameworks. India's engagement in WIPO Advisory Committees on Enforcement and bilateral arrangements with jurisdictions like the EU and US has facilitated better coordination in combating online infringement. Notably, administrative procedures like the Uniform Domain-Name Dispute Resolution Policy (UDRP), administered by ICANN, have provided effective cross border relief in domain-related disputes, allowing trademark owners to obtain orders for domain transfer or cancellation without the delays of multi-jurisdictional litigation.

Instances which including case studies illustrate these tools in successful action. Although domestic, demonstrated how Indian courts could issue orders with extraterritorial implications by directing action through international registrars.[38] Additionally, Tata Sons Ltd. has effectively used the UDRP in several cases to recover infringing domain names registered abroad. These examples highlight that while cross jurisdictional enforcement remains complex, strategic use of treaty frameworks, administrative remedies, and intermediary cooperation offers viable pathways for rights holders. However, for more extensive enforcement issues, like those involving e-commerce or counterfeit products, it is still crucial to have national solutions and collaboration between enforcement bodies.

XIV. EMERGING TECHNOLOGICAL CHALLENGES IN TRADEMARK PROTECTION

The rise of emerging technologies particularly NFTs, virtual goods, block-chain based assets, and the metaverse has complicated trademark protection by enabling new forms of unauthorized use that do not fit neatly into traditional legal categories. Unlike conventional counterfeit goods, these digital items often involve no physical manufacturing, yet they trade on the goodwill of established trademarks, posing enforcement challenges for rights holders. Legal systems globally are adapting by applying established trademark doctrines to these novel contexts.

In, the U.S.A District Court found that Rothschild's "MetaBirkins" NFTs infringed Hermes trademarks by creating a likelihood of consumer confusion and diluting the brand's distinctive character. The court rejected the defendant's argument that the NFTs were protected artistic expression under the First Amendment, holding that the commercial nature of the digital goods outweighed any expressive value.[39]

Similarly, Nike alleged that StockX's sale of NFTs linked to Nike sneakers without authorization falsely suggested sponsorship or affiliation, raising actionable trademark

[38] Yahoo! Inc. v. Akash Arora, 78 (1999) DLT 285 (Del)
[39] Hermes Int'l v. Rothschild, No. 22-cv-384 (S.D.N.Y. Feb. 2, 2023)

infringement and dilution claims.[40]These cases highlight that courts are extending traditional principles such as likelihood of confusion, initial interest confusion and dilution to the virtual goods space, setting precedents for digital trademark enforcement.

Indian trademark law, though untested in NFT and metaverse cases so far, provides the statutory tools to address these challenges. Section 29 prohibits unauthorized use of registered marks where such use causes confusion or takes unfair advantage of the mark's reputation. As scholars have noted, Indian courts could readily apply these provisions to virtual goods, relying on international precedents as persuasive authority.[41] Further, Section 29(4) on dilution may be particularly well suited to address unauthorized use of famous marks in the digital space, where harm arises even without confusion about the source of goods. Legal commentary increasingly calls for Indian courts to take a proactive approach, employing dynamic injunctions and extending passing-off principles to digital assets, rather than waiting for legislative amendments to specifically regulate NFTs and metaverse commerce.[42]

The key challenge lies in adapting enforcement mechanisms to the realities of block-chain anonymity, decentralized platforms, and jurisdictional barriers. While international administrative systems like the UDRP provide models for swift domain related enforcement, similar frameworks are needed for virtual goods to provide cost effective remedies against digital counterfeiters who operate beyond the reach of traditional national courts.

XV. ADDRESSING GAPS IN TRADEMARK ENFORCEMENT IN THE VIRTUAL ERA

The evolution of digital spaces has significantly outpaced the capacity of traditional trademark laws, creating substantial gaps in enforcement and protection. A critical gap

[40] Nike, Inc. v. StockX LLC, No. 22-cv-983 (S.D.N.Y. filed Feb. 3, 2022)
[41] Shivam Goel, *supra* note 34.
[42] Anushka Singh, NFTs and Indian Trademark Law: Time to Act? 15 J. Tech. L. & Pol'y 112 (2022)

lies in the limited scope of national trademark statutes, which often fail to expressly cover digital goods, virtual services, or metaverse assets. For instance, while the Trade Marks Act, 1999 in India defines trademark use largely in the context of physical commerce, it does not explicitly encompass virtual merchandise or NFTs, leaving brand owners vulnerable to virtual counterfeiting and misuse.[43] The United States Patent and Trademark Office (USPTO) and the European Union Intellectual Property Office (EUIPO) have begun issuing guidelines on registering and enforcing rights over digital goods[44], signaling a model that other jurisdictions could adopt to modernize their frameworks.

Furthermore, current laws are ill-equipped to assign responsibility for AI-generated infringements. Cases where generative AI tools create marks resembling existing trademarks raise complex questions of liability. Legislative proposals such as the European Commission's draft AI Act are moving towards clarifying accountability by distinguishing between the roles of developers, users, and platforms.[45] A similar approach could be incorporated into Indian law through amendments to the Trade Marks Act or through specific regulations under the Information Technology Act, 2000.[46]

Block-chain based domains and decentralized web structures represent another regulatory blind spot. Unlike traditional domains regulated by ICANN and covered under the Uniform Domain Name Dispute Resolution Policy (UDRP), block-chain domains evade oversight, enabling cybersquatting and impersonation.[47] The absence of dispute resolution systems for these domains highlights the need for international

[43] Trade Marks Act,1999 (India). Available at https://ipandlegalfilings.com/trademark-infringement-in-the-digital-age/ (last visited June 27, 2025).
[44] USPTO virtual goods guidance, https://www.uspto.gov/trademarks/laws/virtual-goods (last visited June 27, 2025)
[45] European Commission, Proposal for AI Act (COM/2021/206 final), https://artificialintelligenceact.eu/ (last visited June 27, 2025)
[46]INLP, Trademark Infringement in Cyberspace, https://inlp.org/trademark-infringement-in-cyberspace (last visited June 27, 2025)
[47] WIPO, Blockchain and IP report, https://www.wipo.int/meetings/en/details.jsp (last visited June 27, 2025)

cooperation potentially via WIPO administered protocols or new treaties to create governance frameworks for Web3 domains.[48]

In addition, platform liability remains inadequately addressed. Although safe harbor provisions under the IT Act, 2000 (Section 79) offer intermediaries immunity, courts have begun to recognize their duty in preventing trademark misuse.[49]

And [50] To bridge this gap, legislative reform could impose positive obligations on platforms to proactively monitor, block, and act on trademark infringements, drawing inspiration from the EU's Digital Services Act.[51]

Comparatively, jurisdictions like the EU and the US are advancing frameworks to tackle cross-border enforcement challenges. The EU Enforcement Directive and collaborative measures under international instruments such as the Madrid Protocol point to the benefits of harmonized procedures.[52] India could explore bilateral or regional treaties to establish fast track dispute resolution channels and real time cooperation between enforcement agencies. Finally, the opacity created by privacy laws like GDPR has hampered trademark owner's ability to identify infringers. Legislative refinements that balance privacy with brand protection such as permitting access to WHOIS data for verified trademark disputes would support enforcement without undermining data protection goals.[53] Such measures could be accompanied by mandatory advertiser disclosure norms, ensuring accountability in digital advertising.

In light of these gaps, it is recommended that India and similarly situated jurisdictions consider

[48]SanguineSA, Legal implications of digital trademark infringement in the e-commerce era, https://sanguinesa.com/the-legal-implications-of-digital-trademark-infringement-in-the-e-commerce-era/ (last visited June 27, 2025)
[49] Consim Info Pvt. Ltd, *supra* note 7
[50] M/s DRS Logistics (P) Ltd, *supra* note 8.
[51] European Union, Digital Services Act, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last visited June 27, 2025
[52] WIPO, Madrid Protocol, https://www.wipo.int/madrid/en/ (last visited June 27, 2025)
[53] ICANN, WHOIS and GDPR balancing guide, https://www.icann.org/resources/pages/gtld-registration-data-specs_en (last visited June 27, 2025)

- Drafting amendments to include digital and virtual goods under national trademark statutes
- Introducing regulations that address AI-driven infringements and platform liability;
- Creating dispute resolution mechanisms for blockchain domains;
- Negotiating international treaties on cross-border trademark enforcement;
- Requiring advertiser and domain owner transparency for enforcement purposes.

These reforms, supported by comparative experience from the EU, the US, and WIPO would enable more effective protection of trademarks in the virtual era and promote fair digital commerce.

XVI. CONCLUSION

The digital era has expanded the boundaries of trademark infringement, exposing the inadequacy of existing legal frameworks in addressing challenges such as cybersquatting, meta-tagging, keyword abuse, unauthorized use in NFTs, metaverse counterfeiting, and block-chain domain squatting. These practices not only harm brand value and consumer trust but also undermine the fairness of digital markets. While the Trade Marks Act, 1999, the Information Technology Act, 2000, and mechanisms like the UDRP provide partial remedies, they fail to comprehensively address the realities of cross border, decentralized, and technology-driven infringements.

There is an urgent need for legislative reform to protect trademarks in the digital age. First, trademark laws should be amended to expressly cover virtual goods, digital assets, NFTs and metaverse related items as protectable subject matter. Such amendments would provide clarity in enforcement and close gaps exploited by virtual counterfeiters. Second, specific provisions should be introduced to attribute liability for AI-generated infringements, clarifying the responsibilities of developers, users, and platforms. Third, regulation of block chain-based domains should be established

through national laws or international agreements, ensuring that decentralized domains do not remain beyond the reach of trademark enforcement.

In addition, intermediary liability laws must be reformed to require platforms, search engines, and e-commerce intermediaries to actively prevent and respond to trademark misuse, drawing on models like the European Digital Services Act. Measures should also be implemented to balance privacy protections with the legitimate need for rights holders to access domain ownership and advertiser identity information in cases of suspected infringement. Finally, India should pursue international cooperation through treaties or bilateral agreements that enable faster cross-border enforcement of trademark rights, especially against online infringements.

Practically, trademark owners and practitioners must adopt forward looking strategies. These include registering trademarks for digital goods, monitoring blockchain domain activity, implementing technological tools to detect online misuse, and leveraging alternative dispute resolution mechanisms like arbitration and administrative proceedings to secure timely remedies. Such measures will be essential to protect brand identity and consumer trust in an increasingly virtual marketplace. Without these legal reforms and proactive enforcement measures, the law will continue to lag behind technological advancement, leaving brands vulnerable in the rapidly evolving digital economy.

XVII. REFERENCES

A. International / Foreign Instruments

- European Union Trade Mark Regulation (EUTMR)
- Internet Corporation for Assigned Names and Numbers (ICANN), 1998
- Lanham Act, 15 U.S.C. §§ 1051 et seq. (U.S.)

- Madrid Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks, Apr. 14, 1891, as revised June 27, 1989, 828 U.N.T.S. 390
- Paris Convention for the Protection of Industrial Property, Mar. 20, 1883, 828 U.N.T.S. 305
- TRIPS Agreement, Apr. 15, 1994, Marrakesh Agreement Establishing the WTO, Annex 1C, 1869 U.N.T.S. 299
- Trade Marks Act 1994 (UK)
- Uniform Domain-Name Dispute Resolution Policy (UDRP), 1999 (ICANN & WIPO)

B. Indian Statutes

- The Information Technology Act, 2000, No. 21 of 2000.
- The Trade Marks Act, 1999, No. 47 of 1999.
- The Trade Marks Rules, 2002, G.S.R. 740(E).
- The Trade Marks Rules, 2017, G.S.R. 199(E).

C. Case laws referred

- Bennett Coleman & Co. Ltd. v. D.B. Corp. Ltd., 2019 SCC Del 9934
- Bharat Matrimony Ltd. v. Google LLC, 2018 SCC Del 9346
- Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036 (9th Cir. 1999)
- Consim Info Pvt. Ltd. v. Google India Pvt. Ltd., 2011 (45) PTC 575 (Mad)
- DRS Logistics Pvt. Ltd. v. Google India Pvt. Ltd., CS (COMM) 1/2017 (Del)
- Google France SARL v. Louis Vuitton Malletier SA, Joined Cases C-236/08 TO C-238/08, (2010) ECR I-2417

- Hermes Int'l v. Rothschild (MetaBirkins case), No. 22-cv-384 (S.D.N.Y. Feb. 2, 2023)
- Hindustan Unilever Ltd. v. Registrar, Domain Name, 2022 SCC Del 4221
- Infosys Ltd. v. Rajesh Jain, 2016 SCC Del 5184
- Make My Trip India Pvt. Ltd. v. Make My Travel (India) Pvt. Ltd., 2021 SCC Del 2926
- Marico Ltd. v. Abhijeet Bhansali, 2019 SCC Bom 1942
- M/s DRS Logistics Pvt. Ltd. v. Google India Pvt. Ltd., 2021 SCC Del 3814
- Nike, Inc. v. StockX LLC, No. 22-cv-983 (S.D.N.Y. filed Feb. 3, 2022)
- Playboy Enterprises, Inc. v. Welles, 279 F.3d 796 (9th Cir. 2002)
- Policybazaar Insurance Web Aggregator Pvt. Ltd. v. Acko General Insurance Ltd., 2021 SCC Del 3809
- Snapdeal Pvt. Ltd. v. Snapdeallucknow.com, 2016 SCC Del 5004
- Tata Sons Ltd. v. Ramadasoft, 2005 (30) PTC 486 (Del)
- Upcurve Business Services Pvt. Ltd. v. Easy Trip Planners Ltd., 2022 SCC Del 1447
- Yahoo! Inc. v. Akash Arora, 78 (1999) DLT 285 (Del)

D. Websites referred

- European Commission, Proposal for AI Act (COM/2021/206 final) https://artificialintelligenceact.eu
- European Union, Digital Services Act, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
- ICANN, WHOIS and GDPR balancing guide, https://www.icann.org/resources/pages/gtld-registration-data-specs

- Uniform Domain Name Dispute Resolution Policy (UDRP), Internet Corporation for Assigned Names and Numbers (ICANN)https://www.icann.org/resources/pages/policy-2012-02-25-en
- INLP, Trademark Infringement in Cyberspace, https://inlp.org/trademark-infringement-in-cyberspace
- National Internet Exchange of India (Main site), https://www.registry.in/
- IN Domain Name Dispute Resolution Policy (INDRP), National Internet Exchange of India, https://www.registry.in/policies
- SanguineSA, Legal implications of digital trademark infringement in the e-commerce era
- https://sanguinesa.com/the-legal-implications-of-digital-trademark-infringement-in-the-e-commerce-era/
- USPTO virtual goods guidance, https://www.uspto.gov/trademarks/laws/virtual-goods
- WIPO, Madrid Protocol, https://www.wipo.int/madrid/en/