Domain Names As Intellectual Property: Cybersquatting And The Enforcement Vacuum In India

By *Abdul Lateef Khan*

VOLUME I | ISSUE II | ARTICLE I
JULY 2026
The Legalis IP Quarterly

ABSTRACT

India's internet economy is expanding at a pace its legal framework has failed to match. As more and more companies invest in digital identities, the registration of brand names in bad faith as domain names (cybersquatting) has become one of the country's most damaging and under-regulated threats to intellectual property. India has to date been battling domain name abuse but there is no specific legislation to regulate it.

Indian courts have tried to fill this void. Domain names have been held to be protectable business identifiers by courts, from Yahoo! Inc. v. Akash Arora (1999) to Satyam Infoway Ltd. v. Sifynet Solutions (2004). Yet the existing framework still relies on passing off doctrine and arbitration-based remedies such as the INDRP. This creates major enforcement hurdles, particularly for startups and small businesses that struggle to prove goodwill, misrepresentation and damage before any relief can even be considered. Equally neglected is reverse domain hijacking, where corporations misuse dispute-resolution mechanisms to obtain legitimately registered domains from individuals. Indian law neither recognises this harm nor penalises bad-faith complainants.

The impact of this legislative vacuum was such that in Dabur India Limited v. Ashok Kumar & Ors. (2025), the Delhi High Court was required to give systemic directions regarding registrar accountability and e-KYC verification, while adjudicating on more than 1,100 infringing domain names, as there was no legislative guidance on such matters. In comparative jurisdictions, more structured responses are available. For example, the United States' Anti-Cybersquatting Consumer Protection Act, 1999 provides for statutory damages and bad-faith

criteria. The United Kingdom and Australia incorporate safeguards against abusive registrations and complaints.

This article advocates a separate Indian legislation recognising domain names as intellectual property, providing for clear civil remedies, statutory damages and protection from reverse domain hijacking based on these models. Without legislative reform, enforcement will continue to depend upon judicial improvisation rather than coherent digital governance.

Keywords: Cybersquatting; Domain Names; Reverse Domain Hijacking; In Rem Jurisdiction; Trademark Law

I. INTRODUCTION

India's internet economy is expanding at a pace its legal framework has failed to match. As businesses pour resources into building digital identities, the registration of brand names as domain names by bad-faith actors, commonly known as cybersquatting, has emerged as one of the most damaging and under-addressed threats to intellectual property in the country. Indian courts have not been idle. Beginning with the Delhi High Court's intervention in *Yahoo! Inc. v. Akash Arora*[1] (1999) and culminating in the Supreme Court's recognition in *Satyam Infoway Ltd. v. Sifynet Solutions*[2] (2004) that domain names are business identifiers deserving of legal protection, the judiciary has stretched the doctrine of passing off and the Trade Marks Act, 1999[3] to cover domain name disputes. Yet beneath this judicial development lie deeply contested legal vacuums:

a) India's current legal framework against cybersquatting suffers from three critical gaps: no statutory damages, no statutory deterrence, and no *in rem* jurisdiction.
b) The very absence of those three safeguards enables complainants to file baseless cybersquatting complaints without fear of penalty, and Indian law does not recognise or prohibit such abuse as reverse domain hijacking, given the complete absence of statutory recognition, cost-shifting, and transparency provisions.

[1] *Yahoo! Inc. v. Akash Arora*, CS(OS) No. 903 of 1999 (Del. H.C. 1999) (India).

[2] *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*, (2004) 6 SCC 145 (India).

[3] Trade Marks Act, No. 47 of 1999, India Code (1999).

This article examines four analytical units: three gaps arising from India's failure to legislate against cybersquatting and one mirror failure arising from its complete statutory silence on reverse domain hijacking, and proposes a unified statutory remedy for all four.

II. PRELIMINARY: THE INTELLECTUAL PROPERTY STATUS OF DOMAIN NAMES IN INDIAN LAW

The title of this article rests on a proposition that is neither speculative nor novel, but one that Indian courts have affirmed for over two decades: domain names, though conceived as technical routing mechanisms, have acquired the characteristics of intellectual property. A domain name today is not merely a string of characters that directs internet traffic. It is a commercial identifier, a source of goodwill, and an asset capable of transfer, licensing, and assignment.

The Supreme Court of India settled this question in *Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.* (2004), holding that a domain name "may have all the characteristics of a trademark" and that an action for passing off can lie for its misuse.[4] The Court recognised that domain names distinguish goods and services, identify their source, and influence consumer choice functions identical to those of trademarks. Before *Satyam Infoway*, the Delhi High Court in *Yahoo! Inc. v. Akash Arora* (1999) had already rejected the argument that domain names are merely addresses, observing that a domain name is a primary identifier that performs the same function as a trademark in the digital marketplace.[5] Subsequent High Court decisions, including *Rediff Communication Ltd. v. Cyberbooth*[6] and *Tata Sons Ltd. v. Fashion ID Ltd.*[7], reinforced this understanding, treating typo-squatting and deceptive registration as actionable forms of passing off. Indian courts have further recognised domain names as intangible property with economic value, capable of being transferred, assigned, or licensed, characteristics that align domain names with other intellectual property rights in the commercial context.[8]

[4] *Satyam Infoway*, supra note 2, at 152

[5] *Yahoo!,* supra note 1.

[6] *Rediff Commc'n Ltd. v. Cyberbooth*, AIR 2000 Bom 27 (India).

[7] *Tata Sons Ltd. v. Fashion ID Ltd.,* CS(OS) No. 1273 of 2005 (Del. H.C. 2005) (India).

[8] *Satyam Infoway*, supra note 2, at 153–54.

This article does not argue for the creation of a new category of intellectual property, but proceeds from the settled position that domain names, when used in commerce, acquire proprietary characteristics that entitle them to legal protection. The enforcement vacuum examined in the following sections operates in both directions: it fails trademark owners who cannot pursue cybersquatters, and it fails legitimate domain name holders who cannot defend against abusive complainants. Both failures share the same legislative cause. The question is not whether domain names deserve protection, but whether India's current legal framework, fragmented, borrowed, and judicially improvised, can deliver it.

III. CRITICAL GAPS IN THE INDIAN CYBERSQUATTING FRAMEWORK

A. No Standalone Cybersquatting Act

India lacks any dedicated legislation prohibiting cybersquatting, forcing trademark owners to rely on the borrowed framework of the Trade Marks Act, 1999, and the administrative dispute resolution policies, including the Uniform Domain-Name Dispute-Resolution Policy ("UDRP")[9] and.IN Domain Name Dispute Resolution Policy ("INDRP")[10] is a patchwork that fragments enforcement, imposes evidentiary burdens never designed for domain disputes, and creates jurisdictional blind spots that sophisticated squatters routinely exploit.

This fragmented framework operates under the assumption that cybersquatting is merely a subspecies of trademark infringement or passing off, and that administrative alternative dispute resolution ("ADR") can resolve most disputes cheaply and quickly. A trademark owner must prove existing goodwill, a costly and fact-intensive inquiry, before a court will even consider a domain name claim. The UDRP and INDRP, while cheaper, cannot award damages, cannot grant injunctions beyond domain transfer, and have no extraterritorial reach against foreign registrants who register .com domains. The result is a two-tier system: large corporations can afford civil litigation to seek damages, while small businesses, startups, and individual entrepreneurs are effectively limited to the UDRP or INDRP, which offer no financial deterrent whatsoever. Worse still, when registrants hide behind privacy services or use fictitious WHOIS

[9]Uniform Domain-Name Dispute-Resolution Policy, ICANN (Oct. 24, 1999), https://www.icann.org/resources/pages/policy-2012-02-25-en.

[10].IN Domain Name Dispute Resolution Policy, NIXI (2005), https://www.nixi.in/indrp.

details, as in *Colgate Palmolive v. NIXI* (2025), where the Delhi High Court found that Domain Name Registrars ("DNRs") were "providing privacy protection as a default 'opt out' system, thereby masking the identities of registrants even from trademark owners"[11]. As a result, even the UDRP/INDRP cannot proceed because the registrant cannot be identified, resulting in a major procedural failure.

It is argued that strengthening the UDRP/INDRP, expanding the INDRP's scope, reducing fees or mandating registrar compliance would be preferable to a new statute, keeping costs low and decisions fast. But speed is irrelevant when the remedy lacks teeth. Neither policy can award statutory damages, costs, or attorneys' fees. A squatter who loses a UDRP complaint loses only the domain name, a negligible risk. Moreover, the INDRP applies only to .in domains; India cannot unilaterally amend the UDRP for .com, .org, and other generic Top-Level Domains ("gTLDs").

a) **International Models of Standalone Cybersquatting Legislation**

The absence of a standalone cybersquatting act in India is not inevitable. Two jurisdictions in particular offer instructive, if divergent, responses: the United States, which has enacted a freestanding civil cybersquatting statute, and South Korea, which has integrated cybersquatting regulation into a comprehensive internet address resources law.

i. **The United States**

The Anti-Cybersquatting Consumer Protection Act ("ACPA"), 15 U.S.C. § 1125(d), enacted in 1999, was the world's first standalone cybersquatting statute.[12] Congress enacted the ACPA precisely because existing trademark laws were "an inadequate deterrent to cybersquatting because the threat of sanction did not outweigh the reward gained by engaging in the wrongful behaviour."[13] The ACPA establishes cybersquatting as an autonomous civil wrong, not a derivative of trademark infringement, defined as the bad-faith registration, trafficking, or use of a domain name that is identical or confusingly similar to a distinctive trademark. For India, the ACPA demonstrates that a standalone civil statute can transform cybersquatting from a hard-to-prove trademark claim into a clearly defined, easily enforceable wrong,

[11] *Colgate Palmolive Co. v. NIXI*, 2025:DHC:11874 (Del. H.C. Dec. 24, 2025).

[12] Anti-Cybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (2018).

[13] S. Rep. No. 106-140, at 5–6 (1999) (explaining that the threat of sanction under existing trademark law did not outweigh the reward from cybersquatting).

eliminating the requirements of proving goodwill, misrepresentation, or actual consumer confusion that currently paralyse Indian trademark owners.

ii. **South Korea: Comprehensive Regulation Under the Act on Internet Address Resources(AIAR).**

South Korea has enacted a comprehensive, self-contained statutory regime for cybersquatting through its Act on Internet Address Resources ("AIAR"), enacted in 2004 and subsequently amended.[14] Unlike the US ACPA, which remains an amendment to the Lanham Act, Korea's AIAR is a freestanding law governing all aspects of internet address resource management, including cybersquatting. The AIAR establishes a dual-track system: an administrative dispute resolution procedure through the Korea Internet Dispute Resolution Committee (KIDRC) that can order transfer or cancellation of a .kr domain name, alongside civil court actions for damages.[15] For India, Korea's integrated statutory framework shows that a standalone cybersquatting law can coexist with and complement both trademark law and administrative ADR, creating clear statutory definitions and remedies without forcing trademark owners to fit domain disputes into legal categories never designed for them.

India can adopt a blended framework that draws from both the US and South Korean models. From the United States, it should borrow the ACPA's foundational principle: a freestanding civil statute that defines cybersquatting as an autonomous legal wrong, independent of trademark infringement or passing off, eliminating the requirement to prove goodwill or actual consumer confusion, which currently paralyses Indian trademark owners. From South Korea, it should adopt the integrated dual-track architecture of the AIAR: a comprehensive statutory framework that governs domain registration, dispute resolution, and enforcement within a single legal system. The AIAR establishes an Internet Address Dispute Resolution Committee (KIDRC) with powers to order domain transfer or cancellation in expedited, low-cost proceedings, while simultaneously preserving the right of aggrieved parties to pursue civil remedies in court for damages. This dual-track approach allows complainants a choice: a quick administrative remedy for those who only seek domain transfer, or full civil litigation for those seeking financial compensation. Crucially, the AIAR also mandates that bad faith be

[14] Act on Internet Address Resources, Act No. 7142 (S. Kor. 2004, as amended 2009).

[15] Act on Internet Address Resources art. 16–18, Act No. 7142 (S. Kor. 2004).

determined through statutory factors such as whether the registrant has legitimate rights, prior use of the domain, or a pattern of offering to sell domains for profit, providing predictability that Indian courts currently lack. India can replicate this blended model by enacting a standalone Cybersquatting Prohibition Act that combines the US's autonomous civil liability with South Korea's integrated dual-track system, creating a coherent statutory framework that offers both expedited administrative transfer and civil damages.

The absence of a standalone cybersquatting statute identified in this section is not merely a classificatory failure; it has direct and measurable consequences for the remedies available to trademark owners. A statutory damages regime requires a statute to live in. Because India has never enacted one, the question of financial deterrence has been left entirely to the Trade Marks Act's actual loss framework and the UDRP's expressly non-monetary remedies, a remedial vacuum that the next gap examines.

B. No Meaningful Deterrence

India's current legal framework against cybersquatting lacks any effective deterrent, as it provides no statutory damages, leaving trademark owners with no meaningful financial remedy against bad-faith registrants and creating a low-risk, high-reward environment that actively incentivises cybersquatting.

The Trade Marks Act, 1999, India's primary intellectual property statute, predates the commercial internet and contains no provision for statutory damages (a fixed sum recoverable without proof of actual loss). Under Section 135, a court may grant an injunction and, in appropriate cases, award actual damages or an account of profits.[16] The UDRP and the INDRP further provide only for cancellation or transfer of the domain name and expressly prohibit any award of monetary relief. Consequently, a cybersquatter risks nothing more than the loss of a domain name that costs a few hundred rupees to register, while the potential reward, a ransom payment of several lakhs or sustained advertising revenue, remains enormous.

This framework operates under the assumption that monetary relief is either unnecessary (UDRP/INDRP) or requires proof of actual loss. A squatter registers hundreds of domains, demands modest ransoms from each, and even if a few are recovered through UDRP, retains the profits from the rest. Proving actual loss from a parked domain is practically impossible.

[16]Trade Marks Act § 135, No. 47 of 1999, India Code (1999).

The Delhi High Court in *Adobe Inc. v. Namase Patel* (2022) — before Justice C. Hari Shankar — awarded ₹2 crore in exemplary damages because the defendant was a "habitual cyber squatter" – a finding that required full-blown litigation and proof of a pattern, something most trademark owners cannot afford or establish.[17] The absence of statutory damages means that for every *Adobe*, there are dozens of cases where trademark owners abandon their claims, pay the ransom, or settle for a bare transfer without compensation. Small businesses, startups, and individual entrepreneurs are priced out of civil litigation entirely. The UDRP and INDRP, while cheaper, offer no financial deterrent whatsoever. The squatter's calculus remains unchanged: the cost of registration is negligible; the risk is negligible; the potential reward is substantial.

The result is that cybersquatting persists as a predictable, economically rational business model. India's Information Technology Act, 2000[18], contains no provision to penalise cybersquatting, and courts have held that domain disputes are civil in nature.[19] Thus, the absence of statutory damages is not a minor lacuna; it is the central reason why India's current framework has no teeth.

IV. Comparative Models That India Can Adopt

The absence of statutory damages in India's legal framework is not inevitable. Three jurisdictions in particular offer instructive, if divergent, responses: the United States, which has perfected civil deterrence through the Anti-Cybersquatting Consumer Protection Act; the Philippines, which has taken the path of aggressive criminalisation under its Cybercrime Prevention Act; and India's own Jan Vishwas framework, which has pioneered a graded "inform–correct–penalise" model for decriminalising regulatory offences.

A. **The United States.** The ACPA remains the gold standard for civil deterrence. Congress enacted the ACPA precisely because existing laws were "an inadequate deterrent to cybersquatting because the threat of sanction did not outweigh the reward gained by engaging in the wrongful behaviour." The ACPA provides statutory damages of $1,000

[17] *Adobe Inc. v. Patel*, 2022/DHC/005253 (Del. H.C.) (India).

[18] Information Technology Act, No. 21 of 2000, India Code (2000).

[19] *Dr. Madhukar G. Angur v. State of Karnataka*, Crl. P. No. 11024 of 2023 (Karn. H.C. 2025) (India).

to $100,000 per domain name recoverable without proof of actual loss,[20] *in rem* jurisdiction to sue the domain itself when the registrant is anonymous,[21] and nine non-exhaustive bad-faith factors that guide courts and create predictability.[22] The mere threat of statutory damages has led to swift settlements in most cases, with defendants relinquishing domains rather than face up to $100,000 per domain in liability.

B. **The Philippines.** Section 4(a)(6) of Republic Act No. 10175, the Cybercrime Prevention Act of 2012, explicitly criminalises cybersquatting as "the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same."[23] The penalties are severe: imprisonment of six years and one day to 12 years, or a fine of at least PHP 200,000 (approximately USD 3,500), or both. The Philippine Supreme Court upheld the provision in *Disini v. Secretary of Justice* (2014), ruling that "what the law punishes is the bad faith attending the registration, not the mere similarity of names."[24]

C. **India's Jan Vishwas Framework.** The Jan Vishwas (Amendment of Provisions) Act, 2023[25], decriminalised 183 provisions across 42 Central Acts, converting minor defaults from criminal offences into civil penalties. The Jan Vishwas Bill, 2026 (as proposed)[26] seeks to decriminalise 717 provisions across 79 laws, further extending the graded "inform–correct–penalise" model: no penalty for a first-time contravention if an improvement notice is complied with; penalties apply only from the second offence onwards. The philosophy recognises that most violations lack malicious intent and are better addressed through civil penalties, and that it is the repeat violation that justifies criminal liability.

Further, the Delhi High Court has taken a decisive judicial step to address the anonymity that enables cybersquatting. In December 2025, Justice Prathiba M. Singh, in *Dabur India Ltd. v. Ashok Kumar & Ors.*, held that "allowing anonymity in domain registrations had made it

[20] 15 U.S.C. § 1117(d) (2018) (providing for statutory damages of $1,000 to $100,000 per domain name in cybersquatting actions).

[21] 15 U.S.C. § 1125(d)(2)(A) (2018).

[22] 15 U.S.C. § 1125(d)(1)(B)(i) (2018) (listing nine non-exhaustive factors for determining bad faith intent).

[23] Republic Act No. 10175 § 4(a)(6) (Phil. 2012) (Cybercrime Prevention Act of 2012).

[24] *Disini v. Secretary of Justice*, G.R. No. 203335, 716 SCRA 237, 292 (Phil. 2014).

[25] Jan Vishwas (Amendment of Provisions) Act, No. 18 of 2023, India Code (2023).

[26] Jan Vishwas (Amendment of Provisions) Bill, 2026 (India) (as introduced).

difficult for brand owners, banks, and law enforcement agencies to trace offenders" and that "privacy by default" was a key reason for the proliferation of illegal domain names.[27] The Court ordered that all DNRs in India must: (i) implement mandatory e-KYC verification at registration; (ii) end automatic privacy protection, making it a paid, opt-in service; (iii) disclose complete registrant details within 72 hours of a court or law enforcement request; (iv) appoint grievance officers in India to accept court orders by email; and (v) lose safe harbour under Section 79 of the IT Act for non-compliance. Banks were also directed to implement beneficiary name lookup facilities. The e-KYC mandate attacks the anonymity gap directly, attaching a verified legal identity to every domain name. However, it remains a judicial order, not a statute. It cannot award statutory damages, and its enforcement against foreign DNRs is uncertain. Its existence, therefore, powerfully reinforces the central thesis: judicial improvisation is not a substitute for legislation.

India can adopt a blended framework that draws from all three models. From the United States, it should borrow the ACPA's civil remedies: statutory damages of $1,000–$100,000 per domain (adapted as ₹10–25 lakh for first offences), *in rem* jurisdiction to sue the domain itself, and nine bad-faith factors to guide courts. From the Philippines, it should take the criminal deterrence principle, but only for aggravated cases, not blanket criminalisation with imprisonment up to three years and fines up to ₹25 lakh, subject to a judicial filter of wilful bad faith. From India's own Jan Vishwas framework, it should adopt the graded "inform–correct–penalise" model: a first-time cybersquatter receives an improvement notice and faces only civil statutory damages (₹10–25 lakh), with no penalty if the domain is voluntarily transferred; repeat contraventions within five years attract enhanced statutory damages (₹50 lakh) without notice; criminal prosecution is reserved for a pattern of three or more infringing domains, collection of money from victims, or use for phishing or identity theft, and requires a prior judicial finding of wilful bad faith with intent to defraud. Finally, the Delhi High Court's e-KYC mandate must be codified into statute, ending automatic privacy protection, mandating verified identity and 72-hour disclosure, and imposing liability on non-compliant registrars. This hybrid approach gives India the strongest civil deterrent in the world (from the US), reserves criminal sanctions for the worst offenders (from the Philippines, but filtered), anchors enforcement in verified identity (from the e-KYC mandate), and structures liability through a graduated, decriminalised first step (from Jan Vishwas) avoiding the over-criminalisation

[27] *Dabur India Ltd. v. Ashok Kumar & Ors., 2025:DHC:11862 (Del. H.C. Dec. 24, 2025).*

pitfalls of the pure Philippine model while exceeding the purely civil US model where fraud is involved.

C. No In Rem Jurisdiction

a) The Procedural Impossibility

India's current legal framework against cybersquatting offers no mechanism to sue a domain name itself when the registrant is anonymous or cannot be located, requiring trademark owners to obtain personal jurisdiction over an often-untraceable defendant, a procedural impossibility that renders the entire enforcement apparatus useless whenever a squatter hides behind privacy protection services.

Indian courts can only exercise personal jurisdiction over a domain name registrant. The plaintiff must identify the registrant, locate them, and effect service of process within the court's territorial jurisdiction. This framework becomes unworkable when registrants exploit WHOIS privacy protection now offered as a default "opt out" service by most DNRs or provide fictitious, incomplete, or foreign contact information. The Trade Marks Act, 1999, contains no provision for proceeding against a domain name *in rem* (as property), nor does the Civil Procedure Code, 1908[28], recognise a domain name as property capable of being sued independently of its owner.

b) The Scale of the Anonymity Problem

This jurisdictional vacuum operates under the assumption that a cybersquatter can always be identified and personally served. In practice, that assumption is false. The Delhi High Court in *Colgate Palmolive Company & Anr. v. NIXI & Anr.* (2025) found that "the WHOIS details of infringing domain names were systematically masked by DNRs using 'privacy protect' features, preventing plaintiffs from initiating proceedings against the actual perpetrators".[29] The Court further observed that "DNRs were providing privacy protection as a default 'opt out' system, thereby masking the identities of registrants even from trademark owners".[30]

[28] Code Civ. Proc., No. 5 of 1908, India Code (1908).

[29] *Colgate Palmolive,* supra note 11.

[30] *Id.*

The same anonymity crisis emerged in *Dabur India Ltd. v. Ashok Kumar & Ors.* (2025), where the plaintiff discovered numerous infringing domain names, but "WHOIS records often reveal fabricated names, incorrect addresses, inactive phone numbers, and email IDs created solely for the purpose of registration".[31] The Court noted that "by the time a trademark owner secures injunctive relief or disclosure orders, the fraudster has often vanished, funds have been withdrawn, and victims have suffered irreparable loss".[32] The scale of the fraud was staggering: status reports indicated that "crores of rupees had been fraudulently collected from innocent persons duped by these infringing domain names".[33] Yet without personal jurisdiction over the anonymous registrants, the courts could not order transfer or cancellation of the domains except through the imperfect mechanism of John Doe orders and directions to registrars – remedies that require continuous judicial supervision and do not operate against the domain itself as an asset.

The e-KYC mandate issued in *Dabur* requiring DNRs to verify registrant identity, end automatic privacy protection, and disclose details within 72 hours of a court or law enforcement request – is a significant judicial step forward. But it remains a judicial order, not a statute, and does not confer *in rem* jurisdiction where e-KYC fails (e.g., foreign registrants who used verified but offshore identities, or pre-e-KYC registrations). The fundamental procedural gap persists: Indian courts cannot adjudicate rights to a domain name without first finding a human defendant.

c) **International Models That India Can Adopt**

The inability to reach anonymous domain registrants is not an inevitable feature of cybersquatting law. Two jurisdictions in particular offer different but instructive responses: the United States, which has codified a direct statutory *in rem* remedy that allows suit against the domain name itself, and Japan, which has created a statutory dispute resolution policy for its ccTLD combined with a procedural rule treating domain names as property for jurisdictional purposes. Together, they provide a set of legislative experiments and procedural innovations from which India can draw.

[31] *Dabur India,* supra note 27.

[32] *Id.*

[33] *Id.*

i. **The United States: Statutory In Rem Jurisdiction Under the ACPA.** The ACPA, 15 U.S.C. § 1125(d), contains the world's most direct statutory solution to the anonymity problem. Section 1125(d)(2)(A) provides that "the owner of a mark may file an *in rem* civil action against a domain name in the judicial district in which the domain name registrar, domain registry, or other domain name authority that registered or assigned the domain name is located".[34] The ACPA permits an *in rem* action when the plaintiff cannot obtain personal jurisdiction over the registrant, either because the registrant cannot be located through due diligence or because the registrant is outside the court's territorial jurisdiction. The action is brought directly against the domain name itself, treated as property located in the judicial district of the registrar. The court's remedial power is limited to ordering the cancellation or transfer of the domain name, with no monetary damages available in an *in rem* proceeding. This limitation is precisely calibrated: *in rem* jurisdiction solves the procedural problem of anonymity, while statutory damages (addressed in Gap 2) provide the economic deterrent. For India, the ACPA's *in rem* provision offers a directly transposable model. It requires no physical presence of the registrant, no identification of the squatter, and no international service of process. The trademark owner files suit against the domain name; if the domain name's registrar has a place of business in India, an Indian court can assert *in rem* jurisdiction. Given that most major DNRs (GoDaddy, Namecheap, Bigrock, etc.) have substantial operations in India, this would cover the overwhelming majority of gTLD registrations.

ii. **Japan: Statutory Dispute Resolution and the Property-Based Jurisdictional Rule.** Japan has established a statutory framework for .jp domain name disputes through the Japan Network Information Centre ("JPNIC").[35] JPNIC has adopted the "JP Domain Name Dispute Resolution Policy" ("JP-DRP"), which applies to all .jp domain registrations. Under this policy, a trademark owner may request dispute resolution from a provider approved by JPNICC. Currently, the Japan Intellectual Property Arbitration Centre ("JIPAC") and the Japan Arbitration Institute ("JIA") are accredited for this purpose. The complainant may request either cancellation or transfer of the domain name. The policy applies to all .jp domains regardless of who the registrant is or where

[34] 15 U.S.C. § 1125(d)(2)(A) (2018).

[35] Japan Network Information Center (JPNIC), JP Domain Name Dispute Resolution Policy (July 19, 2000), https://www.nic.ad.jp/doc/jpnic-01328.html.

they are located, and the dispute resolution decision is binding under the terms of the registration agreement.

Crucially, Japan has also solved the gTLD anonymity problem through a procedural innovation. Article 1(f) of the Rules for JP Domain Name Dispute Resolution Policy defines "mutually agreed jurisdiction" as either the Tokyo District Court or the court having jurisdiction over the registrant's address recorded by Japan Registry Service (JPRS).[36] For India, this dual approach offers a directly transposable model: a statutory dispute resolution policy for .in domains combined with a court rule treating domain names as property capable of being sued independently of the registrant.

India can adopt a blended framework that draws from both the US and Japanese models to close the anonymity gap. For gTLDs (.com, .org, etc.), where India cannot unilaterally amend the UDRP, the most effective remedy is to replicate the US ACPA's statutory *in rem* jurisdiction provision: a standalone action against the domain name itself, filed in the judicial district where the DNR is located, with the remedy of cancellation or transfer. For .in domains, India should adopt Japan's statutory dispute resolution model: give NIXI statutory authority under a standalone Cybersquatting Prohibition Act to order transfer or cancellation of .in domain names based on documentary evidence alone, without requiring the complainant to identify or serve the registrant. Additionally, India should amend the Civil Procedure Code, 1908, to treat domain names as property located in India for jurisdictional purposes, replicating Japan's "mutually agreed jurisdiction" rule as a fallback for cases where the registrant remains anonymous or is located outside India. One limitation must be acknowledged: even a CPC amendment would not confer jurisdiction over a domain name whose registrar has no presence in India. To address this, India should require, as a condition of doing business with Indian registrants, that all DNRs maintain a registered agent in India, a legislative extension of the *Dabur* court's direction requiring DNRs to appoint grievance officers in India.[37] This hybrid approach gives India a statutory *in rem* remedy for gTLDs (from the US), a statutory dispute resolution committee for .in domains (from Japan), a property-based jurisdictional rule (also from Japan), a legislative fix for foreign registrars (extending the *Dabur* direction), and codified judicial innovation (from the e-KYC mandate) permanently closing the anonymity

[36] *Japan Network Information Center (JPNIC), Rules for JP Domain Name Dispute Resolution Policy art. 1(f) (July 19, 2000),* https://www.nic.ad.jp/doc/jpnic-01222.html.

[37] *Dabur India*, supra note 27*; see also Colgate Palmolive,* supra note 11.

gap and ensuring that Indian courts and dispute resolution authorities can adjudicate rights to domain names without first finding a human defendant. Without the ability to identify or sue the registrant through e-KYC, statutory dispute resolution, or *in rem* jurisdiction, the civil and criminal remedies proposed in other gaps would remain entirely theoretical.

V. THE MIRROR FAILURE: REVERSE DOMAIN HIJACKING AND INDIA'S COMPLETE STATUTORY SILENCE

The three cybersquatting gaps examined above establish that India's enforcement vacuum operates in one direction: it fails trademark owners who cannot effectively pursue bad-faith registrants. But the same legislative silence that empowers cybersquatters also enables abuse in the opposite direction, reverse domain hijacking, where trademark owners themselves file baseless UDRP or INDRP complaints to wrest a domain name from a legitimate registrant. The mirror-failure thesis is this: where cybersquatting is the abuse of the registration system by an anonymous bad-faith registrant, reverse domain hijacking is the abuse of the complaint system by a known but unaccountable complainant. India's law recognises neither wrong, provides no remedy to either victim, and imposes no consequence on either wrongdoer. This Part addresses the mirror harms.

This symmetry is not merely rhetorical; it follows from a single structural fact. India has never enacted a domain name statute of any kind: it possesses only judge-made doctrine borrowed from trademark law, and two privately administered policies, the UDRP and the INDRP, that sit entirely outside the formal legal system. Any regime that creates a cheap, fast mechanism for a trademark owner to recover a domain name will, by the same mechanism, create a cheap, fast mechanism for a trademark owner to seize a domain name it has no right to: the procedural shortcut that helps the genuine claimant is precisely what the illegitimate claimant exploits. Parts II and III of this article, therefore, examine one enforcement vacuum from its two faces: Part II asked what happens when the system is too weak to stop a bad-faith registrant; this Part asks what happens when the system is too weak to stop a bad-faith complainant. Both questions return the same answer: nothing, because neither protection was ever legislated into existence in the first place.

A. India's Statutory Silence on Reverse Domain Hijacking

Indian law does not recognise reverse domain hijacking as any form of legal wrong, not as a civil wrong, not as a statutory violation, not as an abuse of process under the Civil Procedure Code. A legitimate domain name holder who successfully defeats an abusive complaint has no cause of action, no remedy for costs, and no prospect of compensation under India's domestic legal framework.

The reason the CPC offers no recourse is doctrinal, not incidental. Abuse of process under Indian laws, either in relation to tort or as a reason for striking out of pleadings as per Order VI Rule 16 of CPC, relates to the abuse of process of the court in itself. In simple terms, the effect of this rule can be understood in the light of the fact that it provides the court with a power to strike out those matters which are found to be frivolous or vexatious in nature or even amount to an abuse of the process of the court. However, a UDRP/INDRP proceeding is neither a plea filed in an Indian court nor an administrative one. Order VI Rule 16, therefore, has no pleading to strike, because there is no pleading: the power simply has nothing to attach to. Malicious prosecution offers no alternative route either. Indian courts have confined the tort, in its civil form, to proceedings that cause calculable damage—the arrest of a person, the attachment of property, an injury to credit or reputation—and have consistently declined to treat the mere cost of defending an unsuccessful civil claim as sufficient. England scrapped this limitation in Willers v. Joyce [2016] UKSC 43 by expanding the law of malicious prosecution to all civil cases; however, Indian courts have not gone down this road, even if they had, then a proceeding under UDRP/INDRP is not a "prosecution" in any way recognised by the said courts. And this is exactly what makes statutory regulation imperative: not because Indian courts are not interested in policing abuse, but simply because the legal weapons at their disposal were designed for litigation in courts.

Under Rule 15(e) of the UDRP Rules, a WIPO panel may make a finding of "Reverse Domain Name Hijacking" when a complaint is dismissed.[38] But this is merely a declaratory finding. The panel cannot award costs, cannot order damages, cannot sanction the complainant's lawyers, and its finding has no binding effect in India. The same limitations apply to expert determinations under the INDRP. An Indian complainant found guilty of RDNH in a WIPO proceeding, as several have been, faces no domestic legal consequence whatsoever: no order

[38]Rules for Uniform Domain-Name Dispute-Resolution Policy r. 15(e) (ICANN 2013) [hereinafter UDRP Rules]; see also *Rules for Uniform Domain-Name Dispute-Resolution Policy* r. 1 (defining "Reverse Domain Name Hijacking" as "using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name").

to pay the respondent's costs, no statutory damages, no public record of abuse maintained by any Indian authority, and no sanction against the lawyers who filed the abusive complaint. As one WIPO panel observed, the only sanction available to the Panel is to make a finding of Reverse Domain Name Hijacking, a statement that the complaint was an abuse of process, but nothing more. For a legitimate domain name holder who has just spent lakhs of rupees defending a baseless complaint, that statement is no remedy at all.

B. The Scale of the Problem: Indian Complainants and the Absence of Domestic Consequence

This legal vacuum is not theoretical. WIPO panels have found multiple Indian complainants guilty of reverse domain hijacking in recent years, yet none have faced any domestic legal consequences.

In *Innoviti Technologies Private Limited v. Innoviti S.A.S.* (WIPO Case No. D2023-0108),[39] a large Indian payments company filed a UDRP complaint against a Colombian technology company that was using the domain name innoviti.com.co for a legitimate business. The complainant falsely asserted that the respondent was not using the domain for any bona fide offering, despite the respondent's website clearly showing a legitimate business. The panel found that the complaint was "highly misleading," that the certification given by the complainant could not properly have been made, and that the only sanction available was a finding of Reverse Domain Name Hijacking, which the panel imposed.

In *Nalli Chinnasami Chetty v. Jennifer Nalli* (WIPO Case No. D2024-3556),[40] an established Indian textile manufacturer attempted to wrest the domain name nallifinancialservices.com from a US-based entrepreneur whose surname was "Nalli" and who had registered the domain for a bona fide financial services business. The panel found that the complainant should have known that the domain owner had a legitimate right to her own surname and that the case was brought in bad faith. The panel imposed a finding of reverse domain hijacking.

[39] *Innoviti Technologies Private Limited v. Richard Cardenas, INNOVITI S.A.S., WIPO Arbitration and Mediation Center Case No. DCO2023-0108 (January 30, 2024).*

[40] *Nalli Chinnasami Chetty v. Jennifer Nalli*, WIPO Arbitration & Mediation Ctr. Case No. D2024-3556 (2024).

In *Luxury India Solutions PVT. LTD. v. Matrimony.com Limited* (WIPO Case No. D2023-3976),[41] an Indian matrimony website, attempted to reverse hijack the domain jodii.com from a competitor. The panel found that the complainant, represented by counsel, should have appreciated the weakness of its case. The term "jodi" is generic; the domain was registered years before the complainant acquired any trademark rights, and the complainant had made false statements to mislead the panel. The panel imposed a finding of reverse domain hijacking. The panel also noted that the complainant had ignored a prior court order upholding the respondent's rights.

Luxury India Solutions is the most analytically significant of the three cases catalogued here, because it is the only one in which the complainant had already lost on the same dispute in an Indian court before ever filing the UDRP complaint. The panel's finding that the complainant had ignored a prior court order upholding the respondent's rights means an Indian court had already adjudicated this question in the respondent's favour—and the complainant simply pursued the identical claim in a different forum rather than accept that result. This is the structural failure identified in Section A, made concrete: because a UDRP proceeding is not a pleading before an Indian court, nothing in the Civil Procedure Code barred the complainant from re-litigating a question an Indian court had already settled, and no doctrine of res judicata or abuse of process attached to the WIPO filing at all. That the complainant was represented by counsel throughout makes this more troubling, not less: this was not an unrepresented party stumbling into an abusive filing, but a legally advised litigant choosing to press a claim a court had already rejected, in a forum with no mechanism to recognise that prior judgment and no consequence for ignoring it. If reverse domain hijacking persists even against parties with every resource to know better, the case for a mandatory, cost-shifting deterrent—rather than a discretionary declaratory finding—only gets stronger.

None of these Indian complainants faced any domestic legal consequence. The domain name holders who successfully defended their rights were left to bear their own legal costs, often running into several lakhs of rupees, with no recourse under Indian law.

The problem is not confined to isolated cases. Global data confirms a sharp increase in reverse domain hijacking findings. UDRP.tools reports 86 RDNH decisions across WIPO and its main

[41] *Luxury India Solutions Pvt. Ltd. v. Matrimony.com Ltd.*, WIPO Arbitration & Mediation Ctr. Case No. D2023-3976 (2023).

competitor, FORUM, in 2025, compared to 56 in 2024, 50 in 2023, and 47 in 2022.[42] Even where RDNH is not formally found, panels are considering it more often: over 200 cases in 2025, up from 122 in 2024. The rising tide of abusive complaints is a documented global phenomenon. India's legislative vacuum means that Indian complainants can participate in this abusive conduct with impunity, and Indian domain name holders who are targeted have no domestic shield.

C. Comparative Models That India Can Adopt

The global legal architecture for reverse domain hijacking can be understood as a spectrum: a "floor" established by the UDRP, and a "ceiling" established by the most developed domestic statutory remedy, the US ACPA. India currently falls below the floor, because it has domesticated neither.

UDRP Rule 15(e): The Floor. Under Rule 1 of the UDRP Rules, reverse domain hijacking is defined as "using the Policy in bad faith to attempt to deprive a registered domain-name holder of a domain name."[43] Rule 15(e) permits a panel to declare that a complaint was brought in bad faith. But as the *Innoviti* case demonstrates, the panel's only sanction is that declaratory finding – no costs, no damages, no consequences beyond the four corners of the decision. The UDRP floor is a statement, not a remedy. India currently does not even reach this floor, because no domestic statute gives legal effect to a WIPO RDNH finding.

The infrequency of Rule 15(e) findings is itself revealing. Commentators tracking WIPO and Forum decisions have noted that, since the UDRP's introduction in 1999, only around 500 complainants have been found guilty of reverse domain hijacking out of more than 80,000 complaints filed —a vanishingly small fraction, even accounting for the genuine rarity of bad-faith complaints. The reason is structural, not merely behavioural: a panel deciding Rule 15(e) is deciding the merits and the question of the complainant's subjective bad faith in the same proceeding, on the same paper record, usually without live testimony—and panels willing to dismiss a complaint on the merits are frequently unwilling to take the further step of branding the complainant's conduct as bad faith, particularly where the record is genuinely close. Even where a panel does make the finding, as Innoviti illustrates, it has no tool to attach a

[42]UDRP.tools, *RDNH Statistics 2022–2025*, https://udrp.tools (last visited May 31, 2026).

[43]UDRP Rules r. 1. *See supra* note 38.

consequence to it beyond the label itself. The floor is not merely thin by design; it is thin by the practical mechanics of how the finding gets made at all.

The US ACPA: The Ceiling. The US ACPA provides the statutory counter-remedy that India lacks, though not through the provision often assumed. Under 15 U.S.C. § 1114(2)(D)(v), a domain name registrant whose domain has been suspended, disabled, or transferred under a registrar's dispute policy may sue for a declaration that the registration is lawful and for injunctive relief, including reactivation or transfer of the domain back to the registrant—the First Circuit confirmed in Sallen v. Corinthians Licenciamentos Ltda., 273 F.3d 14 (1st Cir. 2001), that federal courts have jurisdiction to hear such a claim even where the registrant has already lost the underlying UDRP proceeding. Fees follow separately, through the Lanham Act's general fee-shifting provision, 15 U.S.C. § 1117(a), which allows a court to award reasonable attorney's fees to the prevailing party in "exceptional" cases—a discretionary standard, not an automatic entitlement. The mechanism has already produced a real-world mirror to the cases catalogued in Section A above. In Domond & Hunter v. PeopleNetwork ApS, No. 16-24026-civ (S.D. Fla. Nov. 9, 2017), a UDRP panel had already found the complainants guilty of reverse domain hijacking after they tried to seize a domain held by the registrant since before the complainants' own trademark existed. The complainants sued anyway in federal court; the court dismissed the case and ordered them to pay the registrant's attorney's fees, treating a complainant's decision to re-litigate a claim a panel had already condemned as bad faith as exactly the kind of conduct § 1117(a) exists to penalise. The lesson for India is not the specific dollar figure recovered, but the structure: a prior adjudicated finding of bad faith converts what would otherwise be ordinary litigation risk into a fee-shifting trigger. The deterrence runs in both directions, which is precisely the mirror-failure thesis in statutory form.

D. Recommendation: Completing the Proposed Cybersquatting Prohibition Act

The three cybersquatting gaps in Part II identified the need for a standalone Cybersquatting Prohibition Act. That Act must include a dedicated chapter on reverse domain hijacking to make the framework bidirectional.

Before turning to those provisions, one objection must be confronted directly: will mandatory cost-shifting and a statutory penalty chill legitimate complainants who lose a close case in good faith? The risk is real, and the proposed framework is structured specifically to avoid it. Three safeguards do the work. First, the rebuttable presumption is triggered only by a formal finding

of reverse domain hijacking by a WIPO panel or INDRP expert—not by losing the dispute. As the cases in Section A show, panels reserve that finding for complaints involving false statements, ignored prior rulings, or claims a represented party should have known were hopeless; a complainant who simply makes a reasonable but unsuccessful argument is never at risk, because no panel makes an RDNH finding against them in the first place. Second, the statutory definition itself requires bad faith and knowledge that the complaint lacks merit, mirroring the subjective element the US ACPA builds into its own complainant-liability provisions, so a complainant who merely misjudges the strength of its case falls outside the Act entirely. Third, the statutory penalty is calibrated deliberately at the floor—at least ₹1 lakh—rather than a punitive multiplier, so the consequence is meaningful without being crushing for a mid-sized business that brought a close case honestly. The object of these provisions is not to punish losing; it is to make complainants who have already been found to have abused the process bear the costs of that abuse, while leaving good-faith litigation exactly as unconstrained as it is today. Three specific provisions are necessary.

a) **Statutory Recognition of RDNH as a Civil Wrong.** The Act should define reverse domain hijacking as "the use of the UDRP, INDRP, or any court proceeding in bad faith, with knowledge that the complaint lacks merit, to deprive a legitimate domain name holder of their domain name." This would create a statutory cause of action for respondents who successfully defend abusive complaints.

b) **Mandatory Cost-Shifting and Statutory Penalty.** The Act should establish a rebuttable presumption that where a WIPO panel or INDRP expert has made a finding of reverse domain hijacking, the complainant shall pay the respondent's full legal costs (on an indemnity basis), plus a statutory penalty of at least ₹1 lakh. This mandatory provision would create a genuine economic deterrent – an abusive complainant would face not only its own costs but also the respondent's defence costs and a statutory penalty. Where RDNH is established in court proceedings rather than UDRP or INDRP proceedings, the court shall have equivalent power to award costs on an indemnity basis and impose a statutory penalty under this Act.

c) **Public Register of RDNH Findings.** NIXI should be required to maintain a public, searchable register of all RDNH findings made against Indian complainants in UDRP proceedings, and all INDRP expert findings of RDNH. The register should include the complainant's name, the domain name at issue, the panel's decision summary, and any

costs ordered. This would create a reputational deterrent; a corporate group or law firm found to have engaged in reverse domain hijacking would face public accountability.

This proposed register is certainly not something new in the regulatory practice of India, as there is a clear domestic precedent in the form of the Reserve Bank of India's treatment of wilful defaulters. According to the RBI (Treatment of Wilful Defaulters and Large Defaulters) Directions, 2024, the borrower can be put in this register following a specific process of identification through a committee, issuing a show-cause notice, giving a response, and further considering it in another committee. The RBI experience demonstrates both that a public register can function as a genuine deterrent within Indian administrative law and where such schemes go wrong: commentators have repeatedly flagged the absence of any clear procedure for removing a name from the list once a classification is reversed or settled, leaving cleared parties with no defined route to correction. NIXI's RDNH register should close this gap rather than inherit it. Because listing follows from a WIPO panel or INDRP expert's finding—itself already an adjudicated determination, unlike RBI's internal committee process—the Act should additionally require NIXI to remove or annotate an entry within a fixed period if the underlying finding is set aside on appeal or in subsequent court proceedings. A deterrent that cannot be corrected is not transparency; it is a permanent record with no error-correction mechanism, and the register proposed here should not repeat that flaw.

Together, these three provisions complete the mirror that Part II began. Just as a standalone Act, statutory damages, and in rem jurisdiction answer cybersquatting's three gaps, statutory recognition, mandatory cost-shifting, and a public register answer reverse domain hijacking's three gaps—a deliberately symmetrical structure, because the underlying legislative failure is itself symmetrical. Neither half of this framework is optional: a statute that disciplines registrants without disciplining complainants would simply relocate the abuse from one side of the UDRP to the other.

VI. SYNTHESIS

The gaps examined in this article, the absence of a standalone cybersquatting act, the absence of statutory damages and civil deterrence, the absence of *in rem* jurisdiction, and the complete statutory silence on reverse domain hijacking, are not independent failures. They are expressions of a single legislative choice: India has never enacted a comprehensive domain name law. Every gap identified, on both sides of the enforcement vacuum, would be resolved

by a single statutory intervention — a Cybersquatting Prohibition Act that defines the wrong, provides civil and criminal remedies, confers procedural jurisdiction, and protects legitimate registrants from abusive complainants.

This symmetry is not merely rhetorical. It reveals that India's enforcement vacuum is not two separate problems—cybersquatting and RDNH—but a single structural failure: the absence of a statutory framework that regulates both sides of the domain-name dispute ecosystem. The three gaps identified in Part II—no standalone act, no statutory damages, no in rem jurisdiction—are not just gaps that hurt trademark owners; they are gaps that, in their very structure, create reciprocal vulnerabilities. A standalone act would define the wrongs on both sides. Statutory damages would deter bad-faith registrants, while a cost-shifting provision would deter bad-faith complainants. In rem jurisdiction would allow courts to reach anonymous squatters, while a public register of RDNH findings would create reputational accountability for known complainants. The legislative silence is singular; the harms are bidirectional. To address only cybersquatting would be to complete only half the mirror, leaving legitimate domain name holders exposed to a different but equally damaging form of abuse.

That correspondence is not loose. The absence of a standalone act is answered by the Act's threshold definitions, which finally give cybersquatting and reverse domain hijacking an existence in Indian law independent of trademark doctrine borrowed for purposes it was never designed to serve. The absence of statutory damages and civil deterrence is answered by fixed-sum remedies running in both directions: statutory damages for registrants modelled on the ACPA, and the mandatory cost-shifting and statutory penalty for complainants proposed in Part III. The absence of in rem jurisdiction is answered by the Act's procedural innovations—a statutory in rem remedy for gTLDs and a NIXI-administered mechanism for .in domains—closing an anonymity gap that John Doe orders and case-by-case judicial improvisation can only ever address one defendant at a time. And the complete statutory silence on reverse domain hijacking is answered by extending that same protective logic to the other side of the docket: a respondent who defeats an abusive complaint should have the same statutory standing as a trademark owner who defeats a cybersquatter, and currently has none. The Delhi High Court's e-KYC mandate in Dabur shows both how far judicial development can reach and exactly where it stops: it can compel registrars to verify identity, but it cannot award a rupee in damages, cannot bind a registrar with no presence in India, and says nothing whatsoever about a complainant who abuses the very disclosure the order makes possible. A court can resolve one dispute. Only a statute can resolve the structure that produces the dispute.

The judicial development that has sustained India's domain name jurisprudence for twenty-five years has reached its limit. The remaining work is Parliament's.

VII. CONCLUSION

India's domain name framework is not merely incomplete; it is incoherent. It recognises domain names as protectable business identifiers but provides no effective remedy when they are registered. It offers a cheap administrative process for transferring domains, but no financial deterrent against abusing that process. It enables courts to find cybersquatting in one case and reverse domain hijacking in another, but it attaches legal consequences to neither. This bidirectional enforcement vacuum is the product of a single failure: the absence of a standalone cybersquatting statute.

This article has proposed a Cybersquatting Prohibition Act that closes all identified gaps. From the United States, it borrows statutory damages, *in rem* jurisdiction, and a reverse-hijacking counter-remedy. From the Philippines, it draws the principle of criminal deterrence for aggravated bad faith (filtered through a prior judicial finding of wilful intent, avoiding blanket criminalisation), while India's own Jan Vishwas framework provides the graded "inform correct-penalise" structure that reserves criminal sanctions for repeat or fraudulent conduct. From South Korea, it borrows an integrated dual-track administrative framework. And from the Delhi High Court's e-KYC mandate, it codifies judicial innovation into lasting statutory law. The enforcement vacuum would be closed in both directions.

India's internet economy will continue to expand. Its legal framework must expand with it, not through judicial improvisation, not through borrowed trademark doctrines, but through a comprehensive, bidirectional, and democratically legitimate cybersquatting statute. The courts have done their work. It is now for Parliament to act.