The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

DOMAIN NAME FRAUD AND TRADEMARK PROTECTION IN THE DIGITAL AGE: A CASE COMMENTARY ON DABUR INDIA LIMITED V. ASHOK KUMAR & ORS. (2025)

~Aviral Goyal

ABSTRACT

This case commentary examines the Delhi High Court's judgment in Dabur India Limited v. Ashok Kumar & Ors., a 248-page framework decision addressing large-scale domain name fraud and trademark impersonation. It traces the judgment's procedural evolution from an ex parte injunction into a consolidated proceeding governing registrar obligations, examines the registrars' doctrinal defenses under Section 79 of the Information Technology Act, 2000 and comparative authorities including Cartier International AG v. British Telecommunications Plc, and analyses the Court's central remedial innovation, the "Dynamic+" injunction, against its doctrinal lineage in UTV Software Communications Ltd. v. 1337X.To, Snapdeal Private Limited v. GoDaddy.com LLC & Ors., and Burger King Corporation v. Swapnil Patil & Ors. It concludes that while the judgment succeeds in mapping the accountability gaps across India's domain registration ecosystem, its practical force remains constrained by unresolved tensions with the Digital Personal Data Protection Act, 2023 and by the limits of Indian judicial jurisdiction over foreign-headquartered registrars.

INTRODUCTION

The Delhi High Court observed in the landmark judgement of *Dabur India Limited v. Ashok Kumar & Ors.* that in today's digital age, a domain name functions as the "Online Soul" of a business. This very framing explains why a suit which began as an ordinary cybersquatting dispute grew into a 248-page framework governing how the entire domain registration ecosystem must respond to trademark infringement.[1] Delivered by Justice Prathiba M. Singh on 24 December 2025, nearly four years after Dabur first approached the Court, the judgment treats large-scale misuse of well-known marks in domain names as a systemic form of cyber fraud which demands a coordinated regulatory intervention rather than simply a private dispute between two commercial parties. This reframing gives the decision its significance well beyond the facts of the case itself; not merely its outcome but the institutional machinery it had to assemble to get there: years of affidavits from banking regulators, telecom ministries, and the very registrars being regulated, folded into a record that reads less like a judgment and more like the minutes of a standing regulatory committee sitting inside a courtroom.

FACTS AND PROCEDURAL BACKGROUND

Dabur found that unknown registrants had begun operating websites under domain names such as daburdistributor.com and daburdistributorships.in, impersonating the company to solicit payments from members of the public seeking franchises, distributorships, or employment. On one such website, prospective franchises were asked to pay a registration fee of twenty-five thousand rupees before being told that no such position existed. The Court granted an ex parte John Doe injunction on 3 March 2022, and what followed was less a single litigation and more an evolving proceeding comprising further infringing domains, including daburfranchise.in, daburfranchise.com, and a typosquatted variant registered as dbraur.in, surfaced under new registrars over the following years, and additional defendants including GoDaddy, Hosting Concepts, Hostinger Operations, and Endurance Digital Domain Technology were progressively impleaded. The suit was heard alongside a growing batch of similar matters filed by other trademark owners; a consolidation the Court had already signaled was necessary in *Fashnear Technologies Private Limited v. Meesho Online Shopping Pvt. Ltd. & Anr.*[2] By the time judgment was reserved on 31 May 2025, the proceeding had absorbed years of affidavits from the Reserve Bank of India, the electronics and telecom ministries, ICANN, and numerous registrars, turning a single commercial suit into a comprehensive judicial audit of the domain registration system.

---

[1] *Dabur India Limited v. Ashok Kumar & Ors.*, CS (COMM) 135/2022, 2025:DHC:11862 (Del. H.C. Dec. 24, 2025) (Singh, J.).

[2] *Fashnear Technologies Private Limited v. Meesho Online Shopping Pvt. Ltd. & Anr.*, CS(Comm) 475/2022 (Del. H.C. order dated July 20, 2022).

THE QUESTIONS BEFORE THE COURT

The judgment organizes its reasoning around three primary questions that recur across the batch: what obligations a registrar owes once it becomes aware of an infringing registration, what measures a court may direct registrars and registry operators to implement going forward, and what consequences should follow when a registrar simply refuses to comply.[3] The third question is where the judgment does its most consequential work, since it required weighing the safe-harbour protection ordinarily available to intermediaries under Section 79 of the Information Technology Act, 2000 against the reality that several registrars, particularly those with no physical presence in India, had shown little inclination to give effect to prior orders at all.[4] It is worth pausing on why this third question needed a judgment of this length to answer. Domain name registration operates through a layered architecture, ICANN at the apex, Registry Operators beneath it, and DNRs closest to the registrant, and each layer had its own account of why responsibility lay elsewhere.

THE REGISTRARS' DEFENSE

The registrars did not simply resist compliance and mounted a considered doctrinal defense. GoDaddy's defense rested on a three-pronged argument. Firstly, that privacy-protect features are mandatory in response to the GDPR's default posture favoring data minimization rather than a discretionary courtesy. Secondly, drawing on the UK Supreme Court's reasoning in *Cartier International AG v. British Telecommunications Plc* that intermediaries complying with blocking injunctions are ordinarily entitled to indemnified costs, it was argued that compliance costs should fall on the trademark owner seeking relief rather than the registrar.[5] Lastly, that trademark rights are territorial and require case-by-case adjudication as illustrated by the American position in *Toyota Motor Sales, U.S.A., Inc. v. Tabari*, where nominative fair use permitted a reseller's use of a manufacturer's mark.[6] GoDaddy further relied on *Shreya Singhal v. Union of India* to argue that an intermediary's due diligence obligation is triggered only by an actual court order, not a mere complaint.[7]

---

[3] Code of Civil Procedure, No. 5 of 1908, § 20 (India); id. Order XXXIX, r. 1-2; The Trade Marks Act, No. 47 of 1999, §§ 28-29 (India).

[4] Information Technology Act, No. 21 of 2000, § 79 (India).

[5] *Cartier International AG v. British Telecommunications Plc,* [2018] UKSC 28.

[6] *Toyota Motor Sales, U.S.A., Inc. v. Tabari*, 610 F.3d 1171 (9th Cir. 2010).

[7] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

WHAT THE COURT ACTUALLY HELD

The Court recognized and affirmed DABUR's status as a well-known trademark built on more than a century of continuous use and drew a sharp line between mere consumer confusion and outright impersonation; holding that websites replicating Dabur's logos, product imagery, and trade dress to solicit payments were involved in an act of impersonating the company rather than simply infringing its marks. The judgment holds that safe-harbour protection is not absolute and can be forfeited where a registrar actively facilitates infringement or ignores judicial directions. The Court treats such persistent non-compliance as amounting to a threat to public order under Section 69A of the Information Technology Act, resulting in the opening of a door to a blocking action against the registrar's own services rather than merely the infringing domain.[8] This finding stands supported by a wide lattice of directions such as mandatory disclosure of registrant details within seventy-two hours, privacy-masking offered only as an opt-in add-on rather than a bundled default, permanent suspension and non-re-registration of identified domains, mandatory Grievance Officers for every registrar operating in India, and the Reserve Bank's beneficiary name look-up facility extended across RTGS and NEFT transfers so that a mismatch between a payee's registered name and the name shown at payment becomes visible before money changes hands.

FROM DYNAMIC TO DYNAMIC+: A DOCTRINAL EVOLUTION

The judgment's central remedial innovation cannot be understood in isolation as it is only the latest link in a chain of Delhi High Court decisions expanding the scope of dynamic injunction beyond its original piracy-website context. The concept was first developed in *UTV Software Communications Ltd. v. 1337X.To* & Ors. to let copyright owners extend an injunction to mirror and redirect websites without filing fresh suits.[9] In *Snapdeal Private Limited v. GoDaddy.com LLC & Ors.*, the Court had held such injunctions must attach to specific domain names rather than a word string, to avoid sweeping in unrelated, legitimate registrants.[10] *Burger King Corporation v. Swapnil Patil & Ors.* pushed the doctrine further by letting a Joint Registrar, rather than the Judge personally, examine newly identified infringing domains at the final relief stage.[11] What *Dabur* adds is the "Dynamic+" label and an explicit statement that the same logic

---

[8] Information Technology Act, No. 21 of 2000, § 69A (India).

[9] *UTV Software Communications Ltd. v. 1337X.To*, 2019 SCC OnLine Del 8002.

[10] *Snapdeal Private Limited v. GoDaddy.com LLC & Ors*., CS(Comm) 176/2021, I.A. 5407/2021 (Del. H.C. order dated Apr. 18, 2022).

[11] *Burger King Corporation v. Swapnil Patil & Ors.*, CS(Comm) 303/2022 (Del. H.C. order dated Dec. 4, 2023).

extends to alphanumeric and homoglyph variants, not merely mirrors of an already-identified domain, a widening the Court reaches almost in passing but that will likely be the paragraph most cited by future plaintiffs.

THE CRACKS BENEATH THE FRAMEWORK

For all its ambition, the judgment leaves at least three structural tensions only partially resolved. The first is the uneasy fit between its disclosure-forward posture and India's own Digital Personal Data Protection Act, 2023, which several registrars invoked, alongside the GDPR, to justify masking registrant data by default; the Court's answer, that privacy-protect features must become opt-in rather than automatic, is workable but does not fully reconcile a consent-based statute with a regime now expecting disclosure the moment a well-known mark is implicated.[12] The second, more stubborn problem is jurisdictional: ICANN declined to submit to the Court's jurisdiction and foreign-headquartered registrars treat Indian court orders as persuasive at best, meaning the most elaborate parts of the framework bind only registrars willing to appear in Delhi. A judgment this comprehensive is only as strong as its weakest complying registrar. The third tension is institutional: delegating the screening of newly identified infringing domains to a Joint Registrar quietly shifts a determination that used to require judicial reasoning onto an officer whose docket incentives favour speed over scrutiny, and the judgment says little about what standard that officer should apply.

CONCLUSION

What makes this case worth close study is not any single doctrinal move but the shift in judicial posture it represents, from courts responding to individual infringing domains one injunction at a time toward courts attempting to redesign the incentive structure of an entire digital ecosystem. The judgment succeeds, on its own terms, at mapping that ecosystem and identifying where the accountability gaps sit between registrants, registrars, registries, banks, and telecom intermediaries. Where it remains tentative is in actually closing those gaps for the registrars least inclined to cooperate. Whether the Dynamic+ framework, the KYC push, and the Grievance Officer mandate survive contact with registrars who simply decline to show up is a question this judgment cannot answer alone, and one that will define how much of it actually protects consumers rather than merely reading well in the law reports.

[12] The Digital Personal Data Protection Act, No. 22 of 2023 (India).