Topic: Domain Name Registrations, e-KYC Verfication, and Trademark Enforcement in India (Registrar Duties and Judicial Remedies)

Based on:

Dabur India Limited v. Ashok Kumar & Ors., CS(COMM) 135/2022

Delhi High Court | Justice Prathiba M. Singh

Decision dated 24 December 2025

Introduction

- Today, Domain names function not merely as technical internet addresses, but as commercial identifiers and primary access points through which consumers engage with businesses. Increasingly, fraudulent actors have been registering domain names incorporating well-known trademarks to impersonate legitimate businesses, solicit franchise fees, collect payments, and mislead consumers.

- The Court has taken note that Infringing domain names are being registered to impersonate the Plaintiffs and falsely offer jobs, dealerships, and franchise opportunities to collect money. Secondly, Infringing domain names are used to host websites offering counterfeit or passing-off products. Thirdly, fraudulent domain names are being used to host websites for providing services posing as the Plaintiffs.

- Prior to this judgment, domain name regulation in India largely operated on a reactive model. Trademark owners were required to identify infringing domains and seek injunction orders on a case-by-case basis. At the same time, Domain Name Registrars (DNRs) permitted registrations with minimal identity verification, and registrant details were often masked through privacy protection services, making enforcement difficult and allowing fraudulent activity to recur.

- Against this background, the Court was required to examine whether the existing domain registration framework sufficiently protected trademark proprietors and consumers, or whether systemic directions were necessary to impose stronger verification, disclosure, and accountability obligations upon Domain Name Registrars and Registry Operators.

Key Stakeholders

- **Domain Name Registrants** – Person registering the domain name
- **Domain Name Registrars (DNRs) -** Entity enabling the registraiton of the domain name
- **Domain Name Registry** – The Registry under which the DNR operates
- **ICANN** – Internet Corporation on Assigned Names and Numbers, the overall regulator of the Internet
- **Banks** – where the bank accounts are opened by infringers
- **Reserve Bank of India** – Banking regulator which had to take steps to curb fraudulent activities through banking channels
- **Telecom Service Providers** – companies which provide SIM cards and associated telecom services
- **Ministry of Electronics and Information Technology (MeitY) and Department of Telecommunications (DoT)** – Ministries which oversee the access to the internet in India and also regulate the internet/telecom service providers
- **Law Enforcement Agencies** – Police and other investigating agencies

Factual Background & Common Issues before the Court

- The present suit was part of a batch of matters relating to domain names being registered by unknown third parties infringing trademark rights of various brand owners and implementation of Court orders by different concerned entities including the Domain Name Registrars.

- The Plaintiff, Dabur India Limited, discovered multiple domain names such as, *www.daburdistributorships.in* and *https://daburdistributor.com/*, incorporating its registered trademark "DABUR", used to host fraudulent websites. These sites were designed to impersonate the Plaintiff and falsely represented themselves as official platforms of the company. Through these websites, members of the public were offered distributorships, franchises, and other business opportunities purportedly on behalf of the Plaintiff. Dabur filed a suit seeking permanent injunction, restraining use of its trademark, suspension and blocking of the domain names, disclosure of complete registrant details, freezing of associated bank accounts, including damages.

- Upon conducting investigations, it was revealed that:

  - Registrant details were masked through privacy services
  - Contact details provided at the time of registration were false or unverifiable
  - Upon suspension or blocking of one domain, mirror domains emerged
  - Fraudulent operators remained untraceable

Key Issues

- **Issue I** – What are the obligations and liabilities of a DNRs and whether the same are sufficient for protecting the Intellectual Property Rights of third parties?
- **Issue II** - What measures may be directed by the Court to be implemented by the DNRs and Registry Operators to safeguard the Trademark rights of the plaintiffs?
- **Issue III** - What measures may be directed by the Court against DNRs who refuse to comply with the Court orders?

Relevant Legal Provisions & Framework

The Court analyzed the interplay of multiple statutes:

1. Trade Marks Act, 1999

Section 29 – Infringement of registered trademark

Passing off principles

Protection of well-known marks

2. Information Technology Act, 2000

Section 79 (2)(c) – Safe harbour for intermediaries

Section 69A – Blocking powers

Rule 3(1)(b)(iv), Intermediary Guidelines & Digital Media Ethics Code Rules, 2021

3. The Digital Personal Data Protection (DPDP) Act, 2023

Section 4 - Grounds for processing personal data

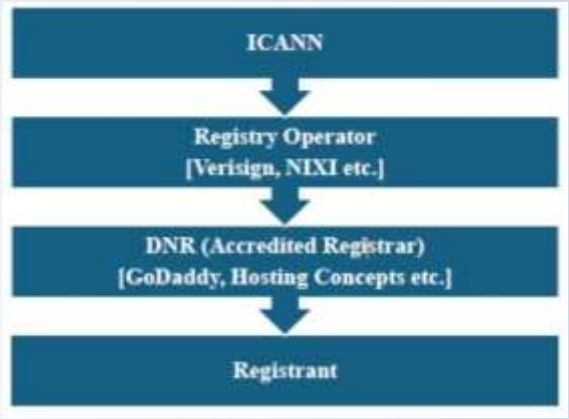
Section 7 - Certain legitimate uses.

4. Contractual Domain Registration Framework

Registrar Accreditation Agreements , ICANN policies & WHOIS data obligations

How DNRs Dealt with Fraud & Trademark Abuse Before This Judgment

- Before this decision, DNRs largely adopted a **notice-and-takedown model:**
  - Registration based on self-declared information
  - No mandatory Aadhaar-based or equivalent e-KYC
  - Privacy masking services enabled by default
  - Action taken only after receipt of court orders
  - Registrars treated themselves as neutral technical intermediaries



- The framework was compliance-driven rather than verification-driven. Registrars would suspend or block domains only upon court direction, but did not proactively verify identity or prevent repeat abuse.
- The system placed the burden on trademark owners to continuously monitor and litigate.
- *"195. However, in the experience of the Court in adjudicating these matters as also in view of the provisions under the NIXI Accreditation Agreement,* ***either the Registry Operators and DNRs are not complying the abovementioned obligations or the same are not sufficient to safeguard the rights of trademark owners in India. These measures in the opinion of this Court appear to have fallen short, by significant degree, since not only do they permit unscrupulous Registrants continue to infringe the rights of various trademark owners, but also defrauding of numerous innocent persons****, by taking shelter under the Privacy policies of the DNRs which mask the Registrant's details." (emphasis supplied)*

Systemic Issues Resulting from DNR Modus Operandi

The Court identified serious systemic deficiencies:

1. **Anonymity as a Shield for Fraud**

   Default privacy masking enabled bad actors to evade detection.
2. **Whack-a-Mole Phenomenon**

   After blocking one domain, identical variations reappeared.
3. **Absence of Real-Time Identity Verification**

   Registrations could be made using disposable emails and unverifiable data.
4. **Ineffective Deterrence**

   Fraudsters faced minimal risk due to lack of traceability.
5. **Consumer Harm**

   Large-scale financial fraud occurred under the guise of trademark legitimacy.

Directions to Domain Name Registrars (DNRs) and Registry Operators (e.g., .IN Registry / NIXI)

- *"The DNRs and Registry Operators shall,* ***henceforth, not resort to masking of details of the registrants, administrative contact and technical contact on a default basis as an 'opt-out' system****. At the time of registration of the domain names, a specific option shall be provided for the Registrant and it is only if the said Registrant chooses for privacy protection, that the said service shall be offered as a value added service upon payment of additional charges. The additional charges shall not be made a part of the default package for registration of domain names.*

- *Whenever* ***any entity or individual having legitimate interest****, law enforcement agencies (LEAs) or the Courts, request for disclosure of data relating to any infringing or unlawful domain name, the following data shall be disclosed by the concerned DNR as soon as possible but not later than 72 hours in terms of the Intermediaries Guidelines 2021:*

  (a) Name of the Registrant;

  (b) Administrative contact;

  (c) Technical contact;

  (d) Addresses of the above mentioned persons/entities;

  (e) Mobile numbers of the above mentioned persons/entities;

  (f) Email address of the above mentioned persons/entities;

  (g) Any payment related information such as details of credit card, debit card, UPI number, payment platform identities, bank account details, etc., which may be available with the DNR;

  (h) Details of any value added services such as hosting of website, brokerage, or any other services offered by the DNR or by Registry concerned." ***(emphasis supplied)***

Directions to Domain Name Registrars (DNRs) and Registry Operators (e.g., .IN Registry / NIXI) (Contd.)

- *"If any particular domain name is restrained by an order of injunction or has been found to be used for illegitimate and unlawful purposes, the said domain name shall remain permanently blocked and* ***shall not be put in a common pool in order to disable re-registration of the same very domain name by other DNRs****. The appropriate steps in this regard shall be taken by the concerned Registry Operator to ensure that all DNRs having an agreement uniformly give effect to the said direction.*
- ***In the case of trademarks/brands, which are well-known or are invented, arbitrary or fanciful marks****, which have attained reputation/goodwill in India,* ***if a Court of Law directs that there would be an injunction on making available the infringing domain name with different extensions or mirror/redirect/alphanumeric variations, the same shall be given effect to by the DNRs*** *and no alternate domain name shall be made available in respect of such brands and marks.*
- ***Upon an injunction being issued by the Court*** *in respect of any domain name and the same being communicated to the DNRs,* ***the DNRs shall ensure that no alternative domain name is promoted or being suggested to a prospective Registrant. Any promotion of alternative domain names of an injuncted domain name would disentitle the concerned DNR for safe harbour protection*** *under Section 79 of the IT Act.*
- ***In respect of descriptive and generic marks, the restraining/injunction orders would be qua the specific domain name*** *and any extension of restraining/injunction order for other infringing domain names would be with the intervention of the Joint Registrar before whom the application under Order I Rule 10 of Code of Civil Procedure, 1908 along with affidavit shall be filed and the injunction would be extended. Where any party is aggrieved by the order of the Joint Registrar, the application may be moved or placed before the ld. Single Judge.*
- *Upon orders being passed by a Court, the infringing domain name shall be transferred to the Plaintiff/trademark owner/brand owner, upon payment of usual charges."* ***(emphasis supplied)***

Directions to Domain Name Registrars (DNRs) and Registry Operators (e.g., .IN Registry / NIXI) (Contd.)

- *"Search engines and DNRs shall not provide any promotion or marketing or optimization services to infringing and unlawful domain names.*
- ***All DNRs offering services in India shall appoint Grievance Officers** within a period of one month from today failing which they would be held as non-compliant DNRs.*
- ***Service by email to the respective Grievance Officer's details would be henceforth sufficient service** for Court orders and any DNRs who insist upon services through MLAT or through other modes of services shall be held to be non-compliant DNRs.*
- *In appropriate cases **where an entity has repeatedly not complied with orders of the Court, and in the opinion of the Court it is a case where the interest of society at large is being adversely affected, such as cases of frauds, the Court may direct the appropriate authority to block access to the said entity under Section 69A of the Information Technology Act, 2000** read with Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.*
- *All Registry Operators having valid agreements with ICANN shall take appropriate steps to **implement the Trademark Clearing House services** and make the same available to all brand owners & registered proprietors of trade marks.*
- *All DNRs offering services in India or to customers in India **shall undertake verification of Registrant's details at the time of registration and periodic verification of the same.***
- *All DNRs who are enabling registration of domain names which are administered by NIXI as a Registry Operator shall comply and provide requisite registration data to NIXI within one month of this judgment and also update the same on a monthly basis."* ***(emphasis supplied)***

Directions to Government Authorities

- *"The following directions are issued to MeitY, MHA and other relevant Government authorities:(a)**The Government shall hold a stake holder consultation with all DNRs and Registry Operators offering services in India and explore the possibility of putting in place a framework similar to the one used by NIXI by all DNRs** for the purpose of domain name registration.*
- *(b)**Consider nomination of a nodal agency such as NIXI as the data repository agency for India** with which all the Registry Operators and the DNRs would maintain details related to Registrants on a periodic basis so that the said details are made available to the Courts, LEAs and the governmental authorities for the purpose of enforcement of orders of Courts and for preventing misuse. Alternatively, **DNRs shall be directed to localize the data in India for easy access**. Irrespective of the decision, it is made clear that processing of personal information would be strictly in terms of the DPDP Act and applicable Rules.*
- *(c) In case of a DNR or Registry Operator, which does not comply with the orders of the Courts or with request from LEAs, **the offering of services of such DNRs or Registry Operator be blocked by MeitY and DoT** under Section 69A of the Information Technology Act, 2000 read with Information Technology (Procedure and Safeguard for Blocking for Access of Information by Public) Rules, 2009.*
- *(d) **MeitY along with NIXI shall coordinate with ICANN to enable brand owners in India to avail of TMCH facilities** on reasonable terms and conditions so that they can receive notifications whenever any conflicting /infringing domain names are proposed to be registered by any third parties across the globe.*
- ***The CGPDTM could also consider publishing the list of well-known marks along with the official and authentic website details of the trademark owners** so that if any consumer or user wishes to verify the authentic website, the same would be made possible through the website of the Intellectual Property Office. The same shall also act as sufficient notice to all potential Registrants as to the actual websites"**(emphasis supplied)***

Directions to Banks

- *"159. One of the major causes of amounts being transferred in favour of such infringers was also because the innocent persons who were making payments did not realise that they were not making payments to the actual brand owners or business owners such as Colgate or to Dabur but in fact to some unconnected individuals.* ***In order to plug this clear loophole that existed in NEFT and RTGS transactions, notice was also issued to the NPCI. After several orders been passed from time to time, the RBI introduced the 'Beneficiary Bank Account Name Lookup' facility for RTGS and NEFT system****, on 30th December, 2024..."* ***(emphasis supplied)***
- *"160.* ***Banks were also directed through the IBA and the Central Economic Intelligence Bureau (hereinafter "CEIB") to share information with LEAs****. A direction was given on 15th April, 2024 for finalisation of a Standard of Procedure (hereinafter "the SOP") for sharing of information by banks with LEAs. The said SOP was finalised and was issued on 31st May, 2024."* ***(emphasis supplied)***
- *"162. In terms of the affidavit of the IBA extracted above, all banks are required to adhere to the SOP and to the RBI's circular on beneficiary name lookup facility. Insofar as digital payments through UPI and other payment apps are concerned, the recipient's name becomes visible when such a payment is made. However, the infringing websites were taking advantage of the non-visibility of the recipient's name while making payments through RTGS and NEFT, which now is a loophole that has been fully plugged with the introduction of the RBI's circular dated 30th December, 2024."*

Dynamic and Dynamic+ Injunctions

- *"251.* ***A perusal of the infringing domain names would show that the DNRs are permitting registration of well-known marks, famous marks, global brands, names of corporate house names to be registered, thereby, resulting in misuse. It is a matter of fact that the same rule cannot be applied for all categories of marks. The relief, therefore, would have to be moulded depending upon the nature and character of the mark.". (emphasis supplied)***

- *"253. In the opinion of this Court, the broader enforcement of law needs to be given primacy in these cases where there is apparent illegality in registration of the domain names which consists of well-known trademarks or brand names. Infringing domain names deserve to be restrained. Insofar as future registrations are concerned, well-known trademarks deserve to be protected. For the said purpose, DNRs can be directed to access the list of well-known trademarks from Controller General of Patents, Designs and Trade Marks (hereinafter "CGPDTM") office and add the said marks into a blocking/Reserved list. Technological solutions would have to be given effect to by DNRs to ensure that the relief is effective. In the opinion of this Court, the broader enforcement of law needs to be given primacy in these cases where there is apparent illegality in registration of the domain names which consists of well-known trademarks or brand names. Infringing domain names deserve to be restrained.* ***Insofar as future registrations are concerned, well-known trademarks deserve to be protected.*** *For the said purpose, DNRs can be directed to access the list of well-known trademarks from Controller General of Patents, Designs and Trade Marks (hereinafter "CGPDTM") office and add the said marks into a blocking/Reserved list. Technological solutions would have to be given effect to by DNRs to ensure that the relief is effective"* ***(emphasis supplied)***

- *"275. C (xvii) The dynamic + injunction would apply under the following circumstances: (i) Wherever the brand/trademark appears as it is in the domain name; (ii)Wherever brand/trademark appears with a prefix or suffix which could lead to confusion; (iii)Wherever the brand/trademark appears as an alphanumeric variation."*

Broader Implications on Intermediary Liability & Safe harbor provision

- *"241. Thus,* ***it is settled that the non-implementation of steps to prevent trademark infringement coupled with various means and methods adopted by the DNRs to maximize their revenues would actually lead to non-grant of safe harbour protection in respect of the said DNRs.*** *Further, as is clear from the screenshots extracted hereinabove, the DNRs continue to promote alternative infringing domain names, several of which are clearly prima facie infringing the trademarks of the Plaintiffs. In such a situation, not only shall the concerned DNRs lose the safe harbour protection, the said DNRs would be liable to be treated as infringers against whom reliefs would be liable to be claimed. Accordingly, such DNRs in an appropriate case could be held to be liable to pay monetary damages as well." ."* ***(emphasis supplied)***

- *"244. Given that such frauds are increasing in number day by day, it is now more than ever necessary to build and maintain trust in the manner in which consumers interact and connect with brands and companies. If the consumer cannot trust the authenticity of the website or domain name she/he has accessed, which would be a logical consequence of the large scale frauds brought to the attention of the Court in the present batch of suits, then it would definitely disturb the economic interests of the businesses and also create disturbance to members of the general public and society. Therefore,* ***in the opinion of the Court, in light of the large scale frauds which are being committed, directions of the Court cannot be rendered ineffective by non-compliant DNRs and Registry Operators, for which the Court may direct the competent authorities to block the services of the non-compliant DNRs itself in order to ensure compliance****.". **(emphasis supplied)***

- *"245.* ***In the opinion of the Court, each of the above factors would squarely apply in respect of DNRs and Registry Operators, who not only provide services in India but are involved in generating significant revenues from numerous customers in India.*** *Thus, applying the same factors, it is clear that even in respect of the ICANN Agreements, Indian Courts would be courts of competent jurisdiction to issue directions to DNRs and Registry Operators for grant of appropriate relief."* ***(emphasis supplied)***

Constitutional & Privacy Considerations

- *"190. Thus, it is the settled position that **disclosure of personal information would have to satisfy the three-fold test** i.e., (i) the disclosure must be made in terms of a law justifying the encroachment of privacy, (ii) the said law must be pursuant to a legitimate aim of the State; (iii) means for disclosure are proportional to the legitimate aim sought to be achieved." ."**(emphasis supplied)***
- *"191. Indian laws i.e., the DPDP Act along with the DPDP Rules, 2023, notified on 14th November, 2025, satisfy the first requirement of the existence of law regulating disclosure of personal information. Under Section 4 of the DPDP Act **processing of personal information may only happen where either the data fiduciary has given her consent or for certain legitimate uses provided under Section 7 of the said Act."** ."**(emphasis supplied)***
- *"192. Thus, as per the above **a DNR will have to disclose the details of the Registrant of an infringing domain name upon a direction in this regard being issued by the Indian Courts**. It is also relevant to note that ICANN in fact has contemplated the possibility of different national laws preventing the DNRs or Registry Operators from complying with the provisions of the agreements with ICANN."**(emphasis supplied)***

Conclusion

- In its recent series of decisions addressing domain-name misuse and online fraud, the Delhi High Court has enacted a far-reaching recalibration of how domain registrations are regulated in India. On one hand, the **Court's directions respond to the very real problem of deceptive and infringing domain names being used to perpetrate large-scale fraud**, and they establish comprehensive systemic measures - including mandatory e-KYC verification, real-time injunctions, enhanced compliance obligations on domain name registrars and registry operators, and coordinated action involving banks, government authorities and law enforcement designed to strengthen digital commerce, protect trademarks, and enhance consumer trust.
- On the other hand, questions are being raised regarding the imposition of **ex ante regulatory burdens**, such as reversing default privacy protections, sanctioning permanent blocking of domains or loss of intermediary safe harbour, treating similarity at the point of registration as presumptively infringing, Shift from Adjudication to Regulation (Separation of Powers Concerns), and Data Protection and Privacy Implications.
- Taken together, **the ruling marks a watershed moment in India's digital ecosystem**: it underscores the judiciary's willingness to confront online fraud and compel systemic reform, even as it prompts important questions about proportionality, intermediary governance, and the boundaries of judicial regulation in a rapidly evolving technological landscape.

THANK YOU!

Questions?

Bhavya & Manish Kumar
Associate

Disclaimer: Views, opinions, and interpretations are solely those of the presenters, not of the firm (ALG India Law Offices LLP) nor reflective thereof.

This presentation hosted at: https://www.algindia.com/wp-content/uploads/2026/02/FINAL_SLIS-GIP_Bhavya-Manish_February-17-2026_-2.pdf