Introduction

In the digital age, legal disputes are no longer confined by geographical boundaries. With the rise of online businesses, social media, and global technology platforms, courts worldwide are confronted with the challenge of determining personal jurisdiction in cyberspace—that is, deciding whether a court has the authority to hear a case involving parties located in different regions or countries.

In India, the concept of jurisdiction has expanded significantly due to online interactions, trademark infringements over the internet, and data-related disputes. This article simplifies key Indian and international cases that have shaped the understanding of personal jurisdiction, intermediary liability, and digital rights, providing a clear, SEO-friendly summary for law students, practitioners, and researchers.

I. Indian Case Laws on Personal Jurisdiction in Cyberspace

1. Banyan Tree Holdings (P) Ltd. v. Murali Krishna Reddy (2008) 38 PTC 288 (Del)

Background:

The plaintiff, “Banyan Tree Holdings” , a Singapore-based hospitality and spa company using the mark "Banyan Tree" since 1994, operated websites accessible globally, including in India. They had a reputation in India through partnerships. The plaintiff alleged that the defendant in Andhra Pradesh had launched a real estate project titled “Banyan Tree Retreat,” infringing upon its unregistered trademark. The defendant advertised the project through a website accessible across India. The plaintiff filed the suit in the Delhi High Court.

Core Legal Issue:

Whether a court could assume jurisdiction when neither party resided nor conducted business within its territorial limits, merely based on the accessibility of a website in that jurisdiction.

Court's Analysis and Ruling:

The Delhi High Court emphasized that mere website accessibility does not automatically confer jurisdiction. Instead, the defendant must have "purposefully availed" itself of the forum's jurisdiction by targeting commercial transactions toward users in that region.

The court adopted a combination of the "purposeful availment" and "effects" tests . Further court also applies the "sliding scale test" (distinguishing between passive and interactive websites) and clarified that:

- This requires the defendant to have intentionally directed commercial activities towards residents of the forum state (Delhi), which must be more than incidental contact. The court differentiated between passive (information-only) and active (transactional) websites. Even with active sites, intent to target the forum state is needed, not just the technical possibility of interaction from anywhere.
- **Trap transactions** (test purchases) can be used as evidence but must be genuine.

Decision:

The court held that the defendant had targeted Indian users and purposefully availed itself of the jurisdiction, granting Delhi High Court authority to hear the case.

Significance:

This case established the **benchmark test for cyber jurisdiction** in India and remains one of the most cited decisions in Indian cyber law jurisprudence.

2. World Wrestling Foundation Inc. v. Reshma Collection (2014) 60 PTC 452 (Del)

Background:

The 2014 Delhi High Court Division Bench judgment in World Wrestling Foundation Inc. v. Reshma Collection significantly shaped the legal landscape for determining territorial jurisdiction in intellectual property (IP) disputes in the age of e-commerce.

Facts of the case

World Wrestling Entertainment, Inc. (WWE), an internationally renowned media and entertainment powerhouse incorporated in the United States, has a massive global following, including in India. They are famous for their wrestling events featuring

unique characters (like John Cena and The Undertaker), and they extensively license and sell branded merchandise such as T-shirts, caps, and DVDs. Their products are sold through various licensees in India and via their own interactive e-commerce websites (e.g., wweshop.com), which are accessible to Indian consumers, including those in Delhi.

The defendants were a Mumbai-based entity, Reshma Collection, found to be manufacturing and selling counterfeit garments and apparel bearing WWE's trademarks, logos, and images of their wrestling stars without authorization.

WWE filed a lawsuit in the Delhi High Court, but a single judge dismissed it due to a lack of territorial jurisdiction. The judge reasoned that WWE, being a foreign company without a physical office or exclusive agent in Delhi, did not "carry on business" there in the traditional sense required by IP laws.

The Appeal and the Core Issue:

WWE appealed, arguing their "virtual presence" and online sales to Delhi customers constituted "carrying on business" within the court's jurisdiction. The key legal question was how to interpret "carries on business" in the context of e-commerce.

Decision and Reasoning by the Court (Division Bench)

The Division Bench allowed the appeal, restoring the suit to the Delhi High Court. The court's reasoning adapted traditional legal principles to the digital age:

- **Broad Interpretation of "Carries on Business":** The court stated that the special jurisdictional provisions in IP laws (Section 134(2) of the Trade Marks Act and Section 62(2) of the Copyright Act) are wider than general rules and provide an additional forum for a plaintiff to file a suit where they operate their business, even without a physical presence.
- **E-commerce Transactions and Location:** Drawing an analogy to contracts made over the telephone, where a contract is concluded where the acceptance is received, the court viewed a website's display of goods as an "invitation to offer." The customer in Delhi makes the "offer" when ordering and paying, and the website accepts this offer, communicating it back to the customer in Delhi. Thus, an essential part of the business transaction occurs in Delhi.
- **Virtual Presence:** The court emphasized that technological advancements allow for a "virtual presence" in a distant location. The ability to conduct transactions through a website in a place is equivalent to having physical shops there.

Distinction from Banyan Tree Case:

Unlike Banyan Tree, which focused on a "part of cause of action" under CPC Section 20, WWF established jurisdiction based on the plaintiff's commercial presence through digital and physical means in Delhi.

Significance:

It expanded the understanding of online business jurisdiction, recognizing digital transactions and virtual presence as valid grounds for filing suits.

II. International Jurisdictional Developments

3. WhatsApp Inc. v. NSO Group Technologies Ltd. (2020) 472 F.Supp.3d 649 (U.S.)

The case of WhatsApp Inc. v. NSO Group Technologies Ltd. centered on a dispute between a major messaging platform and an Israeli firm selling surveillance software to governments, involving allegations of widespread, unauthorized hacking of user phones.

Facts of the Case

In 2019, WhatsApp Inc., a popular messaging platform owned by Meta (formerly known as Facebook), experienced a serious cybersecurity breach that exposed vulnerabilities in its system. WhatsApp is widely recognized for providing end-to-end encrypted communication, ensuring that only the sender and receiver can access messages, which makes it a trusted platform for secure and private conversations.

Between April and May 2019, NSO Group Technologies Ltd., an Israeli technology company best known for developing advanced surveillance tools like the "Pegasus" spyware, exploited a hidden flaw in WhatsApp's software. This flaw, known as a "zero-day vulnerability," was previously unknown to WhatsApp's developers and had no available patch or fix at the time. *(A **zero-day vulnerability** is a software flaw that is unknown to the software developer and has no official patch available at the time it is discovered and exploited by an attacker. The name comes from the fact that the developer has "zero days" to fix the issue before the attack occurs. within the WhatsApp application's code)*

Using this vulnerability, NSO Group was able to remotely install Pegasus spyware onto targeted devices. What made this attack particularly alarming was its simplicity—the installation could occur just by placing a voice or video call to the victim's phone. The user did not even need to answer the call for the infection to succeed. Once the spyware was installed, it allowed attackers to secretly access sensitive information, including messages, calls, contacts, and even the device's microphone and camera.

To make matters worse, in many instances, the call logs related to these attacks were automatically deleted from the victim's device, leaving almost no trace of the intrusion. This made it extremely difficult for users to detect that their phones had been compromised. The incident raised global concerns about digital privacy, government surveillance, and the security of encrypted communication platforms, prompting WhatsApp to take legal action against NSO Group for its role in the exploit.

The Scope of the Intrusion:

- WhatsApp alleged that NSO Group accessed approximately 1,400 target devices globally using this method. These targets included human rights activists, journalists, diplomats, and political dissidents in various countries.
- Once installed, the Pegasus spyware granted NSO's clients near-complete control over the device, allowing extraction of private messages, call recordings, emails, location data, and remote activation of the device's microphone and camera, entirely bypassing WhatsApp's security features.

The Legal Action and Defense:

- WhatsApp filed a lawsuit in a U.S. District Court, claiming violations of the federal Computer Fraud and Abuse Act (CFAA) and breach of contract (WhatsApp's Terms of Service).
- NSO Group sought to dismiss the case by arguing that they were merely a technology provider to "sovereign" government clients who were the actual perpetrators of the surveillance. They invoked the doctrine of Foreign Sovereign Immunity (FSIA), arguing that they should be immune from being sued in a U.S. court because their actions were conducted on behalf of foreign states.

Issues Involved :

- **Foreign Sovereign Immunity:** The primary legal issue was whether NSO Group, a private company, could claim *foreign sovereign immunity* because its clients were government entities.
- **Liability for Hacking:** The court had to determine if NSO Group's actions violated U.S. federal and state laws, specifically the Computer Fraud and Abuse Act (CFAA) and the California Comprehensive Computer Data Access and Fraud Act, which criminalize unauthorized access to computer systems.

Decision and Reasoning by the Court

In the 2020 decision, the U.S. District Court, presided over by Judge Phyllis Hamilton, issued a significant ruling that allowed the majority of WhatsApp's claims to move forward:

- **Rejection of Foreign Sovereign Immunity:** The court determined that NSO Group was a private company and not an arm of a foreign state, and thus could not claim sovereign immunity under the U.S. Foreign Sovereign Immunities Act (FSIA).
- **Direct Liability Established:** The court rejected NSO's defense that its clients were solely responsible. Evidence showed that NSO Group "retained some role" in the operation and deployment process, managing much of the technical aspects of the Pegasus system itself. The judge found NSO was directly liable for hacking WhatsApp's servers and breaching its terms of service.
- The actions violated the **Computer Fraud and Abuse Act (CFAA)** and **California's Data Access and Fraud Act**.

Significance:

This case reinforced that **cyber activities targeting U.S.-based infrastructure** are sufficient to establish jurisdiction, even if the actors are foreign entities. It highlights how **cyberspace jurisdiction transcends territorial borders.**

III. Competition and Privacy Jurisdiction in India

4. Competition Commission of India (CCI) Suo Moto Case No. 01 of 2021 – WhatsApp Privacy Policy

Overview of the Case

The *Competition Commission of India (CCI) Suo Moto Case No. 01 of 2021* centered on WhatsApp's controversial 2021 privacy policy update. The CCI initiated a suo moto investigation to determine whether the mandatory data-sharing terms introduced by WhatsApp and its parent company, Meta (formerly Facebook), amounted to an abuse of dominant position under section 4 of India's *Competition Act, 2002*.

Background and Core Issues

The 2021 Privacy Policy Update:

In January 2021, WhatsApp informed Indian users about a mandatory update to its privacy policy. Unlike the 2016 version, which had allowed users to "opt out" of sharing their data with Facebook for advertising purposes, the 2021 update offered no such option. Instead, it required users to accept the sharing of expanded user data (excluding message content, which remained encrypted) with other Meta companies to continue using the service.

Dominance in the Market:

The CCI identified WhatsApp as the dominant player in India's "over-the-top" (OTT) messaging app market, citing its massive user base and strong network effects that left users with limited alternatives.

Allegation of Abuse:

According to the CCI's *prima facie* assessment, the 2021 update represented an exploitative and exclusionary practice, thereby violating Section 4 of the *Competition Act, 2002*. The Commission expressed concern that Meta could leverage WhatsApp's vast user data to consolidate its market position in online display advertising, which could create barriers to entry for competitors in both messaging and advertising markets.

Investigation and Legal Proceedings

Acting *suo moto* (on its own motion), the CCI ordered an investigation into the matter and combined it with other pending complaints.

Challenges to Jurisdiction:

Meta and WhatsApp contested the CCI's jurisdiction in the Delhi High Court and later in the Supreme Court, arguing that the issue pertained to data privacy—an area outside the CCI's authority—and was already being reviewed in constitutional cases.

Court Decisions:

Both the Delhi High Court and the Supreme Court rejected these jurisdictional challenges. They clarified that while data privacy concerns fall under constitutional and regulatory domains, the CCI is empowered to examine the competition-related effects of such data practices under the *Competition Act, 2002*. The Supreme Court further directed that the investigation proceeds without delay.

Findings and Final Directions

CCI's Final Order (November 2024):

In its concluding order, the CCI imposed a penalty of INR 213.14 crore on Meta for abusing its dominant position. Additionally, the Commission directed Meta and WhatsApp to:

- Cease and desist from engaging in anti-competitive conduct.
- Halt data sharing with other Meta entities for advertising purposes for a period of five years.
- Ensure user transparency and choice by providing clear options for data sharing in contexts other than advertising, ensuring that use of WhatsApp's core service does not depend on accepting such data-sharing terms.

Current Appeal and Status

Meta has appealed the CCI's decision before the *National Company Law Appellate Tribunal (NCLAT)*. The NCLAT granted a partial stay on the order—suspending the monetary penalty (subject to a 50% deposit) and the five-year restriction on data sharing for advertising while the appeal is pending. However, the tribunal did not stay the directions requiring transparency and user choice concerning data sharing for non-advertising purposes.

Significance:

This case exemplifies how Indian authorities assert **extraterritorial jurisdiction** in the digital economy and demonstrates India's growing emphasis on **data protection and competition in the tech sector.**

IV. Intermediary Liability and Online Defamation

5. Google India Pvt. Ltd. v. Visaka Industries (2019 SCC OnLine SC 1587)

The 2019 Supreme Court judgment in *Google India Pvt. Ltd. v. Visaka Industries* dealt with Google's appeal to quash criminal defamation proceedings initiated against it. The key issue before the Court concerned whether Google, as an intermediary, could be held liable for defamatory third-party content posted on its platform. The Supreme Court emphasized that the events in question occurred before the 2009 amendment to the *Information Technology (IT) Act, 2000*. It clarified that, under the pre-amendment legal framework, intermediaries like Google could face liability if they failed to remove defamatory content after receiving proper notice.

Facts of the Case

Visaka Industries Limited, a manufacturer and seller of asbestos cement products, filed a criminal defamation complaint before a Secunderabad court. The complaint was directed against two defendants — (1) the individual coordinator of a Google Group titled *"Ban Asbestos India"* and (2) Google India Pvt. Ltd., which was the Indian subsidiary of Google Inc., the company hosting the online platform.

"Ban Asbestos India" was a public discussion forum hosted on *Google Groups*, a service provided by Google Inc./LLC. The group functioned as an online platform where activists, health professionals, and concerned citizens campaigned for a complete ban on the use and import of asbestos in India.

Allegations

In 2008, two posts appeared on the *"Ban Asbestos India"* Google Group that Visaka Industries claimed were defamatory. These posts allegedly linked Visaka Industries to corrupt practices and highlighted the alleged harmful and hazardous nature of asbestos. The company argued that the statements were false, damaging to its reputation, and constituted criminal defamation under Indian law.

Initial Actions Taken

Upon discovering the posts, Visaka Industries issued a legal notice to Google India Pvt. Ltd., demanding that the defamatory content be removed from the platform. Google India responded by forwarding the notice to its parent company, Google Inc., which managed the Google Groups service. However, Google requested Visaka Industries to provide specific

URLs of the offending content so that it could locate and remove the material. Visaka Industries, however, did not supply these details.

Procedural History

- **Filing of Complaint:** Visaka Industries filed a criminal defamation complaint before the Secunderabad magistrate against the Google Group coordinator and Google India Pvt. Ltd.
- **High Court Proceedings:** Google India filed a petition before the High Court seeking to quash the criminal proceedings, arguing that as an intermediary, it could not be held liable for third-party content hosted on its platform. The High Court dismissed the petition, allowing the case to proceed.
- **Supreme Court Appeal:** Google India subsequently appealed to the Supreme Court, reiterating its position that it was merely an intermediary and could not be held responsible for user-generated content under the *Information Technology Act, 2000*.

Issues involved

- **Intermediary Liability**: Could an intermediary like Google be held criminally liable for defamatory content posted by a third party on its platform?
- **The IT Act's "Safe Harbor":** Did Section 79 of the IT Act, as it existed before the 2009 amendment, protect intermediaries from liability under other laws, such as the Indian Penal Code (IPC)?
- **Timing of the Offence**: What was the relevant version of the law—the unamended law from 2008 when the articles were posted, or the amended version after October 2009?
- **Knowledge and Removal:** Was Google's failure to take down the content after receiving a takedown notice sufficient to attract criminal liability?

Decision and reasoning by the Court

- **Unamended vs. Amended Law**: The Supreme Court held that the law applicable was the one in effect at the time the defamatory content was published and the complaint was filed—specifically, the unamended Section 79 of the IT Act. The complaint was filed in early 2009, based on articles from 2008, both of which were before the 2009 amendment that introduced stronger "safe harbor" protections for intermediaries.
- **Limited Protection Before 2009**: The court clarified that the original Section 79 of the IT Act only provided protection from liability under the IT Act itself, not under other laws like the IPC. As such, Google could not claim blanket protection from criminal defamation proceedings under the IPC.

- **Matter for Trial**: The Supreme Court concluded that whether Google India could be considered a "publisher" in this context and whether it had sufficient knowledge to act were factual matters that needed to be decided by the trial court. This was not an appropriate case to be quashed under Section 482 of the Criminal Procedure Code.

The Supreme Court dismissed Google's petition to quash the proceedings, meaning

Significance of the Judgment

The ruling clarified the legal position on intermediary liability in India during the period prior to the 2009 amendment to the *IT Act, 2000*. It established that intermediaries could be held accountable for third-party content if they failed to act after being notified of its illegality.

This case marked an important precedent in defining the scope of intermediary responsibility in India's digital ecosystem and highlighted the evolution of the legal framework that now provides conditional immunity to online platforms under the amended *IT Act*.

V. Copyright and Digital Platforms

6. Super Cassettes Industries Ltd. (T-Series) v. MySpace Inc. (2011) 48 PTC 49 (Del); Reversed 2016 (236 DLT 478)

The case of **Super Cassettes Industries Ltd. (T-Series) v. MySpace Inc.** involved a critical legal battle in the Delhi High Court over the copyright liability of internet intermediaries for user-uploaded content. The case saw its initial 2011 single-judge ruling, which was later overturned by a landmark Division Bench decision in 2016.

Facts of the Case The Parties:

- **Plaintiff (T-Series/SCIL):** Super Cassettes Industries Ltd., one of India's largest music and film companies, holding vast copyrights to thousands of songs and films.
- **Defendant (MySpace):** MySpace Inc., a U.S.-based social networking and multimedia sharing platform where users could upload, share, and view content. MySpace generated revenue by placing advertisements alongside this user-generated content.

The Dispute:

In 2007, T-Series and MySpace had discussions regarding a potential licensing agreement, which ultimately fell through. However, T-Series discovered that its copyrighted musical works remained available on the MySpace platform without authorization, uploaded by users.

In February 2008, T-Series issued a legal notice demanding the removal of this infringing material. Although MySpace provided assurances that the content had been or would be taken down, T-Series found in December 2008 that much of it remained accessible. Consequently, T-Series filed a suit in the Delhi High Court for copyright infringement, seeking an injunction and damages.

Issues Involved

- Whether MySpace's actions (providing a platform for profit) constituted copyright infringement under Section 51 of the Copyright Act, 1957.
- Whether MySpace could claim protection under the "safe harbor" provisions of Section 79 of the Information Technology (IT) Act, 2000.
- What level of "knowledge" (general awareness vs. specific knowledge) is required to hold an intermediary liable for user-uploaded infringement.
- Whether an intermediary can be required to pre-screen all uploaded content proactively.

The 2011 Single Judge Decision

The Single Judge of the Delhi High Court ruled in favor of T-Series, taking a strict approach to intermediary liability.

- **Held MySpace Liable:** The court found *prima facie* infringement under Section 51(a)(ii) of the Copyright Act (allowing a place for profit to be used for infringement).
- **"General Awareness" was Sufficient:** The judge determined that MySpace had a "general awareness" of the infringement, especially after receiving the legal notice, and should have been more proactive. The presence of a notice-and-takedown mechanism in their own policies was seen as proof of this awareness.
- **Proactive Monitoring Mandated:** The court issued an interim injunction that not only required MySpace to remove specific notified content but also

mandated that they *proactively check* for any future infringing content related to T-Series' vast catalogue, effectively requiring content filtering or pre-screening.

The 2016 Division Bench Decision (Reversal)

MySpace appealed the single judge's order. The Division Bench reversed the earlier decision in a significant judgment that strengthened intermediary safe harbors in India.

- **Rejected Proactive Monitoring:** The Division Bench held that requiring an intermediary to proactively filter all future content was technologically impossible and would lead to "private censorship," having a chilling effect on free speech.
- **"Actual/Specific Knowledge" Required:** The court clarified that liability for an intermediary requires *actual* or *specific* knowledge of the infringing material, not just general awareness. This knowledge must point to specific URLs or links of the infringing content.
- **Harmonized IT Act and Copyright Act:** The judges held that Section 79 of the IT Act (safe harbors) and the Copyright Act must be read harmoniously. Intermediaries are entitled to the safe harbor defense if they follow due diligence as per the IT Act.
- **Balanced Relief:** The final order directed T-Series to provide MySpace with specific details (URLs) of infringing works. MySpace was then required to remove this specific content within 36 hours of notification, in line with IT Rules.

  The Division Bench ruling established a balanced "notice and takedown" regime in India, placing the burden of identifying specific infringing material on the copyright owner rather than forcing intermediaries to pre-screen all user content.

Significance of the Judgment

The 2016 Division Bench judgment in *T-Series v. MySpace* overturned the strict liability standard set by the Single Judge and introduced a more balanced “notice and takedown” regime in India. It placed the burden of identifying infringing material on the copyright holder rather than the intermediary, ensuring a fairer balance between the rights of copyright owners and the operational realities of

online platforms. This decision remains a landmark precedent in Indian law, reinforcing safe harbor protections for intermediaries and aligning India's intermediary liability framework with international digital governance standards.

VI. Emerging AI and Copyright Jurisdiction

7. ANI Media Pvt. Ltd. v. OpenAI Inc. & Anr (2024)

The case of ANI Media Pvt. Ltd. v. OpenAI Inc. is a critical legal battle taking place in the Delhi High Court. It is the first time in India that a major news organization is directly suing a generative AI company over the use of its copyrighted material for training artificial intelligence models.

Facts of the Case

In the 2024 case of *ANI Media Pvt. Ltd. v. OpenAI Inc.*, the major Indian news agency ANI sued OpenAI, the U.S.-based creator of ChatGPT, in the Delhi High Court. ANI alleges that OpenAI "scraped" (copied in bulk) its extensive library of news content from the internet and used it to train its AI systems without permission or payment.This involves two core issues :

- **Copyright Infringement:** ANI claims that using their work to build a commercial AI product is a direct violation of their copyright. They argue that this unauthorized use diminishes the value of their reporting and threatens their business model.
- **Reputation and Misinformation:** ANI also raised concerns that AI models might generate false news or attribute incorrect information to the ANI brand, which could damage their credibility.

Key Issues Involved

The case is navigating complex, uncharted legal territory:

- **Is Training Hacking?** Does the process of feeding copyrighted data into a computer model count as creating an infringing "adaptation" or copy under Indian law?
- **Fair Use vs. Fair Dealing:** India has a "fair dealing" provision in its Copyright Act, which is similar to the U.S. "fair use" doctrine. OpenAI might argue their use falls under this exception, but Indian law on this point is less flexible than U.S. law.

- **Where is the Offense?** OpenAI has argued the Delhi High Court lacks jurisdiction because its servers are in the U.S., and the training happened outside India. The court is deciding if the impact on ANI in India is enough to establish jurisdiction.
- **The Future of Content Creation:** The outcome will set a precedent for how AI companies interact with content creators. Should AI companies be forced to license every piece of data they use for training?

Developments and the Current Status

- **Suit Filed in late 2024:** ANI initiated the lawsuit in the Delhi High Court.
- **OpenAI Blocked ANI (Opt-Out):** In their defense, OpenAI revealed that they had already "blocklisted" ANI's domain (an opt-out mechanism) before the lawsuit was filed to prevent future content from being scraped.
- **Court Seeks Expert Help:** Recognizing the complex technical nature of AI, the Delhi High Court appointed two independent legal and tech experts (*amici curiae* or "friends of the court") to provide neutral, expert guidance.
- **No Immediate Ban:** The court denied ANI's request for an immediate ban on OpenAI using their work while the case is ongoing, but the lawsuit is moving forward.
- **Industry-Wide Implications:** Other Indian news organizations and publishers have signaled their intent to join the case or file their own, showing the widespread concern across the media industry.

The case is ongoing but represents India's **first major AI copyright dispute**, expected to influence AI governance and international IP law. The final judgment in this case will be a landmark decision, defining the rights of content creators and the responsibilities of AI developers in India's digital economy.

VII. Data Protection and Privacy Jurisdiction

Digital Personal Data Protection Act, 2023

The **Digital Personal Data Protection (DPDP) Act, 2023** is India's modern, comprehensive legislation governing how digital personal data is handled. It shifts India

from older, more fragmented rules towards a unified framework that aligns with global data protection standards like the GDPR, while being tailored to India's context.

The Act was officially passed in August 2023 and is being implemented gradually across the country.

- Applies to **all entities processing digital personal data**, even outside India if services target Indian citizens.

Core Structure and Definitions

The Act introduces clear definitions to streamline the data protection ecosystem:

- **Data Principal:** The individual to whom the personal data relates (e.g., you, the user).
- **Data Fiduciary:** The entity (person, company, or government body) that determines the purpose and means of processing personal data (e.g., a bank, an e-commerce company).
- **Data Processor:** Any entity that processes data *on behalf of* the Data Fiduciary (e.g., a cloud service provider used by the bank).
- **Personal Data:** Any data that can identify an individual, whether processed online or offline and then digitized.

Key Principles Driving the Act

The DPDP Act operates on several non-negotiable principles:

- **Consent is King:** Data can only be processed with clear, informed, and explicit consent from the individual, presented in a plain language notice.
- **Data Minimization:** Entities cannot collect more data than is absolutely necessary for the stated purpose.
- **Purpose Limitation:** Data collected for one reason cannot be used for a completely different reason without fresh consent.
- **Accountability:** The Data Fiduciary is entirely responsible for ensuring compliance with the Act at all times.
- **Transparency:** Individuals have a right to know what data is being processed about them.

Rights of the Data Principal (The Individual)

The Act empowers individuals significantly:

- **Right to Information:** You can ask an organization for a summary of the data they hold about you and who they've shared it with.

- **Right to Correction & Erasure:** If your data is wrong or outdated, you can demand correction or complete deletion (right to be forgotten).
- **Right to Grievance Redressal:** A formal path to complain if your data is mishandled, starting with the Data Fiduciary's internal officer.
- **Right to a Nominee:** You can legally designate a nominee to handle your data affairs after you are gone.

Obligations of the Data Fiduciary (The Company/Govt.)

Organizations processing data face strict mandates:

- **Valid Consent Mechanism:** They must provide an easy way to consent (or withdraw consent) via a "Consent Manager," an accredited entity that manages user consent preferences.
- **Data Security:** Must implement "reasonable security safeguards" to prevent breaches.
- **Breach Notification:** If a breach occurs, the Data Protection Board and affected individuals must be notified immediately.
- **Data Erasure:** Data must be deleted once its purpose is fulfilled, or if the individual withdraws consent.
- **Processing Children's Data:** Requires verifiable parental/guardian consent and prohibits processing that could cause harm or targeted advertising towards children.

Enforcement and Penalties

A new regulatory body, the **Data Protection Board of India (DPBI)**, has been established to enforce the Act. It acts as an independent quasi-judicial body to conduct inquiries and impose fines.

- **Hefty Penalties:** Fines can reach up to **₹250 crore** for major breaches like failing to secure data adequately, and up to ₹200 crore for violating children's data protection laws.
- **Appeals:** Decisions made by the DPBI can be challenged at the Telecom Disputes Settlement and Appellate Tribunal (TDSAT).

The DPDP Act marks a major shift, making data governance a serious legal and financial responsibility for every entity operating in India's digital space.

VIII. Trademark and Domain Name Jurisdiction

Tata Sons Pvt. Ltd. v. Hakunamatata Tata Founders (2022) 293 DLT 760

Facts of the Case

Tata Sons Private Limited, the promoter and principal investment holding company of the over 150-year-old and well-known "TATA" Group conglomerate, filed a trademark infringement suit in the Delhi High Court. The plaintiff is the registered proprietor of the "TATA" mark, which is recognized as a "well-known" mark in India with immense goodwill across numerous sectors, including financial services and digital technologies.

The suit was filed against Hakunamatata Tata Founders, an entity allegedly based in the UK, and other associated entities like domain registrars and a blockchain operator. The grievance arose because the defendants were operating websites, primarily www.tatabonus.com and www.hakunamatata.finance, to deal in a cryptocurrency named "TATA Coin" or "$TATA". The plaintiff alleged these websites were accessible in India, targeted Indian customers, and the unauthorized use of the renowned "TATA" mark constituted infringement, passing off, and dilution of its brand reputation.

Initially, a single judge dismissed the plaintiff's application for an interim injunction in October 2021, holding that the Delhi High Court lacked territorial jurisdiction over foreign defendants with no physical presence in India. Tata Sons appealed this decision to a Division Bench. While the appeal was pending, the defendants discontinued the use of the infringing marks and websites and proceeded *ex parte* (did not appear in court) despite repeated service attempts.

Legal Issues Involved

- Whether the Delhi High Court had territorial jurisdiction to issue injunctive directions against foreign defendants who had no physical presence in India but operated websites accessible within the jurisdiction ?
- Whether the mere accessibility of an interactive website to Indian users was sufficient to establish "purposeful availment" of the Indian market ?
- Whether the defendants' use of the mark "TATA" constituted infringement of a well-known trademark and was likely to cause confusion or deception among the Indian public?

- Whether the plaintiff was entitled to a permanent injunction when the defendants were proceeded against *ex parte* ?
- Whether minimal web traffic or a lack of proven sales to Indian customers negates the jurisdiction of Indian courts when a website bearing a well-known Indian trademark is accessible in India ?

Decision and Reasoning of the Court

The Delhi High Court's Division Bench and the subsequent single-judge final order addressed the legal issues as follows:

- **Territorial Jurisdiction:** The Court established jurisdiction, overturning the initial dismissal. It reasoned that the accessibility and "looming presence" of the interactive websites in India, coupled with the potential for confusion among customers, were sufficient. The court referred to precedents stating that websites accessible in a country and potentially engaged in commercial activity causing injury there can be considered as "targeting" that market.
- **Trademark Infringement:** The Court found a clear *prima facie* case of infringement and passing off, noting that the "TATA" mark is widely recognized and associated exclusively with the plaintiff in India. The defendants' use of an identical mark was deemed to be in bad faith, aiming to capitalize on the plaintiff's reputation. The Court concluded that the sale of products using the mark would likely cause irreparable damage to the plaintiff's goodwill.
- **Permanent Injunction:** As the defendants failed to appear and had ceased the infringing activities, the Court proceeded *ex parte*. Based on the evidence, the Court granted a permanent injunction, preventing the defendants from using the 'TATA' mark or similar marks in relation to cryptocurrencies, the www.tatabonus.com domain, or related platforms.
- **Specific Orders:** The Court directed the removal of the infringing website and ordered blockchain operators to delist the "$TATA" crypto assets. However, it found that www.hakunamatata.finance did not infringe, as "Hakunamatata" is a generic term and not likely to cause confusion.
- Further , the court reasoning regarding the minimal web traffic or a lack of proven sales to Indian customers was based on the concept of a **"looming presence"** and the nature of "well-known" trademarks:

- **Well-Known Marks:** When a mark like "TATA" is extremely well-known, even a single instance of a potential user accessing an infringing website can cause harm to the reputation and goodwill within India.

- **Accessibility as Targeting:** The court determined that an interactive website that is globally accessible implicitly targets the Indian market if the trademark in question is famously associated with India.

- **Potential for Harm:** The potential for confusion and damage to the plaintiff's goodwill within the jurisdiction was sufficient to establish a cause of action and jurisdiction, even without extensive evidence of actual Indian sales or traffic.

Thus, the court essentially ruled that in cases involving highly reputed, well-known marks and interactive websites, minimal web traffic is not a sufficient defense to escape Indian jurisdiction.

In short , The Delhi High Court held that even limited website accessibility aimed at Indian consumers constitutes targeting, sufficient for jurisdiction.

Principle Established:

Jurisdiction in cyberspace depends on intent to target, not volume of users or sales.

Conclusion

The evolution of personal jurisdiction in cyberspace represents a balancing act between technological innovation and legal accountability. Indian courts have progressively adopted international tests like purposeful availment, effects, and targeting to handle complex online disputes.

These landmark cases—ranging from *Banyan Tree Holdings* to *ANI v. OpenAI*—demonstrate India's readiness to assert jurisdiction over foreign entities when domestic rights are affected. Combined with data privacy reforms and competition oversight, India is emerging as a jurisdictional hub for digital law in the Global South.

As cyberspace continues to blur borders, clear principles of jurisdiction, accountability, and user protection remain crucial for maintaining fairness, transparency, and justice in the digital world.