REVISITING TRADE SECRETS PROTECTION IN INDIA: THE IMPERATIVE FOR STANDALONE LEGISLATION

Vinothini. V, BA LLB, LLM, VELS University (VISTAS) Pallavaram, Chennai

Jaishree. K, BBA LLB (Hons.) Crescent Institute of Science and Technology

ABSTRACT

Trade secrets represent a critical yet under-codified component of India's intellectual property regime. Unlike patents, trademarks, and copyrights, trade secrets in India are not governed by a dedicated statute but are protected through contractual obligations, equitable doctrines, and judicial recognition of breach of confidence. While Indian courts have provided remedies such as injunctions and damages, the absence of a comprehensive legislative framework has resulted in uncertainty regarding the scope of protectable information, evidentiary standards, available remedies, and procedural safeguards. In a rapidly evolving digital economy marked by technological innovation, cross-border commerce, data mobility, and startup-driven growth, the limitations of this fragmented approach have become increasingly evident. This paper critically examines the existing legal mechanisms for trade secrets protection in India and evaluates their adequacy in light of international obligations under the TRIPS Agreement administered by the World Trade Organization. Through doctrinal and comparative analysis, the study highlights gaps in enforcement, inconsistencies in judicial interpretation, and challenges posed by cyber misappropriation, employee mobility, and multinational disputes. By drawing comparisons with jurisdictions that have enacted specific trade secrets legislation, the paper argues that India's reliance on common law principles is insufficient to address contemporary commercial realities. It proposes that such legislation should clearly define trade secrets, establish civil and deterrent remedies, incorporate procedural safeguards for confidentiality during litigation, and balance commercial interests with public policy considerations.

Keywords: Trade Secrets, Confidential Information, Breach of Confidence, TRIPS, Intellectual Property Law, Innovation Policy, Indian Legal Reform.

Definition and Meaning of Trade Secrets

A **trade secret** refers to confidential business information that derives independent economic value from not being generally known to the public and is subject to reasonable efforts to maintain its secrecy. Unlike other forms of intellectual property such as patents or trademarks, trade secrets are not registered or disclosed to the public; their protection depends entirely upon their secrecy and the legal recognition of confidential obligations.

"At the international level, Article 39(2) of the TRIPS Agreement under the World Trade Organization defines undisclosed information (trade secrets) as information that:

1. Is secret in the sense that it is not generally known or readily accessible to persons within the circles that normally deal with such information;

2. Has commercial value because it is secret; and

3. Has been subject to reasonable steps by the person lawfully in control of the information.[1]

Existing Legal Framework Governing Trade Secrets in India

India does not have a standalone statute specifically governing trade secrets. Protection is primarily derived from a combination of contractual principles, equitable doctrines, and judicial precedents. The principal legal basis lies in the **Indian Contract Act, 1872**, particularly through confidentiality agreements, non-disclosure agreements (NDAs), and restrictive covenants in employment and commercial contracts. Courts enforce these agreements when a party unlawfully discloses or misuses confidential information. However, post-employment non-compete clauses are generally restricted under Section 27 of the Contract Act, which limits restraints of trade.[2]

In addition to contractual protection, Indian courts recognize the equitable doctrine of **breach of confidence**, whereby confidential information shared in a fiduciary or trust-based relationship cannot be misappropriated. The judiciary has repeatedly granted injunctions, Anton Piller orders (search and seizure), and damages in cases involving misuse of confidential business information. This jurisprudential development has created a quasi-proprietary recognition of trade secrets, though without statutory codification.

Trade secrets also receive indirect protection under intellectual property and information technology laws. For instance, the Information Technology Act, 2000 provides remedies against unauthorized access, data theft, and hacking, which may involve confidential business inform ation. However, these provisions address cyber offences rather than defining or protecting trade secrets per se. Similarly, specific sectoral regulations (such as those in pharmaceuticals or banking) may contain confidentiality obligations, but they do not establish a comprehensive legal regime.[3]

"Internationally, India is bound by Article 39 of the TRIPS Agreement under the World Trade Organization, which mandates protection of undisclosed information against unfair commercial use." India is considered compliant through judicial enforcement of confidentiality principles, yet it has not enacted legislation comparable to the U.S. Defend Trade Secrets Act or the EU Trade Secrets Directive. This structural gap has intensified the debate on the need for a dedicated Trade Secrets Act to ensure clarity, predictability, and stronger enforcement mechanisms in the evolving digital economy.

Emerging Challenges in the Digital and Innovation Economy

In the digital and innovation-driven economy, trade secrets face unprecedented vulnerabilities arising from cyber theft, artificial intelligence systems, remote working models, cloud-based data storage, and cross-border data transfers. Unlike traditional physical misappropriation, digital exfiltration of confidential information can occur instantaneously, anonymously, and across jurisdictions, making enforcement complex. Technology companies, startups, pharmaceutical firms, fintech enterprises, and research institutions increasingly rely on proprietary algorithms, source codes, customer databases, and AI training datasets as core competitive assets. The expansion of remote work environments has further blurred boundaries of control over confidential information, increasing risks of employee-driven leakage or inadvertent disclosure.[4] In such a context, India's fragmented protection model largely dependent on contractual remedies and equitable principles appears insufficient to address the scale and sophistication of digital misappropriation.

Indian courts have recognized the importance of safeguarding confidential business information in several landmark decisions. In **Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd.**, though a UK case, the principle of breach of confidence was articulated and later relied upon in Indian jurisprudence, establishing that confidential information shared

in circumstances importing an obligation of confidence cannot be misused.[5] In India, the Delhi High Court in **American Express Bank Ltd. v. Priya Puri** dealt with misuse of customer data by a former employee and clarified the distinction between general skill and knowledge versus proprietary confidential information.[6] Similarly, in **Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber**, the court protected a customer mailing list as confidential information, granting injunction against its unauthorized use. More recently, courts have granted dynamic injunctions and interim relief in cases involving digital data theft and employee mobility disputes, reflecting judicial sensitivity to emerging technological risks.

However, these case-specific remedies reveal structural limitations. The absence of statutory definitions, uniform evidentiary standards, and cross-border enforcement mechanisms weakens deterrence in cases involving cyber espionage or multinational data theft. As artificial intelligence and data-driven innovation become central to economic growth, trade secrets protection must evolve beyond traditional breach-of-contract litigation. The contemporary digital environment demands a comprehensive legislative framework capable of addressing technological realities, ensuring procedural safeguards during litigation, and balancing commercial confidentiality with innovation, employee mobility, and public interest concerns.

The Case for Standalone Legislation: Reform Proposals and Policy Recommendations

The growing centrality of confidential business information in India's technology-driven economy necessitates the enactment of a comprehensive Trade Secrets Act.[7] A standalone legislation would address the doctrinal fragmentation currently arising from reliance on contract law and equitable principles. At the outset, the proposed statute should incorporate a clear and internationally harmonized definition of trade secrets consistent with Article 39 of the TRIPS Agreement under the World Trade Organization, incorporating the three essential elements of secrecy, commercial value, and reasonable steps to maintain confidentiality.[8] A statutory definition would eliminate interpretative ambiguity and provide clarity to courts, businesses, and investors. The burden of proof standards must be carefully designed: while the plaintiff should establish the existence of a trade secret and reasonable protection measures, the statute may allow burden-shifting mechanisms once prima facie misappropriation is demonstrated.

Balancing commercial secrecy with public interest is equally critical. The statute

should include explicit protections for whistleblowers who disclose confidential information in good faith to report illegal activities, fraud, or threats to public health and safety. Exceptions should also be carved out for reverse engineering and independent discovery, thereby preserving innovation and fair competition.[9] Coordination with competition law principles is necessary to ensure that trade secrets protection does not become a tool for anti-competitive practices or market monopolization. Act should address cross-border misappropriation through jurisdictional clarity and enforcement cooperation mechanisms.[10] In an era of cloud computing and global value chains, harmonization with international best practices would enhance investor confidence and facilitate foreign direct investment. Special provisions dealing with digital evidence, cyber theft, and data localization concerns would further modernize the framework.[11]

International Legal Framework and TRIPS Compliance: Article 39 and Global Standards for Undisclosed Information

The international legal protection of trade secrets is primarily governed by Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by the World Trade Organization. Unlike patents, trademarks, and copyrights which are elaborately codified within TRIPS trade secrets are addressed under the broader category of "undisclosed information." Article 39 establishes minimum standards that member states must adopt to protect confidential business information against unfair commercial practices. Although TRIPS does not mandate a uniform legislative model, it obligates member countries to ensure effective legal remedies to prevent misappropriation.

Article 39(2) lays down three cumulative conditions for protection of undisclosed information. First, the information must be secret, meaning it is not generally known or readily accessible to persons within the circles that normally deal with such information. This requirement reflects a relative standard of secrecy rather than absolute confidentiality. Second, the information must possess commercial value because it is secret. The value derives not merely from its existence, but from the competitive advantage gained by restricting access. Third, the information must have been subject to reasonable steps by the lawful controller to keep it secret. This element introduces an objective compliance standard, requiring businesses to implement confidentiality agreements, restricted access systems, cybersecurity safeguards, and internal control mechanisms.

Article 39(3) further extends protection to undisclosed test data and other data submitted to governments for marketing approval of pharmaceutical or agricultural chemical products that utilize new chemical entities. Member states are required to protect such data against unfair commercial use and disclosure, except where necessary to protect the public or unless steps are taken to ensure that the data are protected against unfair use. R.K. Dewan & Co. This provision is particularly significant in the pharmaceutical sector, where clinical trial data represent substantial investment and competitive value.[12]

The global standard established under TRIPS does not prescribe whether protection must be civil, criminal, or administrative; it simply requires that effective legal means be available to prevent breach of confidence, industrial espionage, and unfair competition. Consequently, countries have adopted diverse legislative models.[13] The United States enacted the Defend Trade Secrets Act (DTSA), 2016, creating a federal civil cause of action for trade secret misappropriation and enabling ex parte seizure orders. The European Union adopted the Trade Secrets Directive (Directive (EU) 2016/943), harmonizing definitions and remedies across member states, including provisions to preserve confidentiality during litigation. These legislative frameworks provide detailed definitions, enforcement mechanisms, and procedural safeguards that reflect TRIPS compliance while strengthening domestic protection.[14]

Role of the Information Technology Act, 2000 and Limitations of the Present Framework

The Information Technology Act, 2000 plays a supplementary but indirect role in the protection of trade secrets in India. While the Act was primarily enacted to provide legal recognition to electronic transactions and to address cybercrimes, certain provisions offer incidental safeguards for confidential business information, particularly in cases involving unauthorized access, data theft, and digital misappropriation.[15]

Section 43 of the IT Act imposes civil liability where any person, without permission of the owner or person in charge of a computer system, accesses, downloads, copies, or extracts data or information. In the context of trade secrets, this provision may apply where proprietary databases, algorithms, source codes, or confidential documents are unlawfully accessed or copied. Compensation can be awarded to the affected party for damages suffered. Further, Section 66 criminalizes acts referred to in Section 43 when done dishonestly or fraudulently, thereby introducing penal consequences for cyber theft of confidential information.[16]

Section 72 of the Act provides punishment for breach of confidentiality and privacy by any person who has secured access to electronic records, books, registers, correspondence, or information pursuant to powers conferred under the Act and discloses such material without consent. Similarly, Section 72A penalizes disclosure of information in breach of lawful contract by intermediaries or service providers. These provisions are particularly relevant where employees, consultants, or digital service providers misuse confidential business data entrusted to them.[17]

Despite these protective mechanisms, the IT Act does not define "trade secrets" or "confidential business information." Its focus remains on unauthorized access and cyber offences rather than substantive intellectual property protection.[18] Consequently, while the Act can address the mode of digital theft, it does not determine whether the information in question qualifies as a protectable trade secret. This distinction is significant because trade secret protection requires proof of secrecy, commercial value, and reasonable steps to maintain confidentiality elements that the IT Act does not codify.[19]

Conclusion

Trade secrets have emerged as one of the most valuable yet insufficiently regulated components of India's intellectual property framework. In an era characterized by artificial intelligence, digital transformation, startup ecosystems, and cross-border technological collaborations, confidential business information has become a primary driver of competitive advantage.[20] However, unlike patents, trademarks, and copyrights, trade secrets in India lack a dedicated statutory regime. Protection currently depends on contractual obligations under the Indian Contract Act, 1872, equitable principles of breach of confidence, and limited remedies under the Information Technology Act, 2000. While Indian courts have developed progressive jurisprudence to safeguard confidential information, this case-by-case approach remains fragmented, reactive, and procedurally uncertain. Internationally, Article 39 of the TRIPS Agreement under the World Trade Organization sets minimum standards for protecting undisclosed information. Although India technically complies through judicial mechanisms, the absence of codified legislation creates gaps in enforcement, evidentiary standards, cross-border remedies, and investor confidence. The increasing risks of cyber espionage, employee mobility, cloud-based data storage, and algorithmic innovation further expose structural weaknesses in the existing framework.

ENDNOTES:

1. Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), 1994, Article 39, World Trade Organization, available at: https://www.wto.org

2. V.N. Shukla, *Law Relating to Intellectual Property*, Eastern Book Company, Lucknow, 2022, p. 412.

3. Tata Motors Ltd. v. State of West Bengal, (2009) SCC OnLine Cal 2637.

4. American Express Bank Ltd. v. Priya Puri, (2006) 110 DLT 546 (Delhi High Court).

5. John Richard Brady v. Chemical Process Equipments Pvt. Ltd., AIR 1987 Delhi 372.

6. Anil Gupta v. Kunal Dasgupta, 2002 (25) PTC 1 (Delhi High Court).

7. Nishith Desai Associates, *Protection of Trade Secrets in India*, available at: https://www.nishithdesai.com

8. Akhil Prasad, "Protection of Trade Secrets in India: A Legal Perspective," *Journal of Intellectual Property Rights*, Vol. 18, 2013, available at: https://nopr.niscpr.res.in

9. World Intellectual Property Organization (WIPO), *Trade Secrets and Confidential Business Information*, available at: https://www.wipo.int

10. Confederation of Indian Industry (CII), *Report on Trade Secrets Protection in India*, available at: https://www.cii.in

11. R.K. Dewan & Co., "Trade Secret Protection in India: Need for a Separate Law," available at: https://www.rkdewan.com

12. SpicyIP Blog, "Trade Secrets in India: A Case for Legislative Protection," available at: https://spicyip.com

13. The Information Technology Act, 2000, Government of India, available at: https://www.indiacode.nic.in

14. Indian Contract Act, 1872, Sections 27 and 73, Government of India, available at: https://www.indiacode.nic.in

15. Ritika Private Limited v. Biba Apparels Private Limited, 2016 (65) PTC 479 (Delhi High Court).

16. Law Commission of India, *Report on Intellectual Property Laws and Emerging Issues*, available at: https://lawcommissionofindia.nic.in

17. N. S. Gopalakrishnan, "Trade Secrets and Confidential Information: Legal Protection in India," *Indian Journal of Law and Technology*, available through Google Scholar.

18. OECD, *Trade Secrets Protection and Innovation Policy*, available at: https://www.oecd.org

19. European Union Trade Secrets Directive (2016/943), available at: https://eur-lex.europa.eu

20. United States Uniform Trade Secrets Act (UTSA), National Conference of Commissioners on Uniform State Laws, available at: https://www.uniformlaws.org