



# A Study on Navigating the Current Trends, Challenges, And The Evolving Landscape Of Trade Secret Protection In India

Janist Dhanol<sup>1\*</sup>, Dr. Pradip Kumar Kashyap<sup>2</sup>

<sup>1\*</sup>Research Scholar Raffles University, Neemrana Janist10@gmail.com

<sup>2</sup>Assistant Professor of Law Raffles University, Neemrana pradipragnul@gmail.com

## ABSTRACT

In the contemporary innovation centric economy, trade secrets proprietary information that confers a competitive advantage are increasingly considered valuable assets. This paper examines the complex issues and contemporary developments related to trade secret protection in India. It carefully looks at the existing laws, showing how they rely on common law principles, contracts, and conflicting rules in various laws, while also pointing out the lack of a single, clear law. This paper emphasizes recent judicial rulings and the urgent requirement for legislative reform to tackle the escalating issues of trade secret misappropriation in the digital era. This article proposes enhancements to India's trade secret framework by adopting best practices from countries with strong trade secret laws to promote innovation and equitable competition.

**Keywords:** Trade Secrets, India, Intellectual Property, Misappropriation, Legal Framework, Judicial Reform, International Best Practices, Innovation, Competition.

## Introduction

During a time of swift technological progress and fierce global rivalry, intangible assets, especially intellectual property, have become crucial for economic growth and corporate success. Trade secrets hold a distinct status among the various types of intellectual property. Trade secrets have intrinsic value owing to their confidentiality, in contrast to patents, copyrights, and trademarks, which necessitate registration and public disclosure. They include formulas, methods, designs, tools, or information compilations, representing a diverse array of proprietary knowledge that a corporation might exploit to secure a competitive edge over rivals who are either uninformed or fail to employ it.

The importance of trade secrets in India's emerging economy cannot be overstated. Trade secrets enhance the competitive edge of various Indian enterprises, both large and small. These secrets encompass the complex algorithms that drive the nation's flourishing IT sector and the distinctive manufacturing methods utilized in its varied industrial landscape. However, the absence of explicit, comprehensive legislation marks the complex legal structure governing trade secrets in India. Relying on contracts, common law rules, and some parts of other laws makes it harder to effectively protect these valuable assets from being stolen.(1)

The aim of this Research article is to deliver an exhaustive examination of the advancements and challenges concerning the safeguarding of trade secrets in India. This analysis will scrutinize the existing legal framework, pinpoint its complexities and deficiencies, and evaluate recent judicial rulings that provide clarity on the interpretation of trade secret laws. The article will study best practices from other jurisdictions with established trade secret regimes, such as the United States and the European Union, to find potential options for enhancing the Indian legal system. The primary aim of this study is to enhance the current dialogue on the need for legislative reform in India to strengthen and stabilize the trade secret protection framework, thus promoting fair competition and innovation.(2)

In the Indian context, delineating a "trade secret" requires navigating a legal system that does not provide a cohesive, statutory definition. Indian courts have generally adopted a principle akin to that in common law jurisdictions, emphasizing the confidential nature of the information, its commercial value derived from secrecy, and the prudent measures taken by the owner to maintain its confidentiality. Judicial Definition of Trade Secrets *In Indian Farmers Fertilizer v. Commissioner of Central Excise*.(3) the Customs Excise and Gold Tribunal of Delhi provided the following definition of "trade secrets." A "trade secret" denotes proprietary information that is not widely recognized by the public, confers economic benefits to its possessors, and necessitates stringent confidentiality protocols for its preservation.

**The key elements that Indian courts typically consider when determining whether information qualifies as a trade secret are:(4)**

➤ **Confidentiality:** The data must be suitably classified, not publicly accessible, and challenging to acquire through legal channels. Publicly accessible information is not considered a trade secret.

- **Commercial Value:** The knowledge must provide its owner a verifiable competitive advantage owing to its secrecy. This value may be strategic or financial.
- **Appropriate procedures to Safeguard Confidentiality:** The information's owner must have enacted proactive and diligent procedures to avert unauthorized disclosure. This category may include confidentiality agreements, physical security protocols, information access limitations, and specific company policies pertaining to secret information.
- It is essential to understand that simply having sensitive information does not automatically classify it as a trade secret. To protect their legal rights from infringement, the owner must exhibit utmost diligence in preserving their privacy. This focus on the owner's actions highlights the proactive responsibility that businesses bear in safeguarding their sensitive information.

Trade secrets appear to be the most vulnerable category of intellectual property in India due to insufficient legislative protection. To promote innovation and enhance standards for fair dealing and commercial ethics, quick reinforcement of protection is necessary. "In India, the protection of secrets must comply with contract law." Although it constitutes merely a legal liability, it prohibits an individual from disclosing information acquired through their employment or contractual agreement and provides the aggrieved party with a means of redress. Contractual obligations between the proprietor and the recipient may enhance the safeguarding of a trade secret. An employee possesses an irrevocable duty to serve their employer with fidelity and integrity. Twenty-one A fiduciary relationship has an implicit duty to safeguard trade secrets.

In India, substantial fines for infractions, and even less so criminal liability, are infrequently enforced, with the sole remedies for breach of trust being civil or equitable. Remedies include restitution or damages to the aggrieved person, restoration of all sensitive and proprietary data, and an injunction against third parties releasing information.

The court may mandate the at-fault party to "surrender" such materials. The disclosure of trade secrets is not invariably actionable, and proprietors of trade secrets possess remedies solely for misappropriation. Defenses against the disclosure of trade secrets encompass widespread awareness, parallel development, reverse engineering, innocent acquisition, statutory obligation, and public interest. Once trade secrets are disclosed to the public, they cannot be retracted, irrespective of the product's application that resulted in the revelation. A trade secret loses its protection if disclosed during its utilization. Consequently, it is imperative to enact legislation that renders infringers criminally accountable.

## **THE EXISTING LEGISLATION IN INDIA THAT OVERSEES THE SAFEGUARDING OF TRADE SECRETS (5)**

### ***The Indian Contract Act Section 27:***

This section forbids the dissemination of any information obtained while employed or under a contract and also offers remedies. It is based on the principle of equity, which entails the cessation of contractual duties due to a mutual breach of trust between the parties. However, this section offers no criminal remedies; it solely pertains to civil remedies. This rule mandates that for knowledge to qualify as a trade secret, it must possess the utmost degree of confidentiality.

### ***The Information Technology Act***

This act mandates that information be confined to electronic documents, with Section 72 of the Act offering this protection. Infringements of privacy and confidentiality incur fines as stipulated in "Section 72 of the Information Technology Act." Individuals who obtain or access private information, books, registrations, documents, or other material without the owner's authorization and later reveal or expose such information may face a penalty of up to five lakh rupees. Section 43A of the Information Technology Act stipulates compensation when an institution handling sensitive personal data results in an individual suffering an unjust loss or gain.

### ***Regulations of the Securities and Exchange Board of India, 1992 (Prohibition of Insider Trading):***

It does not offer explicit protection for trade secrets. These regulations stipulate that those who reveal or employ any confidential information in the public domain shall face prosecution under the Securities and Exchange Board of India Act, 1992.

### ***The Copyright Act, 1957:***

While primarily concerned with the protection of original literary, dramatic, musical, and artistic works, certain aspects of software code, which may also constitute a trade secret, could potentially be protected under copyright. However, copyright protection extends only to the expression of an idea, not the underlying idea itself, which is often the core of a trade secret.

### ***The Patents Act, 1970:***

While seemingly counterintuitive, the Patents Act implicitly acknowledges the existence of trade secrets. Businesses may choose to maintain certain inventions as trade secrets rather than seeking patent protection, particularly if the invention has a long lifespan or is difficult to reverse engineer.

**BHARTIYA NYAYA SANHITA AND THE INDIAN PENAL CODE:**

Sections 405–409 of the Indian Penal Code, 1860, regulate criminal breaches of trust. A criminal breach of trust occurs when an individual dishonestly misappropriates or converts property entrusted to them for personal use, or utilizes or disposes of such property in contravention of an explicit or implicit contract or relevant law, or permits another individual to do so. Therefore, the complainant must first establish that the accused or infringer possessed a fraudulent intent to misappropriate, convert, utilize, or dispose of the property. The Bhartiya Nyaya Sanhita, 2023, establishes culpability for the criminal breach of trust, as outlined in section 316 of the IPC.

The fragmented nature of the legal framework leaves significant gaps and uncertainties in the protection of trade secrets in India, hindering effective enforcement and creating challenges for businesses seeking to safeguard their valuable confidential information.

**THE FRAGMENTED LEGAL FRAMEWORK: NAVIGATING THE ABSENCE OF SPECIFIC LEGISLATION(6)**

*The most significant challenge in trade secret protection in India is the absence of a specific, comprehensive legislation analogous to the Defend Trade Secrets Act (DTSA) in the United States or the Trade Secrets Directive in the European Union. Instead, the legal framework for trade secret protection in India is fragmented and relies on a combination of common law principles, contractual remedies, and scattered provisions within other statutes.*

**Common Law Principles:**

The common law principles of breach of confidence and violation of trust are the fundamental legal framework for trade secret protection in India. Upon the receipt of sensitive information by one party from another, a responsibility of confidentiality is established, acknowledged by this equitable principle. The court may provide remedies, including injunctions and damages, if the recipient utilizes or reveals this information without the discloser's consent, resulting in injury to the discloser.

**Relationship Requirement:**

A breach of confidentiality typically necessitates a recognized confidential relationship, such as a fiduciary obligation, a contractual association, or an employer-employee dynamic. *Ambiguity and Indeterminacy: Common law principles are frequently construed on an individual case basis, resulting in ambiguity and unpredictability concerning the precise actions that constitute misappropriation and the remedies that may be pursued. This complicates the pursuit of claims against third parties who misappropriate trade secrets in the absence of a direct link.* **Restricted Criminal Sanctions:**

Due to the predominantly civil basis of common law remedies, criminal prosecution has challenges in deterring intentional and extensive trade secret theft.

**THE SIGNIFICANCE OF LEGISLATIVE REFORM IN INDIA**

*This study highlights the urgent necessity for legislative reform to rectify the shortcomings in India's fragmented trade secret protection legal framework. A specialized statute would improve legal clarity for companies by explicitly defining trade secrets, specifying actions that constitute misappropriation, and detailing potential remedies. This would eradicate ambiguity.*(7)

- A regulatory framework may serve as a more effective deterrent by offering enhanced enforcement mechanisms, including possible criminal penalties for egregious cases of trade secret theft.
- Specific provisions may be included to tackle the distinct issues presented by the digital realm, including data breaches and cyber theft.
- A meticulously designed legislation can attain equilibrium between safeguarding trade secrets and fostering fair competition and workforce mobility by integrating protections against excessively restrictive non-compete agreements.
- Enterprises would be more likely to allocate resources to research and development (R&D) if they were assured that their sensitive information would be protected by a strong trade secret protection system. This would lead to economic growth and innovation.
- A clear legal framework would facilitate enhanced engagement with global partners to combat cross-border trade secret misuse.

**CURRENT TRENDS IN TRADE SECRET PROTECTION IN INDIA(8)**

*The developing technology landscape and the growing interconnectedness of the global economy are introducing new trends and challenges in trade secret protection in India.*

**Digitalization and Data Security:** The advancement of digital technology has led to the electronic storage, transmission, and sharing of trade secrets.

- *Insider Threats:* Discontented or departing personnel with access to sensitive digital information may readily misappropriate trade secrets through data exfiltration methods.

- **Cyber Theft and Hacking:** Sophisticated cyberattacks targeting state-sponsored entities or organized criminal gangs may seek to expropriate valuable trade secrets. **Cloud Computing Risks:** Significant concerns exist around data security and jurisdictional complications in the event of a breach involving trade secrets kept on cloud systems.

**Knowledge Transfer and Employee Mobility:** The heightened mobility of employees, especially in high-tech sectors, presents a significant threat of trade secret misappropriation. In their new positions, former employees may intentionally or unintentionally utilize or disclose trade secrets from their previous company. Indian courts typically exhibit reluctance to enforce agreements that are excessively broad or restrictive, so hindering an individual's professional pursuits; consequently, the implementation of non-compete clauses, which are frequently employed to mitigate this risk, poses a significant legal challenge.

**Globalization and Cross-Border Misappropriation:** As economies become increasingly interconnected, trade secrets are more prone to traversing national borders, complicating the monitoring and enforcement of rights in instances of international misappropriation. The complexities are exacerbated by variations in legal frameworks and enforcement methodologies among jurisdictions.

**Artificial Intelligence and Machine Learning:** The advancement of AI and ML technologies offers both opportunities and challenges for the safeguarding of trade secrets. AI algorithms possess the potential to evolve into significant trade secrets necessitating stringent safeguarding. Conversely, the theft of trade secrets can be identified and executed by artificial intelligence methodologies.

**Inadequate Awareness and Enforcement Capacity:** Numerous Indian enterprises, especially SMEs, may lack sufficient awareness regarding the significance of trade secrets and the necessary protections. The effective investigation and prosecution of trade secret misappropriation cases may be obstructed by the judiciary's and law enforcement's insufficient specialized knowledge.

#### JUDICIAL DECLARATIONS: ANALYZING AND SHAPING THE CONTEXT INDIAN COURTS

*Several notable judicial decisions illustrate the courts' approach and the evolving understanding of trade secret protection have played a crucial role in interpreting and applying common law concepts and relevant statutes to adjudicate trade secret cases, despite the lack of specific legislation.(9)*

**Emphasis on Confidential Relationship:** Courts have consistently underscored that a breach of confidence claim necessitates the existence of a confidential relationship. Cases often focus on the existence of a relationship and the confidentiality of the disclosed information. Courts meticulously evaluate the actions implemented by the trade secret owner to preserve confidentiality. A charge of misappropriation may be undermined by insufficient security measures.

**Balancing Employer Rights and Employee Mobility:** Courts often enforce non-compete agreements with caution, aiming to reconcile the employee's right to seek employment with the employer's legitimate interest in protecting trade secrets. An essential consideration is the acceptability of the limits' duration, geographic scope, and nature.

**Acknowledgment of Digital Theft:** Courts have granted injunctions to prevent unauthorized access, utilization, or disclosure of sensitive electronically stored material due to an increasing awareness of the potential for trade secret theft through digital means. Indian courts have the jurisdiction to grant both temporary and permanent injunctions to avert the misappropriation of trade secrets or their future revelation. They may also award damages to compensate the proprietor of the trade secret for losses sustained due to the theft. Quantifying damages in certain scenarios can be challenging. While these judicial decisions provide useful guidance, the case-by-case methodology of common law adjudication may lead to inconsistencies and a lack of definitive, overarching principles for safeguarding trade secrets. This situation underscores the imperative for a more comprehensive legal framework.

#### CHALLENGES OF TRADE SECRETS PROTECTION IN INDIA

While trade secrets protection is crucial for businesses in India, it comes with its set of challenges:(10)

The absence of formal acknowledgment India depends on common law principles and contractual remedies instead of having specific legislation for the safeguarding of trade secrets. The lack of clarity complicates the definition of trade secrets and the extent of their protection. In contrast to patents or trademarks, trade secrets lack recognition as intellectual property under Indian law, resulting in inconsistent and fragmented protection. While confidentiality agreements offer limited remedies under the Indian Contract Act of 1872, these provisions are inadequate for addressing intricate matters like as reverse engineering or theft by third parties. The absence of statutory recognition hinders India's ability to fulfill its international responsibilities under the TRIPS Agreement, which requires the protection of secret information.

In the absence of written regulations, enterprises must traverse a fragmented array of common law principles, often leading to conflicting judicial decisions. Industries dependent on proprietary information are significantly affected by this disparity, which deters foreign investment and hinders innovation.

The Indian legal system presents considerable procedural obstacles in the enforcement of trade secret protection. Civil remedies, typically pursued for contract violations or breaches of confidence, may include protracted litigation, during which trade secrets may be disclosed in court proceedings. The situation is exacerbated by the lack of strong procedural safeguards such as confidentiality orders. The enforcement process is complicated by challenges related to evidence. It

is essential to exhibit the material's confidential character and improper utilization to establish misappropriation. Although Indian courts recognize trade secret claims, they often lack definitive criteria for assessing evidence, resulting in contradictory rulings. This complicates the burden of proof, especially when the misappropriator asserts independent research or reverse engineering.(12)

The lack of criminal consequences diminishes deterrent, permitting misappropriation to transpire with minimal repercussions. Non-disclosure agreements and confidentiality contracts are largely ineffectual. In India, non-disclosure agreements (NDAs) and confidentiality clauses are often employed mechanisms to safeguard trade secrets. The absence of enforcement mechanisms and inadequate drafting undermine their efficacy. Numerous NDAs are susceptible to legal disputes due to their inadequate specification of the scope of secret information or the absence of provisions for post-employment obligations.(13)

a) The lack of a specific Trade Secrets Act becomes a significant issue in India. In contrast to other nations with dedicated legislation safeguarding trade secrets, India uses a synthesis of existing laws, including breach of confidence, contract law, and principles of unfair competition, to ensure the protection of trade secrets.

b) Depending on principles of unfair competition, breach of confidentiality, and contract law: Implementing non-disclosure agreements (NDAs) and contractual obligations is frequently crucial for protection. Companies must traverse the intricacies of contract law, violation of confidentiality, and unfair competition statutes to pursue remedies for trade secret misappropriation.

c) In legal proceedings concerning trade secret misappropriation, the proprietor of the trade secret holds the burden of proof. This task can be challenging as it necessitates the provision of significant proof of misconduct, which is not always readily available.

d) The potential for other parties to replicate or independently ascertain sensitive knowledge complicates the protection of trade secrets due to the risks of reverse engineering and independent discovery. In particular circumstances, demonstrating that misappropriation transpired can be far more challenging.

## CONCLUSION AND SUGGESTIONS

In India's ever changing economic environment, trade secrets are essential assets. Their effective maintenance is greatly hindered by the existing fragmented legal structure. The lack of targeted law, especially in the digital age, creates uncertainties, hinders enforcement, and leaves businesses vulnerable to misappropriation.

This research underscores the pressing necessity for legislative change in India by analyzing contemporary trends, assessing court decisions, and deriving lessons from international best practices. A separate statute on trade secrets would improve enforcement procedures, tackle the distinct issues of the digital age, and promote a more favorable climate for innovation and equitable competition. Furthermore, it strengthening India's intellectual property environment, especially concerning trade secrets, is essential for maintaining its competitive edge and attracting further investment in research and development as it ascends to global economic prominence. The implementation of legislative reform is not simply a legal update; it is a strategic imperative for India's future economic prosperity. India must embark on this endeavor to fully actualize its innovative potential and reinforce its standing in the global knowledge economy, notwithstanding the intricacies involved in developing a robust and effective trade secret structure.

- An exhaustive enumeration of actions that comprise trade secret misappropriation, including acquisition, utilization, and unauthorized disclosure.
- Provisions regarding employee misappropriation, encompassing the enforcement of allowable confidentiality and non-compete agreements.
- Regulations concerning data security and cybercrime are established to prevent the theft of digital trade secrets.
- A variety of civil remedies, such as injunctions, compensatory damages, unjust enrichment, and maybe punitive damages, are accessible for intentional and malicious misappropriation.
- The evaluation of criminal punishments for severe cases of trade secret theft is underway.
- Protocols to maintain the confidentiality of trade secrets during judicial procedures.
- Safeguards for whistleblowers who lawfully disclose the misuse of trade secrets to relevant authorities.

## REFERENCES

1. Agarwal, A., International Framework for the Protection of Trade Secrets, 11 INT'L J. CREATIVE RES. THOUGHTS (2023), available at <https://ijert.org/papers/IJCRT2303019.pdf> (last visited April 29, 2025).
2. Khan, S., Sharma, S. K., & Laha, A. K., From Misalignment to Synergy: Analysis of Patents from Indian Universities & Research Institutions, arXiv Preprint (2023), available at <https://arxiv.org/abs/2304.12176> (last visited April. 29, 2025).
3. Mishra, R., & Shukla, A. K., Intellectual Property Right and Initiatives of Government of India, 3 J. INTELL. PROP. RTS. L. (2020), available at <https://lawjournals.celnet.in/index.php/jiprl/article/view/718> (last visited April. 29, 2025).
4. Ahuja, V. K., PUBLIC INTERNATIONAL LAW (1st ed., LexisNexis Butterworths 2016).
5. Feng Jiang et al., The Implementation of China's Mental Health Law-Defined Risk Criteria for Involuntary Admission: A National Cross-Sectional Study of Involuntarily Hospitalized Patients, 9 FRONTIERS PSYCHIATRY 560, 560 (2018).
6. Andrew Sparrow, Mental Health Services to Get £2bn Funding Boost in Budget, GUARDIAN (Oct. 28, 2018, 6:30

- PM), <https://www.theguardian.com/uk-news/2018/oct/28/mental-healthservices-to-get-2bn-funding-boost-in-budget>.
7. Carl Baker, Mental Health Statistics for England: Prevalence, Services and Funding: (Briefing Paper Number 6899), NAT'L GREY LITERATURE COLLECTION (May 2,2018),
  8. <http://allcatsrgrey.org.uk/wp/wpfb-file/sn06988-1-pdf/>.
  9. Torleif Ruud & Edvard Hauff, Community Mental Health Services in Norway, 31 INT'L J. MENTAL HEALTH 3, 7 (2002).
  10. Anne Karin Lindahl & Anen Ringard, Norwegian Centre for Health Service, The Norwegian Health Care System, 2013, in INTERNATIONAL HEALTH CARE SYSTEM PROFILES, 2013, at 103 (Sarah
  11. Thomson et al. eds., 2013).
  12. Marit Knapstad et al., Prompt Mental Health Care, the Norwegian Version of IAPT: Clinical Outcomes and Predictors of Change in a Multicenter Cohort Study, 18 BMC PSYCHIATRY 260, 269 (2018).