



# Misappropriation of Trade Secrets Under the Indian Legal Framework: An Analytical Study

Veena TN\*

## Abstract

The main purpose of this paper is to examine the aspects of the misappropriation of trade secrets under the Indian legal framework, and how this can be prevented. The paper also tries to understand the nature of trade secrets, the reasons for protecting them, and the practical challenges in identifying and protecting them as there is no legal framework in India to protect trade secrets from misappropriation. The paper concludes by highlighting the challenges to the Indian legal framework, in handling and protecting the misappropriation of trade secrets.

**Keywords:** Business, Competition, Information, Uniform Trade Secrets Act 1979, Copyright Act 1957

## 1. Introduction

While information is an asset for any business, trade secrets are often crucial for the business's survival. It can include strategies, designs, client databases, formulae, programs, and any other confidential information that needs to be kept a secret<sup>1</sup>. Trade secrets have become increasingly valuable in the digital age, providing businesses with a competitive advantage and contributing to their success. However, protecting these

---

\* BMS College of Law; Email: [veena@bmscl.ac.in](mailto:veena@bmscl.ac.in)

<sup>1</sup> Desai, D. A. (2003). Trade secret protection in India. *Intellectual Property Journal*, 12(2) 175-191.

secrets has become more challenging with the rise of cyberattacks, hacking, and insider threats. Trade secrets may differ across jurisdictions but have three common traits - not being public, offering some economic benefit, and being actively protected. Trade secret law safeguards technological and commercial information that is not commonly recognized in the trade and prevents others from commercially exploiting it without authorization. The purpose of trade secrets protection is to promote research and development by protecting the source of business information and upholding proper business ethics.<sup>2</sup>

Trade secrets encompass both technical information, such as information concerning manufacturing processes, pharmaceutical test data, designs and drawings of computer programs, and commercial information, such as distribution methods, list of suppliers and clients, and advertising strategies. A trade secret may also comprise a combination of elements, each of which is in the public domain, but where the combination which is kept secret, provides a competitive advantage.

As per Article 39(2) of the agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), its members are given the flexibility to frame laws that prevent the unauthorized disclosure and use of certain information<sup>3</sup>. The information must meet the following criteria:

- It is secret in the sense that it is not readily accessible by those
- people who deal with such information on a regular basis.

---

<sup>2</sup> World Intellectual Property Organization (WIPO), <https://www.wipo.int/tradesecrets/en/>

<sup>3</sup>United Nations Conference on Trade and Development, [https://unctad.org/system/files/official-document/ditctnecd20083\\_en.pdf](https://unctad.org/system/files/official-document/ditctnecd20083_en.pdf)

- It has commercial value.
- Reasonable steps have been taken by the person lawfully in control of the information.

Secrecy is to be maintained in such a manner as to prevent access to trade secret information by those who are not entitled to it. Information is secret if it is not generally known to the public and the secrecy is not waived by the owner of the information. The trade secret must be kept secret and should not be used without the owner's permission. To safeguard trade secrets and maintain their competitive advantage in the digital age, employers have to make their employees sign the non-disclosure agreement or other confidentiality agreements. The key objective of a trade secret is to provide an incentive for businesses to innovate by safeguarding the substantial time and capital invested to develop competitively advantageous innovations, both technical and commercial, and especially those that are not patentable or do not merit the cost of patenting. If not protected by trade secret law, then competitors could use these innovations without having to shoulder the burden of costs or risks faced in developing the innovations.

Misappropriation occurs when someone discloses or uses a trade secret without consent, when at the time of disclosure, he or she had reason to know that knowledge of the trade secret was:

- Derived from someone who obtained it through improper means;
- Obtained under circumstances that gave rise to maintaining its secrecy or limiting its use; or
- Derived through a person who owed a duty of confidentiality to the trade secret owner.

The focus of the paper is on addressing the issues pertaining to the misappropriation of trade secrets i.e., under the Indian legal framework. It starts with information that qualifies as a trade secret and threats to the trade secrets. The next part of the paper traces the aspects of the misappropriation of trade secrets, their types, and the liability upon the person for misappropriation. Subsequently, the paper will analyse the protective remedies and reliefs under the Indian legal framework to avoid misappropriation. Further, the paper highlights the inadequacies in the present legal framework to deal with trade secrets misappropriation. Finally, it is asserted that the existing Indian legal system needs to be changed or there should be a *Sui-generis* system to address the issues in the protection of trade secrets.

## **2. Information that Qualifies as a Trade Secret**

The trade secret regime is an important law in ensuring that the information and knowledge generated by companies are protected. The Uniform Trade Secrets Act has been adopted by many countries, which provides comprehensive protection for trade secrets and also helps in their development.<sup>4</sup>

There are many perks in protecting a piece of information as a trade secret. It helps the company keep its information confidential and also prevents its competitors from taking unfair advantage. If the information is protected as a trade secret, then the company can also sue for its misappropriation and gain damages.

The Hon'ble High Court of Bombay, in *Bombay Dyeing and Manufacturing Co. Ltd. v. Mehar Karan Singh*<sup>5</sup>, laid down the

---

<sup>4</sup> Kunal Arora, Trade secrets – As an Intellectual property and its protection, <https://www.legal-servicesindia.com/>

<sup>5</sup> *Bombay Dyeing and Manufacturing Co. Ltd. v. Mehar Karan Singh*, 2010 (112) BomLR3 75.

following factors for information to be classified as a Trade Secret:

- The extent to which the information is known outside the business;
- The extent to which it is known to those inside the business, i.e., by employees;
- The precautions taken by the holder of the trade secret to guard the secrecy;
- The savings affected and the value to the holder in having the information as against competitors;
- The amount of effort or money expended in obtaining and developing the information; and
- The amount of time and expense it would take others to acquire and duplicate the information.

Protection under trade secrets can be enjoyed for an indefinite time, provided the subject matter of the trade secret is commercially valuable and is kept confidential. The information loses its trade secret status if it is accidentally or intentionally disclosed by anyone.

**Scientific or Technical Information:** Information related to the development of upcoming products or services with their functional or technical attributes such as inventions, patents, computer software, passwords, methods for increasing production efficiency, security standards, etc.

- Drawings, blueprints, production and marketing plans, strategies, investment offers, and descriptions of business processes are examples of technological and production information.
- Business information: sensitive information including business ideas, such as ideas for a new product or a new marketing approach, marketing plans, cost and price

information, customer lists, market analysis, data on suppliers and contractors, and customer information.

- **Financial Information:** Information related to management and accounting data, cash flow calculations, reports, pricing mechanisms, etc.
- Any other valuable information that has some value and is not widely known by the company's competitors.

Trade secrets law is the direction towards promoting trade. Hence, only such information must be protected that helps achieve the result. The common law adopted a functional approach for defining the concept of "trade secrets". Courts preferred to restrict between information that is in the public domain and that which is not. However, the "Law Commission of England and Wales"<sup>6</sup> has laid down specific categories of information that can be regarded as trade secrets. The Commission laid down four main specific types of information which can be considered as trade secrets. These are:

- Secrets that are related to specific products
- Technological secrets
- Secrets related to strategic business information; and
- Secrets that are included in the private collections of individual items of public information

## **2.1 Threats to Trade Secrets**

Intense competition in domestic and export markets has also led to an alarming increase in theft by outsiders, known as industrial espionage. Such activities are on the rise due to increasing global competition, shorter product cycles, thinning

---

<sup>6</sup> Law Commission Annual Report 2021-22, <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/12/Annual-Report-2021-22-Final.pdf>

profit margins, and declining employee loyalty. Businesses strive to protect their trade secrets by enacting corporate security measures and confidentiality clauses in employment, technology licensing, distributorship and joint venture agreements.

## 2.2 Misappropriation of Trade Secrets

Trade secret infringement is called “misappropriation.” It occurs when someone improperly acquires, discloses or uses a trade secret without consent or when knowledge of the trade secret is acquired through a mistake or accident. Misappropriation need not be intentional. It can happen inadvertently or through negligence.

According to Section 1(2) of the Uniform Trade Secrets Act<sup>7</sup>, 1979 misappropriation means:

- 1) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secrets was acquired by improper means: or
- 2) Disclosure or use of trade secrets of another without express or implied consent by a person who
  - a. Used improper means to acquire knowledge of the trade secret, or
  - b. At the time of disclosure or use, knew of had reason to know that his knowledge of the trade secret was
    - i. Derived from or through a person who had utilised improper means to acquire it;

---

<sup>7</sup> Uniform Trade Secrets Act, 1979, Section 1(2), (U.S), [https://www.Cga.Ct.Gov/Current/Pub/Chap\\_625.Htm](https://www.Cga.Ct.Gov/Current/Pub/Chap_625.Htm)

- ii. Acquired under circumstances giving rise to a duty to maintain its secrecy or limits its use; or
- iii. Derived from or through a person who owned a duty to the person seeking relief to maintain its secrecy or limits its use; or
- c. Before a material change of his position, knew of had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

Most jurisdictions define misappropriation as the unlawful acquisition of a trade secret, the disclosure or use of a trade secret by one who knows or should know that the trade secret is secret, or the interference with the contractual rights of the trade secret holder. In the initial period, the Indian courts have understood the importance of trade secrets and have adopted several provisions for safeguarding the trade secrets from unlawful acquisition. For instance, the courts applied Sec 37 of the Specific Relief Act, 1963, which provides for Injunctive relief; Sec 73 of the Indian Contract Act, 1872, which provides damages. In addition to that, the courts also applied Sec 27 of the Indian Contract Act, 1872, which deals with an agreement in restraint of trade, and Sec 405 of the Indian Penal Code, 1860, which talks about a criminal breach of trust.

In *John Richard Brady & Ors v. Chemical Process Equipment P Ltd & Anr*<sup>8</sup>, the principles of confidentiality were discussed for the first time in this case. The Court held that “the law on this subject does not depend on any implied contract. It depends on the broad principles of equity that who has received information in confidence shall not take unfair advantage of it.

---

<sup>8</sup> John Richard Brady & Ors v. Chemical Process Equipment P Ltd & Anr, AIR 1987 Delhi 372



At present, the most common types of trade secrets include know-how (including inventions), technical data, customer lists, and business strategies. If there is no contractual agreement between the company and the person, the court may be able to order the person to return the trade secret to the company.

Misappropriation of trade secrets can be understood as the discovery of trade secret by improper methods, which is not covered by any specific law. Therefore, the common cause of action against misappropriation or unauthorized disclosure of trade secrets includes civil action for breach of contract and wrongdoing due to misappropriation; and criminal action for theft and breach of trust.

Under contract law, a person can be bound contractually from disclosing information. Parties can enter into confidentiality agreements, also known as non-disclosure agreements (NDAs), to protect trade secrets and confidential information. These agreements typically impose obligations on the recipient of the information to maintain its confidentiality and restrict its use for unauthorized purposes. Breach of a confidentiality agreement can lead to legal remedies and damages<sup>9</sup>.

An NDA should be specific about the confidential information which should be considered secret and therefore not to be disclosed to third parties. Moreover, hefty penalties specified in the NDA upon its breach can prevent the third party from spilling the beans. Even though there are no specialized alternative dispute resolution (ADR) methods for disputes arising out of trade secrets in India, every NDA should contain an ADR clause so that in case of dispute, the matter can be sorted outside the Courts by traditional ADR methods including mediation, conciliation, and arbitration thereby saving valuable time. Indeed, ADR methods tend to be much

---

<sup>9</sup> Indian Contract Act, 1872, S. 27, No.9, Acts of Parliament,1872

faster and less expensive than judicial actions. If a party violates the terms of a confidentiality agreement or breaches its contractual obligations regarding the protection of trade secrets, the injured party can seek legal remedies under contract law. This may include specific performance, injunctions to prevent further disclosure or use of trade secrets, and monetary damages for losses suffered as a result of the breach<sup>10</sup>.

### **2.3 Liability for Misunderstanding a Trade Secret**

According to Section 1(2) of the Uniform Trade Secret Act,<sup>11</sup> the following groups of people are prohibited from copying, using, or benefiting from one's trade secrets or disclosing them to others without their permission:

- People who are contractually obligated to not disclose or use any such trade secret information. This includes any employee who is regularly in contact with such information as part of his or her employment with the employer.
- People who deliberately gain access to trade secret information by improper means, such as theft, industrial espionage, or bribery.
- People who involuntarily get access to trade secrets by accident or mistake, despite being aware of the fact that such information is protected as a trade secret.
- People who are obligated under non-disclosure agreements have a duty not to disclose trade secret information without getting permission from the owner.

---

<sup>10</sup> Lemley, M. A., & Dumont, J. R. (2010). *Intellectual property in the new technological age* (Vol. 2). Aspen Publishers.

<sup>11</sup> *Supra* note 7

### 3. Protection Under Indian Legal Framework

In India, there is no uniform legislation protecting trade secrets and confidential information. It is protected by numerous, disparate provisions of various statutes. Indian courts have recognized trade secret protection based on equity principles and common law remedies for breach of confidence and breach of contract such as Section 27<sup>12</sup> of the Contract Act, 1872, which states that covenants shall be structured in such a way that they protect the firm's confidentiality while also allowing the employee to work in his preferred profession.

A trade secret cannot be protected against being discovered by fair and honest means, such as by independent invention or reverse engineering. If a person who does not have legal access to the trade secret information, deciphers the information without taking recourse to any illegal means, such as by reverse engineering or as by independent invention, then such a person cannot be stopped from using the information so discovered. Under such circumstances, the owner of a trade secret cannot take any legal action against the other person.

In the case of *Richard Brady v. Chemical Process Equipment Pvt. Ltd*<sup>13</sup>, the Delhi High Court went farther by invoking a broader equitable jurisdiction and awarded an injunction in the absence of a contract. Non-compete covenants, non-solicitation covenants, non-poaching covenants, and confidentiality covenants are all examples of restrictive covenants. The courts have recognized client information kept in databases as copyrightable material under the Copyright Act, 1957, implying indirectly the protection of trade secrets and confidential information from disclosure/infringement<sup>14</sup>.

---

<sup>12</sup> Supra note 8

<sup>13</sup> *Richard Brady v. Chemical Process Equipment Pvt. Ltd*, AIR 1987 Delhi 372

<sup>14</sup> *Id.*

In *Burlington Home Shopping Pvt. Ltd. v Rajnish Chibber*<sup>15</sup>, the Delhi High Court examined an application for interim relief in relation to a suit brought by a mail order service company against an employee seeking an injunction prohibiting "breach of copyright and confidentiality." The Court determined that a compilation of addresses formed through the commitment of time, money, labour, and skill constitutes a literary work in which the author holds copyright. Hence, copyright and trade secret law covers distinct aspects of compiled business data, with copyright protecting the expression contained in these compilations and trade secret law protecting the underlying data.

Confidentiality is the central factor that needs to be proven in any action, when there is a breach. The business must establish that sufficient steps had been taken to ensure that the data/information remains confidential, otherwise, the information lacks the quality of being a trade secret and is therefore not protected as such. Therefore, in practice, the trade secret owner must ensure that appropriate steps are actually taken to keep trade secrets safe and confidential wherein except executing NDAs. Other measures that a company can adopt to protect its valuable information as a trade secret are:

- The companies should identify which information constitutes a trade secret and should review it periodically.
- A trade secret regime should be established in a company. The document should include the main parameters of the protection system and a list of people responsible for regulating protective measures.
- Any valuable business information can be protected by way of encryption.

---

<sup>15</sup> *Burlington Home Shopping Pvt. Ltd. v Rajnish Chibber*, 61(1995) DLT 6

- There should be controlled and limited access to trade secret information by using measures like physical, managerial, technical, and contractual.
- Accessing trade secret information by employees should not be allowed from remote locations.
- There should be confidentiality agreements between the employees and the third parties to grant them access to the trade secret information, and such confidentiality should be maintained even after the expiration of such agreements.
- While preparing employment contracts and standard contracts with contractors, a clause that talks about the liability for revealing confidential information should also be incorporated.
- A vigorous trade secret policy should be implemented by the company if such a trade secret forms a critical part of the business value.
- Technological means, such as mechanisms that can expose a trade secret, should be adopted to manage risks associated with reverse engineering if the company offers a technological product.
- There should be strict control over the use of computer network accounts, with a disclaimer that if anyone transfers a password, that may constitute dismissal due to “disclosure of trade secrets.”

Though not explicitly, but implicitly, trade secrets protection clauses have also been incorporated in Statutes including the Information Technology Act, 2000, the Indian Penal Code, the Securities Exchange Board of India Act, 1992 as well as the

Code of Civil Procedure, 1908. For instance, Section 43A<sup>16</sup> of the Information Technology Act 2000, provides for compensation where any entity handling any personal sensitive information causes wrongful loss or wrongful gain to any person. Further, Section 72<sup>17</sup> of the Information Technology Act ensues criminal liability for breach of secrecy and trust. Similarly, the Indian Penal Code provides for criminal violation of trust and the Code of Civil Procedure<sup>18</sup> protects documents that may be deemed necessary for the Courts to adjudicate effectively. In this context, it is also relevant to refer to the Securities and Exchange Board of India Act, 1992 which makes Insider use and publication of sensitive information a punishable act.

#### 4. Enforcement

When it comes to enforcement, both civil and criminal actions are available for trade secret misappropriation. An injunction granted by courts can restrain the wrongdoer from disclosing trade secrets as well as damages can be sought by the trade secret owner. Other civil actions which the courts can grant to the trade secret owner in case of trade secret leakage is return of trade secrets or materials containing trade secrets. On the other hand, fine or imprisonment can be granted by courts under the penal code, copyright and information technology law.

The relief that a court can grant as civil liability is the legal responsibility an individual or entity may have to compensate another party for damages or losses caused by their actions or omissions. In the context of trade secret misappropriation, civil

---

<sup>16</sup> The Information Technology Act, 2000 Section 43A - Compensation for failure to protect data, No.21, Acts of Parliament, 2000

<sup>17</sup> *Id.* at Section 72 - Penalty for breach of confidentiality and privacy

<sup>18</sup> Indian Penal Code, 1860 Section 405 - Criminal breach of trust, No.45, Acts of Parliament, 1860

liability can arise when one party unlawfully acquires, uses, or discloses another party's trade secrets, resulting in harm or damages.

There are no express criminal remedies available for misappropriation of a trade secret. However, offences such as criminal breach of trust, theft, or cheating may be applicable. The Indian Penal Code 1860 (IPC) and specific subject-matter legislation, such as the Copyright Act 1957 (governing copyrights) and the Information Technology Act 2000 (governing electronic records), contain provisions setting out specific offences that may be punishable by imprisonment or a fine.

Businesses that have information eligible for trade secret protection are required to undertake certain steps that protect such information from being disclosed. These steps should include identifying the exact scope and nature of the information to be protected as a trade secret, developing a proper trade secret policy, limiting the access to such information, executing confidentiality agreements and NDAs whenever necessary.

## **5. Conclusion**

As the world is getting more competitive and everyone wants to build brand value, companies should take the necessary steps to protect their information that has commercial value as a trade secret. There are many advantages that come with protecting information as a trade secret. The biggest one is that, under trade secrets, protection is granted for an indefinite amount of time unless someone breaches a contract or spills it to the outside world. In addition to that, the trade secret holder gets relief in the form of an injunction or damages if someone is liable for the misappropriation of a trade secret.

To conclude, India requires formal legislation in line with Uniform Trade Secrets Act to deter the illegal transfer of trade

secrets by individuals who have access to them as part of their employment responsibilities. These steps, in conjunction with provisions relating to breach of contract or Non-Disclosure Agreements, can help promote a culture of respect in industrial circles for trade secrets and undisclosed information as proprietary assets belonging to their owners. There is an urgent requirement to revamp the present law relating to trade secrets protection.

In India, there is no effective legislation or rule for protection of trade secrets, though Sec 27 of the Contract Act of 1872 provides civil remedy up to a certain limit. There is no uniformity in the views of the courts over this issue. Under, Art.10 of the Paris Convention (1967) and Article 39 of TRIPS ensures protection against unfair competition, which includes the acquisition of undisclosed information by third parties. Therefore, in order to safeguard and protect trade secrets from unfair competition and acquisition of undisclosed information, it is time for Indian legislation to adopt a system that gives all-around protection to the information which are trade secrets. A robust trade secret policy has to be developed and implemented, as trade secrets play a critical part in fostering innovation, competitiveness, and economic growth. India has a responsibility to frame rules and regulations to remove trade secrets ambiguity. So, there is an immediate need for a '*Sui Generis*' system in India for the protection of trade secrets.