E-JAIRIPA

Vol. VII (Issue I), pp.- 63-73

SCRUTINISING PROTECTION OF INNOVATION IN INDIA UNDER TRADE SECRET LAWS: A CRITICAL STUDY

Author: *Shivam Kumar*[1]

Abstract

Trade secrets are one of the most important, yet under-institutionalised, forms of IP in India. Patents, trademarks, copyright and designs, have s0pecific statutory protection, but trade secrets are protected only as a collection of contract law, equity, copyright law, the IT Act, 2000 and the leftover criminal provisions. This is even though India has committed under Article 39(2) of the TRIPS Agreement, which aims to enunciate appropriate safeguard against commercial misuse of the undisclosed information. This article discusses the doctrine of trade secrets in India from a critical perspective, highlighting the judicial journey of the doctrine from various significant cases. It examines the jurisprudence of courts using Section 27 of the Indian Contract Act, 1872, equitable breach of confidence principles and copyright law to bridge the legislative gap and the issues involved in the identification of the problems of definitional uncertainty, inconsistent remedies, weak deterrence and litigation risk, spurred by the absence of confidentiality safeguards in court proceedings. The study uses a doctrinal and comparative approach and contends that the current reliance of India on a common law approach, based on an ad hoc, employer-employee paradigm, is insufficient for an economy that is innovative, based on a digitally networked economy, marked by high labour mobility and cross-border data flows. It's the need of the hour for a codified definition and protection of a sui generis trade secrets statute that strikes balance between interest of the owner and the mobility of the employees, competition and public interest while bringing India's innovation protection regime in line with international best practice and investor, start up and research-intensive industries' confidence.

[1] Shivam Kumar, LLM Student, Chanakya National Law University

Introduction

The concept of innovation is key to the modern knowledge economy and its legal protection is traditionally linked to the legally protected regimes of IP: patents for inventions, copyright for creative expression, trademarks for brand identity and designs for aesthetic form. However, a considerable amount of commercially valuable innovation remains unused in the public domain entirely. It is not rare to see formulae, algorithms, customer databases, manufacturing processes, marketing strategies, negative know-how and unpatented research data protected by secrecy, rather than disclosure-based monopolies. Such intangible assets are referred to as trade secrets. A trade secret does not give a monopoly for a period of time, as a patent does, but in principle it can last forever as long as it remains a secret, like the formula for Coca-Cola[2]. This is particularly appealing to industries in which the rate of innovation exceeds the time it takes to get a patent approved, or where the innovation is not patentable subject matter, or where disclosure would compromise competitive advantage. In India's booming, start-up and information-technology, pharmaceutical, and manufacturing industries, trade secrets are often the only or primary means of protection for commercially sensitive innovations.

Even though this is practically significant, there is no specific trade secrets law in India. Protection is gathered from the general law of contract, the equitable doctrine of breach-of-confidence, the protection of compilations under the copyright law, protection in the Information Technology Act, 2000 and, in extreme cases, the criminal law. It then critically assesses the Report No. 289 of 2024 of the Law Commission of India around Trade Secrets and Economic Espionage and the annexed Draft Protection of Trade Secrets Bill, 2024[3], in comparison with the Defend Trade Secrets Act, 2016 of the US[4] and the EU's Trade Secrets Directive. It also does not align with India's TRIPS commitment under Article 39(2) of the TRIPS Agreement that the member states are to provide legal possibilities for preventing disclosure of undisclosed information that has a commercial value to, acquisition by, or use by others without consent of the rights holder, which is in conflict with honest commercial practices[5].

[2] See World Intellectual Property Organization, Trade Secrets, https://www.wipo.int/en/web/trade-secrets.
[3] The Protection of Trade Secrets Bill, 2024 (Draft), annexed to Law Commission Report No. 289
[4] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.
[5] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

Lack of a defined trade secrets law in India has legal uncertainty for both employees and employers. A combination of contract, equity, copyright and criminal law principles was not intended to protect confidential information, which leads to uncertain results in court, limited remedies for aggrieved parties, and poor protection for confidential information in today's digital and mobile economy. The central problem tackled by this article is if the current patchwork of common-law and statutory provisions of India is sufficient to safeguard innovation through the use of trade secrets and what amendments are required to ensure that the Indian regime matches international standards and domestic innovation policy objectives, in particular in the form of the draft Protection of Trade Secrets Bill, 2024.

Conceptual Framework: What Is A Trade Secret?

There is no definition of a 'trade secret' in Indian laws. The meaning of the term, however, has been assembled judicially, most often in employer-employee conflicts. The Delhi High Court in the matter of *American Express Bank Ltd v Priya Puri*[6] has defined a trade secret as something which an employee holds during the course of the employment which thereby is protected and confidential and ought not to be known to others in the interest of the employer and notes that it may be a 'formula, technicalities of know-how or any business method which may be adopted by an employer which may be unknown to others. This distinction between the protected use of information and the general skill, experience, and know-how of an employee that the employee is free to use after the employment relationship ends is critical, and can explain how the court has been able to balance the need to protect such information with an employee's rights of earning a living.

The Bombay High Court, in the case of *Bombay Dyeing and Manufacturing Co Ltd v Mehar Karan Singh*[7], went further and laid down a multi factor test, taking into consideration the factors namely knowledge of the information outside business, knowledge of the information to the employees regarding the business, the precautions taken by the holder to guard the secrecy of information, the weight of information to the holder as compared with other businessmen; effort and expenditure required to develop the information; and the scope where the information can be acquired or duplicated by others easily. Applying this test, the court recognized that the customised software and manual which had been developed at substantial cost was a trade secret, but that discussions in the boardroom and general business strategy

[6] Am. Express Bank Ltd. v. Priya Puri, (2006) III L.L.J. 540.
[7] Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh, (2010) 112 Bom. L.R. 375

were not. The court emphasized that what it recognized as a trade secret had to be created at significant expense and that it could not simply be an employer's unilateral declaration that something was 'confidential'.

This multi-factor concept of judicial development, though very broad, is alike to the internationally accepted concept in Article 39(2) of TRIPS[8] which covers information that (a) is secret, (b) commercially valued, (c) person lawfully in control of the information has taken the reasonable steps to keep it secret. This tripartite approach is expressly incorporated into the draft Protection of Trade Secrets Bill, 2024[9], which defines the trade secret that is not known generally or otherwise easily accessible to the public, has economic value that is derived from the fact that it is not generally known or readily accessible by others, has resulted from the application of reasonable measures for the maintenance of its secrecy; and disclosure of which could be detrimental to the position of the person to whom the information is attributable.

One of the recurring challenges that one faces in Indian jurisprudence is the difference between the term 'trade secrets' and the larger category of ‘confidential information'. Others use the terms interchangeably; still others consider that trade secrets constitute a limited class of confidential information, only that which is of more or less technical or commercial importance, as opposed to normal internal letters or information that is otherwise commonly or generally known in the business. This boundary is not clearly defined by statute, which adds to uncertainty in the outcome of disputes.

Trips And Others: Sight Over The International Agreements

India is a founding member of the World Trade Organization (WTO) and is therefore a member of the TRIPS Agreement, which under Article 39, obligates the countries to provide protection against unfair competitions under Article 10bis of the Paris Convention[10], which covers the protection of the undisclosed information therein. Article 39(2) does not require a legislation to take a particular shape[11]; it leaves to the discretion of member states to protect the trade secrets by means of unfair competition law, by contract law or by a special legislation as long as the substantive threshold of protection is fulfilled. This obligation has been met in India, in

[8] TRIPS Agreement, supra note 4.
[9] Trade Secrets Bill, 2024, supra note 5, cl. 2(f).
[10] Paris Convention for the Protection of Industrial Property art. 10bis, Mar. 20, 1883, as revised at Stockholm, July 14, 1967, 828 U.N.T.S. 305.
[11] TRIPS Agreement, supra note 10.

a composite common-law fashion, but the effectiveness of this common-law approach, in terms of remedies, deterrence, and procedural safeguards, is not uncontested.

The EU Trade Secrets Directive introduces a harmonization of the definition of a trade secret, which is materially very close to the definition under Article 39(2) of TRIPS[12], and also provides for procedural measures to ensure confidentiality of the trade secret in court proceedings, such as the need to limit access to documents, conduct closed court hearings and ensure the confidentiality of court personnel. This procedural aspect directly subverts the one of the most important practical deterrents against litigation in India, namely the requirement for the claimant to provide the very information that it is trying to defend in order to plead and prove the case in open court.

Trade Secrets Through Domestic Regulatory Lenses

The American and European experience shows that the codification of a principle does not necessarily mean the elimination of flexibility, indeed, the specification of a principle and the possibility of adapting remedies and procedures to fit the specific case can yield a more predictable and better enforced system than one derived solely from general contract and equity principles. If there is no specific statute to protect trade secrets, at least five different sets of Indian law have been invoked by the courts to achieve this goal, but they are not all equally effective. The following are comparative models to inform the recommendations that are advanced in Part VIII of this article.

a. <u>The Indian Contract Act, 1872</u>

In Indian scenario, the trade secret protection is mostly based on a contractual basis through confidentiality clauses in employment and commercial contracts. But Section 27 of the Act, 1872 vitiates any agreement to the contrary, except under a very limited statutory exemption for the sale of goodwill[13]. The Indian courts have repeatedly ruled that post-employment non-compete covenants will not be upheld under Section 27, but confidentiality clauses that only restrict the disclosure or use of confidential information of the employer (and not prevent the recipient from working at all) will be enforceable as they do not constitute a restraint of trade in the statutory sense. This separation, which was upheld in cases involving non-solicitation clauses, means that an Indian employer can enforce workplace confidentiality, but not stop

[12] EU Trade Secrets Directives, 2016/943.
[13] The Indian Contract Act, No. 9 of 1872, s. 27.

competitors, is consistent with the constitutional protection of the freedom to engage in any profession or trade (Article 19(1)(g)[14]) and is subject to case-by-case judicial interpretation.

Equity: The Doctrine of Breach of Confidence- A contract does not need to expressly provide this but Indian courts have admitted such an obligation of confidence, which is enforceable through the mechanism of an injunction. The Delhi High Court in *Diljeet Titus v Alfred A Adebare*[15] had ruled that the duty of confidentiality might exist without a contract between the parties, based on the relationship that the parties had, and could be imposed on the former associates of a law firm who tried to access the data of their client while being associated with the firm. This equitable jurisdiction will supplement the contract law and a third party who is the defendant, is not in privity of contract with the trade secret holder, will also be bound by the obligation of confidence in *Zee Telefilms Ltd v Sundial Communications Pvt Ltd* before the Bombay High Court.[16]

b. The Copyright Act, 1957

In regard to the confidential information contained in a compilation, like a client database, catalogue or manual, Indian courts have often relied on the "sweat of the brow" doctrine of copyright, which applies to a compilation that reflects the application of labour, skill and judgment in its selection and arrangement, on the basis of the early decision in *V Govindan v E M Gopalakrishna Kone*[17]. In *Burlington Home Shopping Pvt Ltd v Rajnish Chibber*[18], Delhi High Court stated that a customer database compiled after spending time, money and manpower was an original literary work protected by copyright and prevented one of its former employees from using a database that was substantially similar. Diljeet Titus also acknowledged the copyright of a specific list of customers as well. But this approach does not confer any copyright on the confidential information itself, which courts have since clarified, in Navigators Logistics Ltd v Kashif Qureshi[19], are not eligible for copyright protection; this leaves an important class of routine but commercially sensitive data unprotected by this means.

c. The Information Technology Act, 2000

[14] Indian Const. art. 19, cl. 1(g).
[15] Diljeet Titus, Advocate v. Alfred A. Adebare, (2006) 130 D.L.T. 330.
[16] Zee Telefilms Ltd. v. Sundial Commc'ns Pvt. Ltd., (2003) 5 Bom. C.R. 404.
[17] V. Govindan v. E.M. Gopalakrishna Kone, AIR 1955 Mad 391
[18] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, 1995 IV AD (Delhi) 732
[19] Navigators Logistics Ltd. v. Kashif Qureshi, 2018 SCC OnLine Del 10944

Sections 43 and 66 of the IT Act, 2000[20], make it an offence to access with the intention of downloading any data from a computer system or to access a computer system to extract any data, if the data is stored or transmitted in electronic form, and Section 72 makes it an offence to breach confidentiality by accessing electronic records under statutory powers[21]. These provisions have been applied to prevent computer data being stolen, but are focused on unauthorised computer access, not on the misappropriation of trade secrets in general, and do not provide a detailed civil remedy framework for the misappropriation of trade secrets.

Precedents Framing Trade Secrets Concepts

A precedent-setting decision came up in mid-90s by the Delhi High Court and is often termed to as the beginning of trade secret jurisprudence in India. The court ruled that a list of customers compiled by a past employee "in the course of his employment" was an original literary work that is subject to copyright umbrella, considering the facts that the information in the list was unoriginal or publicly ascertainable. It created an important principle, namely that the function of aggregation and organisation of otherwise ordinary information can itself be considered a protectable subject-matter, which remains relevant for today's data-driven companies.[22]

Further ruling *American Express Bank Ltd*[23] provided Indian law's most often-quoted definition of trade secret. It was also important, however, for what it didn't protect, the court rejected the former banking employee's attempts to prevent him from relying on general banking knowledge and skill, or from approaching customers who were free to choose their bank, ruling that customer names, addresses and portfolio information, which were confidential in relation to the banking relationship, could not be monopolised to the extent of restricting any customer's freedom of choice. It's a fine balancing act that is playing out throughout this field, that is, balancing the rights of customers and the mobility of employees with the ability to maintain genuine secrecy.

The clash of departing lawyers at a law firm established that confidentiality is not required by contract, but rather is inherent in the nature of the professional relationship of trust, and that confidentiality may exist with regard to compiled client information even if the facts themselves are not particularly unusual. The decision of *Diljeet Titus* [24] is important because of

[20] The Information Technology Act, No. 21 of 2000, ss. 43, 66.
[21] *Id,* s. 72.
[22] Burlington Home Shopping v Rajnish Chibber 61 (1995) DLT 6.
[23] American Express Bank Ltd v Priya Puri (2006) SCC OnLine Del 638.
[24] Diljeet Titus v Alfred A Adebare, 130 (2006) DLT 330.

its attempt to be expansive in its protection of professional service providers, a sector that is not well-served by patent or trademark law, but also because of the doctrinal unction of the court's reliance on copyright as a substitute remedy for a trade secret cause of action, which was grounded in the plaintiff's authorship of the database, instead of a de novo property right claim.

Bombay Dyeing and Manufacturing Co Ltd[25] provides the most analytically mature judicial treatment of trade secrets in India, and sets out the six-factor test. Its split decision protects the proprietary software and manual, but not the boardroom discussions on the strategy, shows that the judges are willing to draw fine lines between what is truly secret but has commercial value in terms of technological information and what is more business planning and thus less secret. Its bifurcated holding protects proprietary software and manual, but not boardroom strategy discussions which illustrates judicial willingness to make fine distinctions between technological information that is truly secret but commercially valuable, and business planning, which is less secret.

This latter decision is helpful to clear up any misimpression that Burlington and Diljeet Titus protect all business databases. The Delhi High Court[26] found that a customer database created by a mere mechanical process does not enjoy any copyright protection and separately found that if a customer database is created by a company, the company must identify the human author to prove ownership of the copyright. The ruling reveals the structural flaws of any reliance on copyright to serve as a replacement for a trade secret action: while copyright could cover the expression and arrangement of the data, it doesn't encompass the confidentiality of the data or the value of the underlying information, and so mundane but sensitive information, such as pricing sheets, vendor terms, operational factors, can be lost between the copyright originality barrier and the lack of a standalone trade secret action.

Scrutinising The Regulatory Gaps And Inconsistencies

The statutory provisions in the Indian arena shows certain limitations and gaps which finds out the vulnerability of the Trade secrets regulation. There is no statutory definition of trade secret, so courts deal with trade secret protection on a case-by-case basis. This leaves businesses with a limited amount of guidance to go on when designing a confidentiality procedure ex ante. Remedies are mostly confined to injunctions. Civil remedies are not well deterrent where there

[25] Bombay Dyeing and Manufacturing Co Ltd v Mehar Karan Singh, 2010 (112) BomLR 375.
[26] Navigators Logistics Ltd v Kashif Qureshi (2018) 254 DLT 307.

is no specific damages regime. In fact, India has no specific criminal law on trade secret misappropriation, compared to that in the United States (Economic Espionage Act)[27] and China (Anti-Unfair Competition Law).[28] Doctrinally it is a strain and weak prosecution to rely on general penal provisions for tangible property. Enforcement necessitates that claims must be made in public. Without such protective orders and sealed-record regimes that exist in the US or EU, this litigation paradox is a deterrent for enforcement, particularly for resource constrained start-ups. Precisely, when one see ticks, he sees that the law is the result of problems with the departing worker, leaving non-employment scenarios underdeveloped, such as competitor misappropriation, cyber-intrusion, joint ventures, and cross-border supply chains. Lastly, modern assets, such as algorithms, AI training data, cloud processes, are easily stolen and cannot be always be protected by bilateral contracts. This is an ancient common-law system that's poorly equipped to serve the digital world.

Towards Codification: The Protection Of Trade Secrets Bill, 2024

The Department of Legal Affairs, after detailed consultation with the judiciary, academia, industry and government departments, submitted a report to the 22nd Law Commission of India, which in 2024, presented its Report No. 289 titled 'Trade Secrets and Economic Espionage'. The Report suggests the adoption of sui generis legislation and proposes an annexe to the Report, namely a draft Protection of Trade Secrets Bill, 2024.

The Draft Bill includes the following key features:

The 'trade secret' covered by clause 2(f)[29] defines it as ‘information that is not known generally or easily accessible, has economic value because of its secrecy realm, has been taken to be the subject of reasonable measures designed to avoid disclosure and whose disclosure could be detrimental to the owner'.

The concepts of unfair competition and misappropriation that underlie a common law approach to protecting a trade secret are also based on breach of a common law duty of confidence principle, and that doctrine is left unchanged to maintain a sense of doctrinal continuity with previous case law, while providing statutory structure. Allowing for compulsory licensing and compulsory government use of trade secrets within specific public-interest conditions, as would also be the case with patents. Protection of the whistle-blower, such that disclosures for

[27] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488.
[28] Fan Bu Zhengdang Jingzheng Fa, Anti-Unfair Competition Law, (2019).
[29] Trade Secrets Bill, 2024, supra note 5, cl. 2(f).

disclosing illegal activities are not treated as misappropriations and therefore protected from liability.

What Can We Underline Through These Progresses?

The draft Bill is a major conceptual improvement as it would, for the first time, provide a single statutory definition for Indian law, codify the equitable and contractual principles that have been formulated over the years by courts, and add confidentiality-preserving procedure. It explicitly rejects the property concept of a trade secret, with a view to avoiding the possibility of a trade secret claim being used against a legitimate competitor or to prevent an employee from departing from a firm. Its explicit rejection of the idea of a trade secret as a property is a deliberate and defensible policy choice, and one that aims to avoid the possibility of a trade secret claim being used against a legitimate competitor and to prevent an employee from leaving a firm. Meanwhile, the Bill's failure to include specific criminal penalties and the inconsistencies between compulsory licensing and the very secrecy that makes a trade secret valuable are areas for valid concern. The Bill is currently in draft status, and has not been introduced in Parliament, so it is unclear how it will change or be amended during the parliamentary process and what form it will take when it eventually becomes law.

Conclusion

In the last 30 years, India's judiciary has fashioned a remarkably consistent field of trade secret law from its doctrinally disconnected sources like contract, equity and copyright while always keeping an eye out for genuine commercial secrecy without stifling employee mobility, customer choice, or competition. The decisions of the above-mentioned tagged case laws are a good example of the ingenuity of the judges in the absence of any legislation. But there is no substitute for codification when it comes to ingenuity. The resulting exposure of the Indian innovator to definitional uncertainty, inconsistent remedies, weak deterrence, lack of meaningful criminal sanctions, and perhaps most damaging to a litigation averse business world the paradox of being required to disclose a secret in order to protect it leaves them vulnerable. The rationale for establishing a codified, sui generis trade secrets regime, as recommended by the 22nd Law Commission and embodied in the draft Bill on Trade Secrets protection of 2024, is all the stronger in the era where India is aspiring to become a global start-up hub, research and development, and digital innovation hub. Such a law thoughtfully designed in light of the comparative histories of the US and the EU, and mindful of India's constitutional dedication to the freedom of trade and employment would be a stark and overdue

move to bring India's innovation protection system more into line with the requirements of a modern knowledge economy.