INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

TRADE SECRET PROTECTION IN INDIA: THE NEED FOR LEGISLATIVE REGIME.

AUTHORED BY - AANCHAL BARY
Student at NMIMS KPMSoL

1. Abstract

One of the most significant and legally protected types of intellectual property (IP) in India is trade secrets. Other types of IP like patents, copyrights, trademarks- they are governed by their own dedicated statutory law however trade secrets in India is dependent on largely unfragmented combination of general principles of laws, equitable doctrines and contractual mechanism.

This paper critically examines and studies the competence of India's prevailing legal system for the protection of confidential and secrets of business information and also at the same time argues that the absence of legislation creates systemic vulnerability of Indian enterprises, blocks foreign investments, and leaves India non-compliant with the spirit, if not the letter of article 39 of the TRIPS agreements.

Keywords- trade secrets, confidential information, TRIPS agreements, Defend Trade Secrets Act,

2. Introduction

In the recent knowledge economy, the value of a product increasingly resides not in the physical form but also in the non-physical i.e. intangible ones- For example customer databases, manufacturing formulation, proprietary algorithms, Business strategies, recipes etc. Trade secrets also defined as commercially valuable material are protected by secrecy rather than formal registration, has emerged as a dominant instrument of IP protections.[i] A trade secret is proprietary info about a business that provides a competitive edge in the marketplace. For instance, the recipe for Coca-Cola has been kept a secret since 1891. When we talk about India, the country lacks a dedicated legal armor for trade secrets. Proprietors of secret information often go through an extensive patchwork of contractual obligation, equitable principles, general

ISSN: 2582-6433

legal provisions in statutes enacted for broad purposes. All of this in its entirety results in uncertainty, inconsistency and inadequate deterrence against misappropriation.

While there exists a lack of law, the stakes are still substantial as India's it services contributes a lot to GDP and it's pharmaceutical industry is the world's 3rd-largets by volume and both the sectors rely heavily on trade secrets (secrets—source code, process know-how, clinical data, client methodologies). And with increasing misappropriation risks due to AI etc the need for a statute has become a practical emergency.

3. Research questions

This paper deals largely with the 2 utmost important questions-

1. Is the already existing legal framework adequate to protect trade secrets in this economy?
2. What can India learn from us defend trade secrets act, 2016 in designing a dedicated legislation?

4. Findings

The existing position of Trade secret protection in india

A. Lack of dedicated legislation

India is a noticeable outlier among big economies in lacking a dedicated trade secrets statute. The 22nd Law Commission of India has likewise acknowledged this inadequacy: in a report released on 5 March 2024, it recommended a sui generis statute and annexed a draft Protection of Trade Secrets Bill, 2024.

Courts have used the English theory of breach of confidence as the main means of protecting trade secrets in the absence of a legislation. According to the concept, a plaintiff must prove three things, as stated in the 1969 decision of Coco v. A. N. Clark (Engineers) Ltd.

(i) There was actual or threatened illegal use causing harm;

(ii) the material/information was provided in circumstances requiring an obligation of confidence; and

(iii) the information possessed the required character of confidence.

While workable in straightforward cases, this framework suffers from the significant limitations as it is remedially weak as the courts only award injunctions, damages, with

ISSN: 2582-6433

no disgorgement of profits or exemplary damages.[ii]

B. Section 27 of contracts act

One of the most deliberating limitation of Indian framework is section 27 of the Indian contracts act, 1872- it renders "every agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind" void[iii]. In simple terms, the law doesn't allow employers to stop previous employees from working elsewhere after leaving the company. Indian courts have also applied this provision with rigidity to invalidate post-employment non-compete and non-disclosure agreements even when they are intended to protect genuine trade secrets or confidential business information.

The post-employment non-disclosure agreements deals with the idea that even after an employee leaves the company, the employer wants them to not reveal confidential information like customer lists, secrets formulas, pricing strategies etc. However if such clauses are drafted too broadly to prevent someone from working, courts may refuse to enforce them as it goes against section 27.

C. Judicial decisions

Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber (61 (1996) DLT 6) is a significant Indian trade secret decision. The court applied the springboard doctrine and iterated that a customer database constituted a trade secret by the virtue of the effort, skill and investment in its compilation. The court prevented a former employee from exploiting copied data for competitive advantage.

American Express Bank Ltd. v. Priya Puri ((2006) 110 DLT 308) demonstrates the framework's limitation. The Delhi High Court refused an injunction against a former Relationship Manager who had taken client information to a competitor, holding that the plaintiff had failed to identify with precision which specific information constituted a protectable trade secret as opposed to general professional skills. The verdict showcases the critical consequence of not having a statutory definition: courts must make ad hoc, unpredictable distinctions between protectable secrets and unprotectable expertise.

D. Other Statutory Provisions

Peripheral protection is provided by many legislation. Sections 43, 66, and 66B of the Information Technology Act of 2000 provide criminal responsibility for illegal

ISSN: 2582-6433

computer access and data theft; however, they do not cover trade secrets per se. Sections 37–38 of the Specific Relief Act of 1963 permit perpetual injunctions. Directors are subject to secrecy requirements under Section 166 of the Companies Act, 2013. None of these rules define 'trade secret,' establish civil remedies calibrated to trade secret misappropriation, or impose criminal sanctions similar to those available in the US or EU. At most, the framework provides unintentional protection.

5. Comparative study, US framework

A. The Defend Trade Secrets Act, 2016

DTSA was enacted on May 11th, 2016 and it denotes the most comprehensive statutory trade secret regime in any major jurisdiction. A federal private civil cause of action for trade secret misappropriation was created by it thereby ending the long realiance of divergent state laws under uniform trade secrets acts.

All forms and types of economic, business, scientific, technical, or engineering information—including designs, formula, methods, prototypes, techniques, processes, or codes—are considered trade secrets under the DTSA as long as the owner has taken reasonable precautions to keep the information confidential and the information derives independent economic value from its secrecy.

According to the DTSA, "misappropriation" includes:

(i) obtaining a trade secret by someone who knows or has reason to believe that it was gained improperly; and

(ii) disclosing or using a trade secret without permission by someone who got it improperly or in violation of a duty of confidence.

'Improper means' explicitly includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, and espionage through electronic means. The explicit inclusion of electronic espionage—absent from Indian law—is critically important in the digital context.

B. Civil remedies

The DTSA provides a comprehensive suit of civil remedies which is very contrasting to the India's limited equitable toolkit. Courts may award injunction to prevent any possibility of, or actual misappropriation, while keeping in mind an important carve out preventing injunctions that conflict with applicable state law or that solely prevent a person from entering into an employment relationship, as this preserve labour mobility

ISSN: 2582-6433

while also protecting genuine confidential secrets.

Damages are calculated as the greater of- actual loss which is cause by misappropriation + unjust enrichment which is not captured in the actual loss; or an acceptable and reasonable royalty for the period of unauthorized use.

Very importantly, in cases of malicious and willful misappropriation, courts may award exemplary damages which can go up to twice the actual damages awarded, this also creates a powerful deterrent entirely absent from Indian law.[iv]

C. The ex-parte seizure order

This is available in special cases where a court determines that an injunction would be insufficient because the defendant would avoid, evade or not comply with it and thus the harm to the applicant of denying the order outweighs the harm to the defendant. These orders allow law enforcement to confiscate items that are required to stop the trade secret from spreading. This remedy has no counterpart in Indian law and is specifically tailored to the digital environment, where a stolen algorithm or customer list may be sent anywhere in the world in a matter of seconds.

D. Economic Espionage Act:

The DTSA supplements the Economic Espionage Act (EEA) of 1996, which governs criminal trade secret protection in the United States. The EEA establishes two specialized federal criminal offenses: theft of trade secrets, which attracts a maximum sentence of 10 years in prison and equivalent fines, and economic espionage, which is defined as misappropriation for the benefit of a foreign government and carries a maximum sentence of 15 years in prison and fines of up to $5 million per person.[v] A fine of up to $5 million USD, or at least three times the value of the stolen business secret, might be applied on organizations. India lacks a comparable criminal code since trade-secret-specific offenses were not included in the Bharatiya Nyaya Sanhita, 2023, which superseded the IPC. This was a lost legislative opportunity.

E. Protections for Reverse Engineering and Whistleblowers

Important restrictions are included in the DTSA to avoid overprotection. It expressly grants whistleblower protection, meaning that a person who confidentially divulges a trade secret to a government official or lawyer in order to expose a suspected legal breach would not be held accountable. This exemption, which is not included in Indian

ISSN: 2582-6433

law, guarantees that trade secret protection cannot be used as a weapon to stifle the revelation of corporate misconduct. Additionally, the DTSA protects the right to reverse engineering: independent research or development using appropriate methods, such as reverse engineering of legally obtained goods, does not amount to misappropriation.

6. Needs for a dedicated Indian trade secret act

The comparative analysis makes the shortcomings of India's framework unquestionably clear. A legislative solution is required for seven structural flaws.

First, systemic uncertainty results from the lack of a formal definition. Businesses are unable to organize their information security procedures around a trustworthy legal norm since courts in Chennai, Mumbai, Delhi, and Kolkata have adopted different formulations. This ambiguity would be eliminated by a law that offers a precise, technology-neutral definition based on the DTSA.

Second, employers are left without effective post-departure protection due to the Section 27 issue. The balance between employer protection and employee mobility would be adjusted by a tailored law reform that permits limited, proportional covenants particularly aimed at specified trade secrets, as opposed to general non-compete agreements. A paradigm is provided by the DTSA's employment-mobility carve-out, which protects true secrets without preventing full labor market participation.

Third, misappropriation is still economically rational even after it is found since there are insufficient civil remedies, especially exemplary damages and disgorgement. A positive anticipated value for bad-faith actors is obtained by subtracting the estimated compensatory losses of a fraction of the USD 5 million in stolen data from the litigation expenses. Deterrence would be restored by exemplary damages calculated to the worth of the stolen secret.

Fourth, a crucial gap is the lack of criminal sanctions. India's ongoing placement on the Priority Watch List was expressly attributed to its insufficient trade secret protection, especially the lack of criminal penalties, according to the US Trade Representative's 2023 Special 301 Report. As the Economic Espionage Act shows, criminal culpability produces deterrent that civil litigation cannot match, especially against sophisticated, state-sponsored, or organized misappropriation

ISSN: 2582-6433

Fifth, when digital theft is about to occur, courts are helpless due to the lack of ex parte seizure procedures. Once divulged, trade secrets communicated electronically cannot be retrieved; thus, the legislation must provide for emergency interception prior to dissemination. There is an urgent need for a legislative ex parte seizure process with suitable abuse prevention measures.

Sixth, the innovation ecosystem is let down by the framework. India's 40th-place score in the Global Innovation Index 2023 is indicative of fundamental IP flaws. When assessing India as a location for R&D or production, foreign technology businesses need to take the legal sensitivity of their sensitive information into consideration.

Seventh, the deficiency has become more severe due to the development of artificial intelligence. Large language models, recommendation algorithms, and computer vision architectures are examples of AI systems that are incredibly valuable trade secrets. They may have spent years developing their model weights, training data, and fine-tuning techniques. A statute that specifically incorporates algorithmic and AI-related information under the concept of "trade secret" is crucial since India's common law system lacks a logical foundation for resolving disputes about AI-related secrets.

7. Conclusion

India's current trade secret regime is essentially insufficient, as this research has shown. Indian businesses—as well as the foreign investors they aim to draw in—are deprived of the dependable, calibrated legal protection that a knowledge economy requires due to the reliance on common law breach of confidence principles, a Contract Act that thwarts post-employment protection, and statutes created for other purposes. Even while the judicial method is innovative and generally compassionate, it cannot offer the comprehensive remedies, criminal deterrent, and definitional certainty that only a statute can.

A specific Indian Trade Secrets Act should be passed by Parliament, with precise exclusions, extensive civil and criminal consequences, and statutory definitions. To allow for specific, reasonable post-employment covenants aimed at safeguarding identifiable trade secrets, Section 27 of the ICA, 1872 should be modified. An economic espionage clause should be added to the Bharatiya Nyaya Sanhita, 2023, along with other criminal offenses relevant to trade secrets. Exclusive jurisdiction over trade secret disputes should be granted to designated

ISSN: 2582-6433

commercial courts, together with procedural guidelines that guarantee the confidentiality of disputed secrets. To eliminate cross-border enforcement gaps, India should ratify international accords and develop bilateral trade agreements with clear trade secret enforcement clauses. An Indian Trade Secrets Act is long overdue.

8. References

1. Books and Articles Agarwal, Siddharth, 'Trade Secrets in India: The Need for Statutory Reform,' 13 J. Intell. Prop. L. & Prac. 192 (2022).
2. Indian contracts act, 1872
3. Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber (61 (1996) DLT 6)
4. American Express Bank Ltd. v. Priya Puri ((2006) 110 DLT 308)
5. Bone, Robert G., 'A New Look at Trade Secret Law: Doctrine in Search of Justification,' 86 Cal. L. Rev. 241 (1998).
6. Kapoor, Aditya, 'Employee Mobility and Trade Secrets: Rethinking Section 27,' 22 NLU Delhi L. Rev. 89 (2023).
7. Lakshminath, A., 'Confidential Business Information and the Law in India: The Case for Legislative Reform,' 42 Delhi L. Rev. 1 (2020).
8. Lemley, Mark A., 'The Surprising Virtues of Treating Trade Secrets as IP Rights,' 61 Stan. L. Rev. 311 (2008).
9. Pooley, James, 'Trade Secrets: The Other IP Right,' 5 WIPO Magazine (2013).
10. Singh, Kavya & Namita Srivastava, 'Reforming Trade Secret Law in India: A Comparative Perspective,' 11 NUJS L. Rev. 1 (2024).
11. Varadarajan, Deepa, 'Trade Secret Settlements and the Public Interest,' 103 Geo. L.J. 1297 (2025).
12. Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, 1869 U.N.T.S. 299, art. 39.
13. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016, 2016 O.J. (L 157) 1.
14. Jack E. Staub, Intellectual Property Rights, Genetic Markers, and Hybrid Seed Production, Journal of New Seeds, 10.1300/J153v01n02_04, 1, 2, (39-64), (2008).

[i] James Pooley, Trade Secrets: The Other IP Right, 5 WIPO Magazine (2013)
[ii] Robert G. Bone, A New Look at Trade Secret Law: Doctrine in Search of Justification, 86 Cal. L. Rev. 241 (1998).

ISSN: 2582-6433

[iii] Indian contracts ACT, 1872
[iv] Deepa Varadarajan, Trade Secret Settlements and the Public Interest, 103 Geo. L.J. 1297 (2025).
[v] 18 USC §§ 1831–1832 (1996).