NEED FOR A SUI GENERIS LEGISLATION ON TRADE SECRET PROTECTION - A CRITICAL AND COMPARATIVE APPROACH

Harinibai. R, SASTRA Deemed University.

Poorna K, SASTRA Deemed University.

ABSTRACT

In the contemporary digital-driven world, intangible assets such as trade secrets have emerged as an important strategy driving businesses and giving them a competitive edge. Unlike other forms of IPR such as patents, copyrights, and trademarks, the trade secret still lacks a standalone legislation for its protection and are currently governed under different legislations such as the contracts act, IT act, companies act and equity principles. This piecemeal approach has created a legal certainty, weak enforcement mechanism and limited remedies leading to exposure of companies especially startups and MSMEs to data theft and misappropriation especially through modern means such as phishing, hacking, insider leaks, cyber-attacks etc.,

The 289th Law commission Report recommended a dedicated trade secret protection Act but failed to include analysis on how modern cyber threats could be combatted.

This paper reassesses the need for a sui generis legislation through a comparative study of regimes in the United States, European Union, United Kingdom, China, and Japan, while analyzing TRIPS obligations under Article 39 and recent developments including the 289th Law Commission Report (2024). The paper further integrates whistleblower-protection models, especially the U.S. DTSA framework, to propose balanced mechanisms that protect trade secrets while preserving public interest and whistleblower rights. It argues that India must adopt a dedicated, technology-responsive statute incorporating confidentiality safeguards, cyber-crime deterrence, whistleblower immunity, and exemplary compensation to encourage compliance, investment and fair competition.

Keywords: trade secrets, sui generis legislation, whistleblower immunity, cyber theft, TRIPS Article 39.

Introduction

At the Global level, trade secret theft is still a hard-to-determine cost because companies might not even know that their IP has been stolen, nor are businesses motivated to report their losses when found. Since IP piracy continues to be difficult for companies to identify, much less receive legal recourse for, their incentives are to depend increasingly on their own resources to hide trade secrets and decreasingly on patents that involve public disclosure.[1] New estimates place trade secret theft at between 1% and 3% of GDP, so the damage to the $18 trillion American economy is between $180 billion and $540 billion. In India, particularly because of the piecemeal law making, there is a legal uncertainty, which puts businesses and the IBM's Cost of Data Breach Report 2022 reported the average cost to Indian firms was INR 17.6 crore per incident (compared to INR 16.5 crore in 2021)[2]. Also. India repeatedly features in the top five nations that are attacked by cyber-attacks around the worlds, adding to this weakness.[3]

Globally, more than 40 nations have adopted a *sui generis* trade secret laws, offering more explicit, enforceable protections. The European Union Directive 2016/943 standardized such protection in 27 member states, whereas nations such as the US, China, and Japan have enhanced criminal enforcement provisions to prevent economic espionage. Embracing these issues, the 22nd Law Commission of India recently tabled a complete Protection of Trade Secrets Bill, 2024, an essential step towards bringing India in line with international best practices and meeting the specific issues arising due to the contemporary digital era.

Research Methodology

This study uses a doctrinal and comparative approach to critically evaluate the Indian legal framework for protection against trade secrets. Primary sources of law such as statutes, judicial precedents, and international treaties like the TRIPS Agreement (Article 39) serve as the basis of analyzing India's existing fragmented regime of protection. Secondary materials like scholarly articles, law commission reports—particularly the 289th Law Commission Report—

[1] R. Mark Halligan, "Trade Secrets v. Patents: The New Calculus," Landslide, July/August 2010, http://www.americanbar.org/content/dam/aba/migrated/intelprop/magazine/LandslideJuly2010_halligan.authcheckdam.pdf

[2] Cost for Data Breaches Averaged Rs. 17.6 Cr. in 2022, Highest Ever: IBM Study, Bus. Standard (July 26, 2022), https://www.business-standard.com/article/companies/cost-for-data-breaches-averaged-rs-17-6-cr-in-2022-highest-ever-ibm-study-122072701127_1.html

[3] India Ranked Second in Global Cyber Attack Targets: Report, Times of India (Jan. 1, 2025), https://timesofindia.indiatimes.com/india/india-ranked-second-in-global-cyber-attack-targets-report/articleshow/116893292.cms

and legislative bills like the Trade Secrets Bill 2024 are examined systematically. The research contrasts India's approach with well-established sui generis laws and enforcement measures in the US, EU (Directive 2016/943), UK, China, and Japan. Analytical assessment identifies gaps in statutory definitions, enforcement, and remedies. Case law and policy reports add texture to this analysis by demonstrating real-world enforcement challenges and economic consequences. Through this doctrinal and comparative examination, the study finds gaps and recommends a technology-conscious, harmonized legislative scheme for India's socio-economic context.

- ***The Concept of Trade Secrets and the Rationale for Their Protection***

A trade secret can be generally defined as confidential commercial information which derives independent economic value from being generally unknown and for which the owner makes reasonable efforts to maintain secrecy. Such information can include formulas, processes, and technical knowledge on one hand to business information like customer lists, pricing, or marketing strategies on the other.[4] They need not be registered, unlike patents, copyrights, or trademarks; their worth lies solely in secrecy, which, lost once, cannot be regained.[5]

The economic and fair reasons behind protecting trade secrets lie in both of these. Economically, proper protection encourages investment in research and development, avoids wasteful duplication of effort, and enables cross-border technology transfer.[6] For startups and micro, small, and medium enterprises (MSMEs) — many of which are resource-constrained and unable to seek formal intellectual property registrations—trade secrets are often their greatest intangible asset, allowing them to compete with larger companies.[7] From a viewpoint of equity, employees', competitors', or hackers' misappropriation of such information amounts to unfair competition and destroys the legitimate interests of the owner. This principle gets its place in Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights

[4] World Intellectual Prop. Org., *Trade Secrets: The Hidden IP Right* (2023), https://www.wipo.int/web/wipo-magazine/articles/trade-secrets-the-hidden-ip-right-40225.
[5] IAM Media, Cyril Abrol, *A Closer Look at Protecting Trade Secrets in India as New Legislation Could Be on the Horizon* (Sept. 4, 2024), https://www.iam-media.com/article/closer-look-protecting-trade-secrets-in-india-new-legislation-could-be-the-horizon.
[6] World Intellectual Prop. Org., *IP Panorama Module 4: Trade Secrets* (2022), https://www.wipo.int/documents/d/business/ip_panorama_4_learning_points.pdf.
[7] Anand & Anand, *Trade Secrets 2025* (2025), https://www.anandandanand.com/news-insights/trade-secrets-2025/.

(TRIPS), which requires member states, including India, to safeguard undisclosed information against unfair commercial practices.[8]

Around the world, from the United States to the European Union, the United Kingdom, China, and Japan, there exist statutory regimes fully codified combining both civil and criminal forms of remedy. In India, on the other hand, the lack of a sui generis statute compels the use of a piecemeal framework involving contract law, equity, and industry-specific statutes, leaving companies open to insider thefts and cyber-enabled thefts.[9]

- ***Modes of Misappropriation and Disclosure of Trade Secrets***

Trade secrets by their nature are exposed to loss as soon as confidentiality has been violated. The 289th law commission report of India has already identified various forms of misappropriation like violation of contractual mandate, theft of papers by the employees etc. [10] Conventional risks include employee mobility, where the exiting employees take sensitive information to the competitors, and contractual violations, where non-disclosure or confidentiality arrangements are broken. [11] These risks have been recognized by courts, which in *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co*. held that there could be an obligation of confidence even after the termination of employment, even if there is no restraint on trade.[12]

In the internet age, however, exposure is not confined to human transgressions. Contemporary trade secrets are vulnerable to cyber intrusion, phishing, ransom ware, cloud storage vulnerabilities, and insider cyber leakage. [13] Reports indicate that Indian businesses are ranked among the global leaders that are attacked via cyber-attacks, and such breaches are often undertaken for the purpose of stealing proprietary business information. [14] Unlike patents or trademarks, trade secrets are not registered with a government authority, making detection of theft difficult and remediation dependent on tracing misuse after the fact.

[8] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.
[9] Law Comm'n of India, 289th Report: *Protection of Trade Secrets* (2024).
[10] Law Comm'n of India, 289th Report: *Protection of Trade Secrets* 17–22 (2024).
[11] IAM Media, Cyril Abrol, *A Closer Look at Protecting Trade Secrets in India as New Legislation Could Be on the Horizon* (Sept. 4, 2024), https://www.iam-media.com/article/closer-look-protecting-trade-secrets-in-india-new-legislation-could-be-the-horizon.
[12] *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co.*, (1967) 2 S.C.R. 378 (India).
[13] World Intellectual Prop. Org., *Trade Secrets: The Hidden IP Right* (2023), https://www.wipo.int/web/wipo-magazine/articles/trade-secrets-the-hidden-ip-right-40225.
[14] PwC & Confederation of Indian Industry, *Cybersecurity in India: Securing the Digital Frontier* 11–14 (2022).

There is also a risk during litigation itself. Plaintiffs need to define their trade secrets adequately enough to seek relief, but over disclosure threatens to undermine the secrecy that generates value.[15] While some other jurisdictions use mechanisms like "confidentiality clubs" or sealed proceedings, India has no legislative tools to balance litigation disclosure with secrecy protection.

Accordingly, forms of disclosure now reach as far as conventional forms of violation (employee or contractual) and vectors of attack (cyber-attacks, AI scraping, data spying). The lack of explicit statutory protection exacerbates these vulnerabilities, emphasizing the imperative for a sui generis regime specific to India's developing digital economy.

- ***The Legal Vacuum: Current Framework Governing Trade Secrets in India***

India lacks a sui generis law specifically focusing on the protection of trade secrets. Business has to depend on a piecemeal combination of contractual, statutory, and equitable relief. It has resulted in uncertainty, uneven enforcement, and narrow deterrence, putting confidential information at risk.

Indian Contract Act, 1872 provides the basis to safeguard confidential information by non-disclosure agreements and confidentiality clauses. Courts generally enforce secrecy commitments but have always held wide-ranging post-employment non-compete clauses as being in contravention of Section 27, which declares contracts in restraint of trade to be illegal[16]. This role was reinforced in *Superintendence Co. of India v. Krishnan Murgai*, where the Supreme Court held that the protection of trade secrets should not go to the extent of unreasonably restricting an employee's freedom to trade.[17] And simultaneously, in *Niranjan Shankar Golikari v. Century Spinning*, the Court acknowledged that confidentiality duties can permissibly extend beyond the period of employment.[18]

Sectorial legislations complement contractual protection in restricted areas. The Information Technology Act, 2000 makes unauthorised access or copying of electronic records criminal, thus including theft of digital trade secrets. [19] Also, the Companies Act, 2013 imposes

[15] Factum Law, *Describing the Trade Secret in Your Plaint*, Mondaq (Apr. 30, 2021), https://www.mondaq.com/india/trade-secrets/1055284/describing-the-trade-secret-in-your-plaint.
[16] Indian Contract Act, No. 9 of 1872, § 27 (India).
[17] *Superintendence Co. of India (P) Ltd. v. Krishan Murgai*, (1981) 2 S.C.R. 453 (India)
[18] *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co.*, (1967) 2 S.C.R. 378 (India)
[19] Information Technology Act, No. 21 of 2000, § 43 (India).

obligations of business secrecy upon directors and officers, while the SEBI Act, 1992 prosecutes insider trading in unpublished price-sensitive information. [20] There are even criminal sanctions under the provisions of the Bharatiya Nyaya Sanhita, 2023, which punish criminal breach of trust or theft of property, albeit not specifically designed for contemporary trade secret misappropriation.[21]

Lacking statute, Indian courts have bridged gaps by invoking the equitable principle of breach of confidence, evolved out of English common law. In *Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh*, the Bombay High Court established tests for determining trade secrets, such as secrecy, commercial value, and efforts made by the owner to keep information secret. [22] Yet, enforcement continues to be ad hoc, and plaintiffs are frequently subjected to the irony of being required to disclose the same information they wish to conceal during suit.[23]

This disjointed strategy, without consistent definitions, statutory redressal, and procedural protection, has made Indian companies—start-ups and MSMEs especially—prone to insider spills and cyber-facilitated appropriation. The legal void also erodes investor confidence and makes India's negotiating position in trade talks even more difficult, with developed partners always insisting on enhanced protection of trade secrets.

- ***TRIPS mandate:***

Article 39 of the TRIPS Agreement mandates member States to protect undisclosed information and regulatory data against unfair commercial use and unauthorized disclosure. While TRIPS does not require a specific legislation, India complies with these obligations through a combination of common law principles, contract law, and equitable doctrines that safeguard confidential business information such as trade secrets, client lists, technological know-how, and formulae. Indian courts have consistently recognized breach of confidence as an actionable wrong, and protection is typically enforced through non-disclosure agreements, employment contracts, and injunctions. However, unlike jurisdictions such as the United States (DTSA, 2016) and the European Union (Trade Secrets Directive, 2016), India lacks a dedicated

[20] Companies Act, No. 18 of 2013, § 166(2) (India); Securities and Exchange Board of India Act, No. 15 of 1992, § 15G (India).
[21] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 316–17 (India).
[22] *Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh*, AIR 2010 Bom 122 (India).
[23] Factum Law, *Describing the Trade Secret in Your Plaint*, Mondaq (Apr. 30, 2021), https://www.mondaq.com/india/trade-secrets/1055284/describing-the-trade-secret-in-your-plaint

trade secret statute, resulting in fragmented protection, procedural hurdles, and uncertainty for innovators, particularly in emerging sectors like biotechnology, pharmaceuticals, and digital technologies. Consequently, while India is TRIPS-compliant in form, the absence of a specific trade-secret law underscores the need for a comprehensive legislative framework to enhance legal clarity, strengthen innovation ecosystems, and align with global best practices.

- ***The 289th law commission report: Analysis and Limitations***

The 289th Law Commission of India Report (2024) is the most serious effort so far to acknowledge the immediate necessity for a specific legal regime for trade secrets. In March 2024, the Law Commission of India published its 289th Report "*Protection of Trade Secrets*", acknowledging for the first time the imperative necessity for a specific legal regime.[24]

Entitled Protection of Trade Secrets, the report recognizes that trade secrets underpin contemporary innovation and are becoming ever more core to investment flows, technological progress, and economic competitiveness. It recognizes India's dependence on a fragmented combination of the Indian Contract Act, 1872, the principles of equity, the Information Technology Act, 2000, and sectorial laws, and finds that such fractured protections cannot answer the demands of contemporary misappropriation. The Report emphasized that trade secrets play a crucial role in innovation, competitiveness, and investment, and that the existing patchwork of legislation—contracts, equity, and sectorial laws—is insufficient. It suggested the introduction of a sui generis law giving precise definitions, protection standards, and remedies for misappropriation.

Key Recommendations:

The Report recommended a definition of trade secrets consistent with Article 39 of the TRIPS Agreement, laying stress on the fact that information should possess commercial value and be subject to reasonable measures of secrecy.[25] It called for statutory protection of contractual confidentiality clauses, civil remedies like injunctions and damages, and restricted criminal liability in the event of economic espionage. [26] The Report further emphasized striking a

[24] Law Comm'n of India, 289th Report: *Protection of Trade Secrets* 1–5 (2024).
[25] Id at 9-11
[26] Id at 23-25

balance in the protection of trade secrets with legitimate interests like whistle-blower disclosures, public health, and freedom of expression. [27]

The Report takes the TRIPS Agreement Article 39 definition to be its reference point, and it is recommended that Indian law should safeguard information that is commercially significant, secret, and amenable to reasonable protective steps. It made recommendations for statutory recognition of confidentiality terms in employment agreements and NDAs, instead of leaving it to the vagaries of applying Section 27 of the Contract Act alone. Civil remedies suggested were injunctions, damages, and account of profits, while criminal liability was proposed for intentional economic espionage. The Report also acknowledged the need for balancing protection against competing interests such as whistleblowing, freedom of expression, and public health disclosures, stressing that overprotection could strangle transparency and accountability.

A second most important suggestion was the establishment of a sui generis regime, as opposed to placing trade secrets within the general unfair competition law. The Commission believed this would bring about uniformity, enforcement, and more clarity for the courts, businesses, and investors. Moreover, the Report mentioned the function of trade secrets to enable foreign direct investment and international partnerships and proposed that increased protection would place India on par with international expectations in free trade agreements.

Limitations:

Notwithstanding its importance, the Report is beset by significant limitations.

To start with, its discussion is largely based on conventional unfair competition principles, and there is little in it about recent cyber dangers like hacking, ransom-ware, cloud security breaches, or AI-assisted data scraping, all of which are new primary methods of trade secret expropriation. [28] Above all, it gives very little attention to cyber-enabled misappropriation—one of the most significant dangers in contemporary's digital economy. New threats like phishing, ransom ware, cloud vulnerabilities, and AI-based data scraping are set largely aside in its discussion. That is a point of importance because the majority of the trade secret pilferage

[27] Id at 26-29

[28] IAM Media, Cyril Abrol, *A Closer Look at Protecting Trade Secrets in India as New Legislation Could Be on the Horizon* (Sept. 4, 2024), https://www.iam-media.com/article/closer-look-protecting-trade-secrets-in-india-new-legislation-could-be-the-horizon.

faced by Indian business today is carried out through electronic intrusion, not contractual violation.

Second, even as it recognizes employee mobility issues, it does not adequately address statutory protection with India's constitutional prohibition on post-employment restraints under Article 19(1) (g). [29] It fails to respond sensibly to the profound tension between legislative protection of trade secrets and judicial animus against post-employment restraints. The Law Commission does not go as far as embracing more sophisticated approaches, like the proportionality tests adopted in the UK or Japan, which permit limited restraints without imposing unjustifiably on employee mobility.

Third, the Report leaves functional gaps outstanding: it does not suggest mechanisms like confidentiality clubs, sealed proceedings, or protective orders other jurisdictions use to maintain secrecy in litigation.[30] It does not suggest statutory mechanisms for confidentiality clubs, sealed hearings, or protective orders, tools which have become the norm in the EU and the U.S. to maintain secrecy in litigation. This is an obvious loophole: without procedural protections, plaintiffs will continue to put at risk their own trade secrets in open court.

Lastly, the economic analysis in the Report is short of accomplishments. Whereas it recognizes India's TRIPS obligations and suggests foreign investment advantages, it fails to adequately investigate how strong protection of trade secrets would bolster India's bargaining position in free trade agreement talks or support policy success under Digital India and Make in India. Its doctrinal convergence agenda, instead of policy integration, reduces the report's recommendations from being persuasive.

Overall, while the 289th Law Commission Report is a landmark in realizing the gap in Indian law, it is not close to being definitive. It lays a foundation, but the failure to address contemporary cyber threats, constitutional balancing, procedural advances, and economy-wide ramifications points toward a more future-oriented and integrated approach.

- ***Comparative Analysis of Trade Secret Legislations across Jurisdictions***

A comparative survey of global trade secret regimes highlights the diversity of approaches and

[29] Indian Const. art. 19(1)(g); Indian Contract Act, No. 9 of 1872, § 27 (India).
[30] Factum Law, *Describing the Trade Secret in Your Plaint*, Mondaq (Apr. 30, 2021), https://www.mondaq.com/india/trade-secrets/1055284/describing-the-trade-secret-in-your-plaint.

the lessons that India can draw in shaping its own sui generis law. The following jurisdictions—United States, European Union, United Kingdom, China, and Japan—illustrate both convergences and divergences in defining, protecting, and enforcing trade secrets.

United States:

The United States offers one of the most sophisticated and layered regimes for trade secret protection. In the United States, trade secrets are protected under a dual regime: the Uniform Trade Secrets Act (UTSA), adopted in some form by most states, and the federal Defend Trade Secrets Act of 2016 (DTSA). Together, they adopt the TRIPS-aligned definition of trade secrets, requiring secrecy, commercial value, and reasonable steps to maintain confidentiality. At the federal level, the Defend Trade Secrets Act of 2016 (DTSA) provides a uniform civil cause of action, supplementing the Uniform Trade Secrets Act (UTSA) adopted in some form by most states. Both adopt the TRIPS-based definition: information that is secret, economically valuable, and subject to reasonable secrecy measures. Remedies are expansive: courts may grant injunctions, damages for actual losses or unjust enrichment, and in some cases, reasonable royalty damages. In instances of willful and malicious misappropriation, courts may award exemplary damages up to twice the actual damages, along with attorney's fees. One of the most distinctive features of the DTSA is the provision for ex parte civil seizure, permitting courts to seize misappropriated materials to prevent dissemination, though this remedy is used sparingly given its extraordinary nature. Remedies include injunctions, damages for actual loss or unjust enrichment, and reasonable royalties. The DTSA goes further by authorizing exemplary damages and attorney's fees for wilful misappropriation and allowing for an ex parte civil seizure to prevent dissemination. [31] **On the criminal side, the *Economic Espionage Act of 1996* criminalizes theft of trade secrets and economic espionage,** particularly when connected to foreign governments or competitors**, extending in certain cases to extraterritorial conduct.** [32]. On the criminal side, the Economic Espionage Act of 1996 criminalizes theft of trade secrets and economic espionage, particularly when connected to foreign governments or competitors, extending in certain cases to extraterritorial conduct. A landmark case, United States v. Liew (2014), saw employees convicted for misappropriating DuPont's titanium dioxide production technology for a Chinese company. Such cases illustrate how trade secret protection intersects with national security. Procedurally, U.S. courts employ

[31] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2018).
[32] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2018).

confidentiality orders, sealed records, and in-camera review to safeguard trade secrets during litigation. The DTSA also introduced whistleblower immunity, protecting employees who disclose trade secrets in sealed filings or to government authorities in the public interest.

U.S. courts also provide procedural safeguards, including protective orders, sealed filings, and in-camera review, while the DTSA includes a whistle-blower immunity provision for disclosures to government officials or in sealed proceedings.[33]

European Union:

The Directive (EU) 2016/943 creates a uniform framework throughout Member States by identifying trade secrets using the TRIPS test: information which is secret, has commercial value, and contains secrecy measures.[34] The Directive (EU) 2016/943 harmonizes trade secret protection throughout Member States, embracing the TRIPS triplet of secrecy, commercial value, and reasonable measures. The Directive forbids unlawful acquisition, use or disclosure, but not independent discovery, reverse engineering, and lawful whistle-blower disclosures. The remedies available are injunctions, damages, and account of profits, and remedial measures like recall or destruction of infringing products.[35] One of the most radical of the Directive's contributions is the requirement it imposes on Member States to empower the courts to limit access to sensitive information, to conduct private hearings, and to deliver redacted judgments.

Significantly, the Directive requires procedural protection to ensure secrecy in litigation, e.g., limiting access to documents, conducting secret hearings, and publishing non-confidential versions of judgments.[36] In contrast to the U.S. or China, the Directive does not prescribe criminal sanctions, which are left to Member States individually. Remedies include injunctions, damages, account of profits, destruction or recall of infringing products, and corrective orders.

Some national cases have put the Directive to the test. For example, the French case *Fédération Nationale des Syndicats D'Exploitants Agricoles v. Union Nationale des Syndicats Autonomes*

[33] Overview of U.S. Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)
[34] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information, 2016 O.J. (L 157) 1.
[35] Id. arts. 10–12.
[36] Id. art. 9.

highlighted the need to differentiate between confidential information and general know-how. In Germany, the courts have imposed stringent damages remedies for misappropriation, showing the Directive's teeth when paired with national enforcement. The Directive is not harmonizing criminal sanctions, but numerous Member States—including France and Germany—have maintained or improved criminal provisions for trade secret theft.

United Kingdom

In the United Kingdom, the Trade Secrets (Enforcement, etc.) Regulations 2018 transposed the EU Directive into domestic law, keeping the secrecy–value–measures test. [37] The provisions coexist with the common-law doctrine of breach of confidence, which has traditionally protected confidential business information.

Courts grant injunctions, damages, and delivery-up orders, and examine the reasonableness of restrictive covenants to ensure they are proportionate in time and geographical scope. UK courts are also versed in employing confidentiality clubs and protective orders to maintain confidentiality in proceedings. [38]

UK common law is brimming with trade secret cases: in *Faccenda Chicken Ltd. v. Fowler (1986)*, the Court of Appeal drew a line between trade secrets capable of protection and the run-of-the-mill skill and knowledge that employees bring with them. Recently, in *Vestergaard Frandsen A/S v. Bestnet Europe Ltd. (2013),* the Supreme Court asserted once again that liability could be imposed even on those who happen to use misappropriated secrets unknowingly if they consciously profit from them. UK courts are also very skilled at utilizing procedural safeguards, such as confidentiality clubs and sealed evidence, to protect sensitive information throughout litigation. Even in the aftermath of Brexit, the UK has maintained these standards, keeping a hybrid system that combines statutory clarity with the common law's flexibility.

China

China significantly enhanced trade secret protection by amending the Anti-Unfair Competition Law (AUCL) and complementary judicial interpretations. The AUCL defines a trade secret as

[37] Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018/597 (UK).
[38] Overview of U.K. Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)

technical or business information that is not public, possesses commercial value, and is protected by confidentiality means.[39] Unlawful acquisition encompasses theft, bribery, coercion, electronic intrusion (hacking), and tempting employees. Civil remedies would consist of injunctions, damages, and, in extreme instances, punitive damages up to five times actual loss, with statutory damages possible where harm is hard to measure. [40] **It actually covers electronic misappropriation, for example, hacking or unauthorized access, as criminal acts. Administrative enforcement reinforces civil remedies, and serious violations can lead to criminal liability under China's Criminal Law.**[41] These reforms emphasize China's deterrence policy and are part of its overall innovation-led strategy. Administrative punishment is another channel, with local market supervision administrations given the right to investigate and punish violations.

Judicial judgments by the Supreme People's Court have further buttressed these safeguards. In the high-profile cases of DuPont v. Kolon (counterpart cases), courts exacted huge damages against local parties convicted of trade secret misappropriation. Additionally, Chinese Criminal Law provides criminal sanctions, demonstrating the seriousness with which trade secrets are handled in China's policy of developing innovation. Such actions complement China's overall objective of deepening its intellectual property system to attract foreign investment and enhance indigenous technological advances.

Japan

Japan safeguards trade secrets under the Unfair Competition Prevention Act (UCPA), including technical and business information that is not publicly disclosed, possesses economic value, and is subject to secrecy management. [42] Unlawful acquisition, use, or disclosure gives rise to both civil and criminal liability The UCPA establishes civil remedies in the form of injunctions and damages, as well as criminal penalties for unlawful acquisition, use, or disclosure. Japanese courts use procedural protections, including confidentiality orders and restricted-access evidence, to safeguard secrets during litigation. [43] The regime also acknowledges wrongful electronic acquisition and is extraterritorial, allowing Japanese courts to deal with cross-border

[39] Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment) (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 23, 2019, effective Apr. 23, 2019) art. 9 (China).
[40] Id. art. 17.
[41] Overview of China Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)
[42] Unfair Competition Prevention Act, Act No. 47 of 1993, as amended by Act No. 33 of 2019, art. 2(6) (Japan)
[43] Id. arts. 5–7.

misappropriation.[44] Importantly, Japanese courts also evaluate the reasonableness of non-compete provisions, weighing protection of employer interests against freedom of movement by employees.

Remedies are available in the form of injunctions, damages, and criminal sanctions like imprisonment and fines. Japanese law also has extraterritorial application, allowing courts to deal with misappropriation between foreign parties. Japanese judicial practice emphasizes secrecy management. In *Benesse Corp. v. Araki (2015)*, an ex-employee was convicted of revealing customer information, reflecting Japan's preparedness to criminalize outrageous violations. Procedurally, Japanese courts utilize secrecy precautions like restricted-access evidence and in-camera hearings to maintain secrecy throughout litigation. Notably, Japan reconciles employee mobility and employer protection by subjecting non-compete covenants to a reasonableness test, preventing them from being unduly restrictive.

Comparative Observation

Throughout these jurisdictions, some patterns are found. They all share the TRIPS triad as the definitional foundation of trade secrets, reflecting the widespread minimum standard consensus. Civil remedies of injunctions and damages are available everywhere, although the scope of punitive or exemplary damages differs. The U.S. and China implement strong criminal sanctions, whereas the EU and UK prioritize civil redress and voluntary criminalization at national level. Procedural protection in litigation is becoming ever more essential, especially in the EU, UK, and U.S., where confidentiality clubs, sealed proceedings, and protective orders are the norm. Lastly, all jurisdictions recognize the necessity of striking a balance between protection and genuine exceptions such as employee mobility, reverse engineering, and whistleblowing.

Lessons for India: Insights from Global Practices

Comparative analysis of the United States, European Union, United Kingdom, China, and Japan brings to fore some shared principles and unique mechanisms that India can avail itself of while developing a sui generis trade secret regime.

[44] Overview of Japan Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)

First, paramount is the necessity for a standard statutory definition. All of the surveyed jurisdictions apply the three-part test consistent with Article 39 of the TRIPS Agreement: information needs to be secret, commercially valuable, and subject to reasonable measures to keep it confidential.[45] Adoption of this standard in Indian law would be clarificatory, harmonize with global practice, and assist India in fulfilling expectations in free trade negotiations.

Second, robust civil remedies are necessary. U.S. law gives a strong arsenal consisting of injunctions, actual loss or disgorgement damages, and reasonable royalties.[46] The European Union and United Kingdom add to the remedies with the corrective relief of withdrawal or destruction of infringing products.[47] China also goes beyond, authorizing punitive damages for wilful misappropriation, with Japan also permitting criminal penalties to be added to civil relief. [48] An Indian law in the future must take this multi-level approach—restraining relief to block dissemination, damages to pay for loss, and higher penalties in extreme cases.

Third, criminalization of serious misappropriation has a deterrent effect. The U.S. Economic Espionage Act and China's Criminal Law criminalize trade secret theft, including cyber-enabled misappropriation, as an acknowledgment of national security and economic threats.[49] The EU leaves this to Member States but the trend indicates that India ought to enact narrowly defined criminal provisions, at least for large-scale or state-sponsored misappropriation.

Fourth, procedural protections in the course of litigation are essential. Courts must, under the EU Directive, institute confidentiality measures including limited access, redaction, and closed hearings.[50] U.S. courts similarly use protective orders and sealed filings.[51]. Absent such protections, plaintiffs would be discouraged from bringing suit out of fear of revealing their own secrets. Indian courts have no statutory power currently to institute confidentiality clubs or sealed proceedings, and the legislation should directly close that loophole.

[45] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39, Apr. 15, 1994, 1869 U.N.T.S. 299.
[46] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2018).
[47] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016, arts. 10–12, 2016 O.J. (L 157) 1.
[48] Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment) art. 17 (China); Unfair Competition Prevention Act, Act No. 47 of 1993, as amended by Act No. 33 of 2019, arts. 2, 5–7 (Japan).
[49] Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39 (2018); Overview of China Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)
[50] Directive (EU) 2016/943, supra note 3, art. 9.
[51] Overview of U.S. Trade Secret Protection, Eur. Union Intellectual Prop. Off. (2021)

Lastly, the balance between protection and competing interests is essential. The U.S. DTSA has whistle-blower immunity provisions, while the EU Directive itself protects employee freedom of movement and expression.[52] Japan tests non-competes for reasonableness, and the UK examines restraints under common law. These practices demonstrate how statutory protection can be maintained alongside constitutional guarantees, a lesson especially applicable in India considering the limitations under Article 19(1) (g).

Considered in aggregate, these international practices emphasize that an Indian law needs not only to define and safeguard trade secrets, but also to incorporate digital protections, procedural safeguards, and provisions of exceptions for valid disclosures. This kind of regime would fill the current legal gap, improve investor confidence, and position India within adapting international norms.

Conclusion

The above analysis proves that even though trade secrets are crucial to business in the contemporary era, India remains dependent on an array of contractual, statutory, and equitable principles falling short of exhaustive protection. Courts have struggled to bridge these gaps, particularly in Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh, in which the Bombay High Court defined criteria for determining trade secrets in terms of confidentiality, commercial value, and efforts directed towards maintaining secrecy. [53] While valuable, such judicial interventions underscore the ad hoc nature of protection in the absence of a statutory framework.

Comparative experience reveals the shortcomings of India's existing strategy. Jurisdictions like the United States, the European Union, the United Kingdom, China, and Japan have shifted towards transparent statutory definitions, multi-layered civil and criminal remedies, procedural mechanisms to maintain confidentiality during trial, and equity-based exceptions for whistle-blowers and workers.[54] These approaches yield both deterrence as well as certainty—attributes

[52] Defend Trade Secrets Act of 2016, supra note 2, § 1833(b); Directive (EU) 2016/943, supra note 3, art. 1(2).
[53] *Bombay Dyeing & Mfg. Co. v. Mehar Karan Singh*, AIR 2010 Bom 122 (India)
[54] Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2018); Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016, 2016 O.J. (L 157) 1; Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment); Unfair Competition Prevention Act, Act No. 47 of 1993, as amended by Act No. 33 of 2019 (Japan).

crucial for innovation generation, foreign direct investment attraction, and cross-border technology transfer.

India's over-reliance on Section 27 of the Indian Contract Act and equitable doctrines of breach of confidence cannot alone meet twenty-first century challenges. Contemporary misappropriation is more often digital, stemming from hacking, phishing, insider cyber leaks, and artificial intelligence-powered data scraping.[55] The 289th Law Commission Report (2024) was a step in the right direction, but it is still limited in its handling of cyber perils and procedural gaps. [56] A sui generis law, on the other hand, might provide a uniform definition, statutory redress, confidentiality procedures in litigation, and graduated criminal sanctions, while striking a balance between constitutional rights under Article 19(1) (g).

Embracing a framework of this sort would put India on the global best practices track, give it greater leverage in trade talks, and most significantly, safeguard the lifeblood of its innovation economy—trade secrets. Without a law, Indian businesses, especially start-ups and MSMEs, will be open to misappropriation in the domestic as well as foreign markets. The argument for a sui generis trade secret law is therefore not only doctrinally compelling but economically necessary.

[55] World Intellectual Prop. Org., *Trade Secrets: The Hidden IP Right* (2023), https://www.wipo.int/web/wipo-magazine/articles/trade-secrets-the-hidden-ip-right-40225.
[56] Law Comm'n of India, 289th Report: *Protection of Trade Secrets* (2024).