ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 3 | Issue 1

2025

Website: www.ijlae.com
Email: editor@ijlae.com

ISSN (O): 2584-2196

LEGAL FRAMEWORK FOR TRADE SECRET PROTECTION

Meenu Singh
Amity University Noida
&

CS Monica Suri
Assistant Professor
Amity University Noida

INTRODUCTION

The TRIPS Agreement emphasizes that safeguarding against unfair competition should extend to undisclosed information, building on principles established in the Paris Convention for the Protection of Industrial Property, overseen by WIPO. While trade secrets are inherently confidential, their commercial nature necessitates limited sharing with employees and partners. Consequently, legal frameworks accommodate controlled disclosure within a restricted circle, ensuring the information remains non-public and known only to a select few. This dual characteristic—confidential yet commercially shared—shapes the broadly consistent definition of trade secrets across nations.

Article 39 of TRIPS outlines three key criteria for trade secret protection, aligning with prevailing practices in many countries and influencing subsequent legislation. These criteria are generally applied as follows:[1]

- Secrecy: The information must not be publicly accessible, though absolute secrecy is not required. Disclosure to employees or partners is permissible, provided broader public access is restricted.
- Commercial Value: The information must derive economic value from its secrecy, typically protecting commercially useful data that benefits from remaining confidential.
- Reasonable Efforts to Maintain Secrecy: The rights holder must demonstrate reasonable steps to protect the secret. While complete success isn't required, some

[1] Feroz Ali Khader, "Trade Secret Law in India: A Blueprint for Legislative Reform", (2008) 13(2) JIPR 148.

ISSN (O): 2584-2196

proactive measures are necessary. National laws often interpret "reasonable" broadly, though some jurisdictions impose specific requirements, such as contractual confidentiality obligations or written agreements.

Trade secrets encompass a wide range of economic activities, primarily falling into technical information (e.g., formulas, plans) or confidential business data (e.g., customer lists, strategies). Unlike patents or copyrights, trade secrets do not grant exclusive rights; they can be lawfully obtained through independent discovery, reverse engineering, or public sources. Once disclosed fairly, protection ceases, making their duration indefinite but vulnerable to legitimate competition.

TRIPS mandates that WTO members establish national systems to combat unfair competition involving trade secrets, yet Article 39's flexibility leads to diverse implementations. Some countries enact specific laws, while others rely on broader legal concepts like breach of contract or dishonest acquisition. This variability influences business and employment practices, suggesting that trade secret protection may have significant economic implications.

INTERNATIONAL LEGAL INSTRUMENTS

There is growing acknowledgment of the critical role trade secrets and their protection play, both in the United States and globally. Studies suggest that most operational technologies worldwide rely on trade secret protection rather than patents. Additionally, as commerce becomes increasingly globalized, even small businesses must safeguard their trade secrets across borders. Failure to do so can result in a loss of competitive advantage when operating in foreign markets.

Several international treaties and agreements aim to protect intellectual property on a global scale, including trade secrets. Notably, both the **North American Free Trade Agreement (NAFTA)** and the **TRIPS Agreement** (established during the **Uruguay Round of GATT**) contain provisions aimed at strengthening trade secret protection.[2] However, no comprehensive international treaty solely dedicated to trade secrets exists—NAFTA and TRIPS only address the issue briefly.

[2] Shamnad Basheer, "The Invention of an Indian Trade Secrets Law: Confronting the Myth of Confidentiality", (2011) 6(3) NUJS L Rev 425.

ISSN (O): 2584-2196

In recent years, particularly over the past decade and a half, many countries—especially in Asia—have moved toward enacting domestic laws specifically designed to enhance trade secret protection. While international treaties and agreements offer some level of safeguarding, the differences in protection across these frameworks remain relatively minor.

TRIPS AGREEMENT

The discussion of intellectual property rights (IPR) as a trade-related issue began during the **1978 Tokyo Round of the General Agreement on Tariffs and Trade (GATT)**. At this time, negotiations focused on developing international rules to combat counterfeit goods.

Simultaneously, discussions on global IP protection were taking place at the **World Intellectual Property Organization (WIPO)**, a **United Nations specialized agency**. However, WIPO faced several challenges, including

The **World Intellectual Property Organization (WIPO)** faces significant limitations in enforcing intellectual property (IP) treaties, primarily due to two key issues:[3]

1. **Weak Enforcement Powers** – WIPO treaties lack strong enforcement mechanisms. The **WIPO General Assembly** can only issue **recommendations** for corrective measures, leaving compliance largely voluntary.
2. **Consensus-Based Adoption** – Treaty ratification depends on unanimous agreement among member states, with adherence being entirely optional. As a result, if a member violates a treaty, **no swift or binding remedies** are available.

Additionally, treaty negotiations and amendments often reach **deadlock** due to conflicting interests between **developed and developing nations**. Frustrated by these limitations, the **United States**, seeking stronger global IP protections, pushed for a more enforceable framework—leading to the development of the **TRIPS Agreement under the WTO**, which introduced binding dispute resolution mechanisms.[4]

Frustrated by the limitations of WIPO's framework, the United States—seeking more robust international IP protections—reframed weaknesses in developing countries' IP systems as trade-related issues. This strategic shift led to the proposal of negotiating "trade-related aspects

[3] Raju K.D., "Protection of Trade Secrets: A Comparative Study of Indian and American Legal Systems", (2009) 51(4) JILI 541.
[4] *Ibid*

of intellectual property, including trade in counterfeit goods" (TRIPS) within the trade-focused forum of GATT.

Key Milestones in TRIPS Negotiations:

1. **1986 Punta del Este Declaration**: At the GATT ministerial meeting in Uruguay, member states agreed to launch TRIPS negotiations. By January 1987, 15 negotiation groups were established across different trade areas.
2. **Early-Stage Conflicts (1988–1989)**: An interim report emerged from the 1988 Montreal meeting, but stark divisions persisted:
    - Developed nations pushed for stringent IP protections.
    - Developing countries contested GATT's authority to regulate IP, arguing it fell outside trade policy.
3. **Prolonged Deadlocks**: Originally slated for completion in 1990, negotiations stalled over agricultural disputes and North-South tensions, prompting an extension at the Brussels ministerial meeting.
4. **Breakthroughs (1991–1993)**:
    - Streamlining negotiation groups from 15 to 7 in 1991.
    - GATT Director-General Arthur Dunkel's 1991 draft agreement.
    - The 1992 U.S.-EU compromise on agriculture, paving the way for the final consensus in December 1993.

North-South Tensions:

The process exposed fundamental clashes: Developed economies viewed strong IP regimes as essential to innovation and trade, while developing nations resisted perceived overreach into sovereign policy domains. Only through iterative compromises did TRIPS eventually crystallize under the new WTO framework.

FEATURES

The TRIPS Agreement is a comprehensive accord containing 73 Articles organised into 7 Parts. Part I outlines the general provisions and foundational principles. It mandates that member states must adopt national laws to implement its provisions. The term "intellectual property" under TRIPS refers to the areas covered in Sections 1 to 7 of Part II, which include copyright

ISSN (O): 2584-2196

and related rights, trademarks, geographical indications, industrial designs, patents, layout-designs of integrated circuits, and the protection of undisclosed information, such as trade secrets (Article 1).

Moreover, Article 2 of the Agreement obliges members to uphold their responsibilities under existing international treaties related to intellectual property. These include the Paris Convention, the Berne Convention, the Rome Convention, and the IPIC Treaty.

Earlier treaties on intellectual property primarily emphasised national treatment. This occasionally led to situations where foreign nationals received more favourable protection than the citizens of the country, often as a result of reciprocal trade-offs through bilateral negotiations. To avoid such disparities, TRIPS enshrines both national treatment (Article 3) and most-favoured-nation treatment (Article 4) as core principles. While the latter had already been a feature of GATT, it applied only to trade in goods. Under TRIPS, it extends to the holders of intellectual property rights, including both individuals and entities.

WIPO FRAMEWORK

International treaties pertaining to intellectual property rights are coordinated by the World Intellectual Property Organisation (WIPO), a United Nations body. WIPO was founded in 1967 with the goal of advancing intellectual property protection globally. It now oversees 24 treaties and helps negotiate a number of proposed treaties pertaining to copyrights, patents, and trademarks. Its headquarters are in Geneva, Switzerland. Promoting a broad culture of intellectual property, incorporating intellectual property into national development policies and programs, creating international intellectual property laws and standards, providing high-quality services in international intellectual property protection systems, and improving the effectiveness of WIPO's management and support procedures are the five strategic goals of the organisation.[5]

With a General Assembly supervising its operations and several issue-specific committees addressing important issues, WIPO functions on a "one country, one vote" basis. Under the direction of the WIPO Secretariat, the agency is run by individual member nations who convene in committees, assemblies, and working groups. Under the WIPO Convention, the

[5] *Ibid*

ISSN (O): 2584-2196

WIPO Secretariat has a great deal of authority to shape and guide the organization's activities and goals. Another agreement that WIPO oversees is the Agreement on Trade-Related Aspects of Intellectual Property Rights, or TRIPS Agreement. The TRIPS Agreement was signed in 1994 and contains strong enforcement tools that compel nations to abide by its terms, including trade sanctions and World Court lawsuits. To help with the TRIPS Agreement's implementation, the WTO and WIPO inked a cooperation agreement in 1996.

The Internet Corporation for Assigned Names and Numbers (ICANN), which launched the Uniform Domain-Name Dispute-Resolution Policy (UDRP) in 1999, is closely associated with WIPO. The majority of country code top-level domain name (ccTLD) registration authorities and generic top-level domain name (gTLD) registrars that have earned ICANN accreditation are required by contract to submit to arbitration through WIPO's Arbitration and Mediation Centre. Anyone can contest a domain name's registration and ownership under the UDRP on the grounds that it violates a trademark. Independent service providers approved by the Centre manage the actual dispute resolution procedure.

Trademark holders now have the unique ability to pre-emptively register and contest the registration of new gTLDs thanks to procedures that WIPO and ICANN have put in place regarding the launch of new gTLDs. However, the highest court in the United Nations, the International Court of Justice (ICJ), has more rights than trademark holders do. The contentious policy of ICANN's WHOIS database and its posting of private data online has also been suggested by WIPO.[6] Because of this regulation, one of the biggest sources of information for consumer abuses like fraud, identity theft, and other privacy crimes is the WHOIS database. WIPO has been "circling the waggons" and impeding reform efforts in response to the global civil society movement. Although women delegates from poor nations play a vital role in fostering consensus and advancing the Development Agenda at WIPO, the organisation is still largely dominated by men in senior roles. Since the 1990s, WIPO has had little influence over the regulations governing information and communications technologies (ICTs) because of the changing nature of intellectual property rights. As personal communication technologies, especially computers and the internet, have advanced, intellectual property laws have emerged as a key factor in establishing ICT policy and regulation. A significant shift in WIPO's role in establishing ICT regulations and copyright law was brought about by the WIPO Copyright

[6] Arpan Banerjee, "The Development of Trade Secret Law in India: A New Beginning?", (2015) 20(2) CTLR 37.

ISSN (O): 2584-2196

Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). The 1998 Digital Millennium Copyright Act (DMCA) in the US and the EU Copyright Directive (EUCD) in Europe both put these WIPO treaties into effect. But compared to the WIPO Internet Treaties, the DMCA and EUCD prohibit a lot more activity and technology. Working closely with ICANN to establish its UDRP policy to address domain name infringement claims and to implement clauses that grant trademark holders early registration and cancellation rights for new domain names, WIPO has also started to participate in the broader "internet governance" discussions.

From 2003 to 2005, WIPO attended the United Nations World Summit on the Information Society (WSIS), however it did not have a major influence. To promote discussion on the subject of intellectual property in the information society and to advance WSIS's objectives, WIPO hosted an Online Forum on Intellectual Property in the Information Society in 2005. However, because the UN Internet Governance Forum (IGF) is a debate forum rather than a body that makes treaties, WIPO has not significantly contributed to it. Prominent legal experts, scientists, activists, public-interest NGOs, and a former French prime minister released the Geneva Declaration on the Future of WIPO in 2004. WIPO was urged by the Declaration to change its practice of granting and extending monopoly powers, frequently without considering the repercussions. It called on WIPO to balance the public sphere and competition and comprehend the true economic and social repercussions of overly stringent intellectual property rights.[7] Additionally, the Declaration asked WIPO to develop a Development Agenda and innovative strategies for fostering creativity and innovation. In order to change WIPO's pattern of mindlessly expanding intellectual property rights, the 2004 WIPO General Assembly passed a resolution calling for the creation of a Development Agenda. A fundamental review of WIPO's overall mandate and governance structure, the adoption of prodevelopment norm-setting standards, the proposal by the Group of Friends of Development (FoD), and the proposal of principles and guidelines for WIPO's technical assistance program, as well as guidelines for technology transfer and competition policy work at WIPO, were all part of the proposal. In July 2005, the US and Japan rejected all of the recommendations for a Development Agenda, even though the FoD concept was widely supported by the public. The richest member nations, such as the US and Europe, declined to support any of the

[7] Aditi Subramaniam, "Employee Mobility and Trade Secret Protection in India", (2016) 9(1) Indian Journal of Law and Technology 99.

ISSN (O): 2584-2196

recommendations despite the WIPO General Assembly's 2006 vote in favour of a Development Agenda.

EU TRADE SECRETS DIRECTIVE

The term 'trade secret' encompasses a broad range of information that goes beyond technical expertise about commercial data, including supplier, customer, business plans, market research, strategies, and new products, as long as it is undisclosed and meant to be kept private. Confidentiality is used as a tool for innovation management and commercial competitiveness by companies in all industries. Trade secrets are just as valuable as other forms of intellectual property protection for their innovation-related endeavours, such as patents, design rights, copyrights, and others. SMEs, or small and medium-sized businesses, are especially dependent on trade secrets. In order to safeguard important business information and know-how, trade secrets have grown in importance for companies as a supplement or substitute for intellectual property rights as a result of the economy's rapid digitisation and the widespread availability of technologies like artificial intelligence. Businesses are becoming more vulnerable to trade-secret misappropriation through "cyber theft," data breaches, and industrial espionage as a result of increased digitalisation, connection, and globalisation.

Legal safeguards against the unlawful acquisition, use, and disclosure of trade secrets in the European Union were weak and uneven among EU member states prior to the Trade Secrets Directive. The ability of European enterprises to innovate and effectively operate in the internal market is adversely affected by the combination of a relatively low degree of protection and the absence of a standardised framework for trade secrets. As long as adherence to specific statutory exclusions and safeguards is maintained, EU member states are permitted to offer more extensive protection, as the Trade Secrets Directive created a uniform set of basic levels of protection throughout the EU.[8] As a result, there is some leeway for EU member states to incorporate the Directive into their own national legislation. Only civil remedies against the illegal acquisition, use, and disclosure of trade secrets are covered by the Trade Secrets Directive. It leaves out unimportant knowledge, expertise, and abilities that workers acquire during the regular course of their jobs. The definition of a "trade secret" does not specify how

[8] T. Ramakrishna, “Intellectual Property and Trade Secrets: Challenges in the Indian Context”, (2012) 17(3) CULR 114.

ownership is determined, but it does describe a "trade-secret holder" as any individual or entity that is legally in control of a trade secret.

The Trade Secrets Directive, in contrast to other types of intellectual property protection, provides protection against the unauthorised acquisition, use, and disclosure of trade secrets but does not confer an exclusive right on the trade secret holder. Specific standards for determining a trade secret's state of secrecy prior to misappropriation or disclosure are not provided by the Trade Secrets Directive. Nonetheless, it necessitates that the owner of the trade secret prove that the information was not widely known or easily accessible by those in the circles that typically handle it, and that reasonable measures were taken to keep it confidential under the given circumstances. National courts and eventually the Court of Justice of the European Union (CJEU) will need to provide guidelines on how these criteria should be applied in practice. Regardless of whether a trade secret has real or potential commercial worth, its commercial value is determined. For instance, if a trade secret's illegal acquisition, use, or disclosure is likely to jeopardise the interests of the person legally in control of it, then it should be deemed to have commercial value. Information on illegal or dishonest business practices would also be recorded. Even while such knowledge might meet these requirements to be considered to have commercial value derived from its confidentiality, trade-secret protection would be dubious in this situation.[9] At the IT level, technological safeguards like access limitations and a trade-secret policy must be put into place, and the information and document management system must be built appropriately. Using firewalls and encryption technologies is essential, particularly for home office equipment, mobile devices, and bring your own device. Particularly in front of the COVID-19 epidemic, working-from-home policies ought to be compared to and in line with the organization's trade-secret policy. Identification and proof of potential trade-secret theft cases depend on monitoring and tracking the flow, use, and access of sensitive information both inside and outside the organisation. Reviewing current agreements with partners, customers, and suppliers; making sure sufficient non-disclosure agreements (NDAs) are employed in the course of business; and fortifying confidentiality sections in employment contracts are examples of legal (contractual) procedures. Due to their general or vague nature, standard clauses frequently run the danger of being unenforceable

[9] Aditi Subramaniam, “Employee Mobility and Trade Secret Protection in India”, (2016) 9(1) Indian Journal of Law and Technology 99.

ISSN (O): 2584-2196

under the applicable legislation. It's also important to make sure that clauses pertaining to trade secrets, intellectual property, and non-compete agreements complement one another.

NATIONAL LEGAL FRAMEWORKS

United States: Defend Trade Secrets Act (DTSA)

The Defend Trade Secrets Act (DTSA) is a legal provision that allows U.S. employers to protect their confidential information and trade secrets from potential misappropriation by employees or others. This practice note addresses various issues, including redress for trade secret misappropriation under the DTSA, state and common law claims for misappropriation of trade secrets or theft of confidential information, the Economic Espionage Act of 1996 (EEA), the Computer Fraud and Abuse Act (CFAA), common law tort claims, common law contract claims, and employee raiding. The DTSA allows employers to seek redress in federal court, which can be advantageous as federal courts are more adept at addressing complex technical issues in trade secret cases. However, bringing a claim under the DTSA can make a case that an employer wishes to keep in state court removable to federal court by the defendant.

The DTSA does not preempt existing state trade secret law regimes, meaning that a trade secret owner can bring parallel state and federal claims for trade secret misappropriation in federal court. It is important to consider bringing concurrent state and federal trade secret claims to avail the employer of all potential causes of action. Understanding the definitions of key terms is crucial before bringing a claim under the DTSA or state or common law.

The Trade Secrets Act (DTSA) defines trade secrets as commercially valuable information that is not publicly known and is protected by reasonable efforts to preserve its confidentiality. It covers all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes. The DTSA's definition is similar to the UTSA's definition, which requires the trade secret to derive independent economic value from not being generally known and that the owner has taken reasonable efforts to keep the information secret. The DTSA also defines misappropriation as the acquisition of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means or that the knowledge was acquired under circumstances giving rise to a duty to maintain the secrecy or limit the use of the trade secret.

ISSN (O): 2584-2196

Employers must ensure that the trade secrets at issue meet the definition of trade secret under all applicable statutes.

When filing a complaint under the Trade Secrets Act (DTSA), it is crucial to explain why the allegedly misappropriated information qualifies for trade secret protection. A plaintiff must plausibly allege how the information qualifies as a trade secret, as failing to do so can lead to dismissal with prejudice. The DTSA allows employers to maintain the secrecy of allegedly misappropriated trade secrets during court proceedings by allowing them to file a submission under seal that describes their interest in keeping the information confidential. The DTSA has a three-year statute of limitations for claims under the DTSA, which begins when the misappropriation is discovered or should have been discovered. This period generally applies to trade secret misappropriation that occurred on or after the date of the Act's enactment or began before the Act's enactment and continued after the Act took effect. The DTSA provides for an ex parte civil seizure mechanism, which allows a court to issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action. This tool allows employers to quickly prevent further dissemination of the misappropriated information during the pendency of a formal DTSA case.[10]

- Civil seizure may be ordered only in "extraordinary circumstances" and requires the moving party to show all the following:
- An order pursuant to Fed. R. Civ. P 65 or other equitable relief would be inadequate.
- An immediate and irreparable injury will occur if seizure is not ordered.

Harm to the applicant from denial of a seizure order (1) outweighs the harm to the person against whom seizure is ordered and (2) substantially outweighs the harm to any third parties by such seizure. To make civil seizure effective, employers must quickly explain to the court what information was stolen, who stole it, and where it is being kept. A well-developed trade secret asset management plan can greatly assist in this process. The Trade Secrets Act (DTSA) provides several remedies for trade secret misappropriation, including seizure, injunctions, damages, and attorney's fees. If extraordinary circumstances are not present, a judge may grant a seizure request as part of a TRO or preliminary injunction related to allegations of trade secret

[10] T. Ramakrishna, “Intellectual Property and Trade Secrets: Challenges in the Indian Context”, (2012) 17(3) CULR 114.

ISSN (O): 2584-2196

theft under the DTSA. The DTSA also provides for remedies other than seizure, such as granting an injunction to prevent any actual or threatened misappropriation, requiring affirmative actions to protect the trade secret, and requiring future use of the trade secret on payment of a reasonable royalty. The DTSA explicitly rejects the inevitable disclosure doctrine, which allows courts to prevent a former employee from working for a competitor of their former employer if it would require the employee to rely on their former employer's trade secret information. However, trade secret plaintiffs can still allege misappropriation under the inevitable disclosure doctrine under a state law cause of action where the state common law allows application of the doctrine. To take advantage of these remedies, employers must advise their employees of the existence of whistleblower immunity in any contract or other employment agreement entered into after the enactment of the DTSA. The DTSA also includes a safe harbor for whistleblower employees, providing immunity from criminal or civil liability under any federal or state trade secret law for disclosure of a trade secret in confidence to an attorney or governmental official.

The Trade Secrets Act (DTSA) is a law that protects employers' confidential information and trade secrets. Employers may include the DTSA in employment agreements entered into after its enactment, as it does not affect immunity under 18 U.S.C. §§ 1833(b)(1) or (2). The DTSA allows individuals to disclose trade secrets in confidence to government officials, attorneys, or in a complaint or document filed in a lawsuit or other proceeding. The DTSA can also be applied to overseas conduct, particularly in cases of economic and corporate espionage originating in China. The DTSA's ability to address trade secret misappropriation overseas is valuable, especially in countries with weak IP rights protections. The DTSA may also become the trade secret statute of choice to remedy trade secret misappropriation through a Section 337 investigation before the International Trade Commission (ITC). The ITC is a quasi-judicial administrative agency with the authority to address unfair trade practices related to imports, including the authority to exclude articles from importation into the United States. A complaint in a Section 337 investigation generally must show the importation of an article into the United States related to an unfair method of competition or unfair act, misappropriation of the trade secret at issue, and injury to a domestic industry tied to the imported article.

The Uniform Trade Secrets Act (UTSA) is a common definition for "trade secret" and "misappropriation" in state courts. Employers can use state laws to bring a claim against a former employee for misappropriation of an employer's trade secrets. To state a claim, a party

must show that the information constitutes a trade secret, the plaintiff took reasonable steps to preserve the secrecy of the trade secret, and the defendant misappropriated the secret using improper means.To preserve the secrecy of information in public filings, employers should impound or seal the filings or attached documents according to local court rules. They may also need to obtain hard forensic evidence demonstrating that the former employee is or was unlawfully in possession of the employer's confidential information or trade secrets.

Preliminary injunctions in state court can be requested to prevent the use and disclosure of the employer's trade secrets during the pendency of the litigation. Employers should examine potential venue options, prepare expedited discovery requests, and instruct the employer to immediately begin compiling all evidence relating to the employee's liability for theft of confidential information and trade secrets and the damages suffered by the employer as a consequence. The UTSA and many state statutes permit courts to award attorney's fees to prevailing parties where the misappropriation is willful and malicious, which can also be used to assert leverage for any potential settlement prior to trial. The Economic Espionage Act of 1996 (EEA) protects trade secrets by providing criminal sanctions for misappropriation, including fines, payment of restitution, and prison time.[11] Section 1832 of the EEA makes it a crime to steal a trade secret for the economic benefit of anyone other than the owner while intending or knowing that the offense will injure any owner of that secret.[12] The statute defines "trade secret" as all forms and types of financial, business, scientific, technical, economic, or engineering information, provided that the owner has taken reasonable measures to keep such information secret and the information derives independent economic value from not being generally known to, and not being readily ascertainable through proper means by, the public.

The DTSA amended the EEA to create a private cause of action for the misappropriation of trade secrets. Employers can generally be satisfied taking civil action under the DTSA and state law against former employees who misappropriated trade secrets. However, in certain circumstances, it may still be useful to notify and cooperate with the attorney general, U.S. Department of Justice, and/or FBI to seek criminal prosecution, as enabling such a prosecution can be a powerful deterrent against future thefts of an employer's trade secrets.

[11] T. Ramakrishna, “Intellectual Property and Trade Secrets: Challenges in the Indian Context”, (2012) 17(3) CULR 114.
[12] Aditi Subramaniam, “Employee Mobility and Trade Secret Protection in India”, (2016) 9(1) Indian Journal of Law and Technology 99.

ISSN (O): 2584-2196

European Union: Trade Secrets Directive (2016/943)

The Trade Secrets Directive (Directive (EU) 2016/943) is a key legislative measure established by the European Union to ensure the universal protection of trade secrets throughout Member States. Prior to its adoption, the laws governing trade secrets differed greatly between jurisdictions, sometimes resulting in legal confusion and fragmented enforcement. The Directive was adopted to establish a unified legal framework, thereby promoting legal clarity and fostering innovation and fair competition within the internal market. The Directive defines a trade secret as information that is secret in nature, holds commercial value because it is not commonly known, and has been subject to reasonable procedures to keep it confidential. This definition follows the approach set out in the TRIPS Agreement, keeping compatibility with international norms. Crucially, the Directive distinguishes between the authorised and unlawful acquisition, use, and disclosure of trade secrets. Lawful ways may include independent discovery, reverse engineering, or public observation, whereas unlawful acts involve violations of confidentiality requirements, unauthorised access, or inducement to expose protected information.

In terms of enforcement, the Directive obliges Member States to offer effective legal remedies, including as injunctions, temporary relief, destruction of infringing items, and compensation for losses suffered. It also includes significant protections to ensure the secrecy of trade secrets during judicial procedures, which may include restricting access to sensitive materials or limiting the attendance of hearings. The implementation date for Member States was 9 June 2018. While most have adopted the Directive into their national legislation, the scope of its impact continues to evolve. The Directive has proved particularly useful for small and medium-sized firms, which typically lack effective systems for protecting commercially vital know-how. Overall, the Trade Secrets Directive marks a major step towards securing intangible assets in the knowledge economy, reaffirming the EU's broader commitment to a harmonised and innovation-driven legal structure.

INDIA: COMMON LAW APPROACH & PROPOSED LEGISLATIVE REFORMS

In India, trade secrets are generally protected under the common law framework, as the country does not yet have a specific legislation equivalent to the European Union's Trade Secrets Directive (2016/943) or the United States' Defend Trade Secrets Act (2016). The Indian legal approach to trade secrets has been fashioned largely by judicial interpretation, contractual

responsibilities, equitable principles, and specific statutory provisions, reflecting the flexibility and adaptability of the common law system. However, this reliance on judge-made law has also given rise to ambiguities and restrictions, sparking discussions about the need for fundamental legislative change.[13]

Under Indian law, trade secrets are recognised as a sort of confidential information, protected by the equitable doctrine of breach of confidence. The underlying premise is that when a person obtains knowledge in confidence, they must not misuse it to the detriment of the person who disclosed it. This is especially essential in employer–employee interactions and commercial partnerships, where sensitive corporate information such as production processes, customer databases, pricing tactics, and technical know-how are regularly exchanged. Courts have consistently upheld the sanctity of such private agreements, understanding that the abuse or unauthorised disclosure of trade secrets can cause irreparable harm to corporate interests.

While contractual mechanisms—such as non-disclosure agreements (NDAs), non-compete clauses, and confidentiality clauses in employment contracts—form the backbone of trade secret protection, these too are subject to the constraints of Indian contract law. Section 27 of the Indian Contract Act, 1872, for instance, declares agreements in restraint of trade unenforceable, except in extremely limited instances. As a result, non-compete agreements are often not enforceable beyond the time of employment, so diminishing the legal armoury available to employers to prevent the misappropriation of trade secrets post-employment. Several sector-specific regulations grant incidental protection to trade secrets. The Information Technology Act, 2000 penalises the unlawful access or download of data from computer systems, which may overlap with trade secret theft in digital environments. The Copyright Act, 1957 and the Patents Act, 1970 also grant protection to some kinds of expression or innovations, but only when the information satisfies the threshold of originality or novelty, which trade secrets may not always fulfil. Thus, while these statutes provide supplemental support, they are not tailored to the special character of trade secrets. Recognising these shortcomings, legal experts, industry groups, and policymakers have urged for an independent trade secrets legislation in India. The need for reform has gained urgency in the backdrop of India's growing knowledge economy, increased foreign direct investment, and international commitments under the TRIPS Agreement, particularly Article 39, which obliges WTO

[13] N.S. Gopalakrishnan, "Trade Secret Protection: Need for a Legislative Framework", (2010) 35(1) Indian Bar Review 23.

ISSN (O): 2584-2196

members to protect undisclosed information against unfair commercial use. Although India has broadly complied with this need through court enforcement, the lack of a particular statute is sometimes considered as a regulatory deficiency in global comparisons.

In 2016, the Department of Industrial Policy and Promotion (now DPIIT), in its National IPR Policy, emphasised the necessity of trade secret protection and the need to investigate legislative remedies. The Policy promoted the creation of best practices and contractual templates for industry, but went short of recommending a statutory framework. Since then, there have been intermittent debates among legal circles on draughting a Trade Secrets Bill, although no real legislative proposal has yet materialised. A model trade secrets legislation for India would ideally include a clear definition of trade secrets, criteria for acceptable protection measures, civil and criminal sanctions for misappropriation, and procedural tools to ensure secrecy during litigation. It should also address permitted exceptions like as whistleblowing, independent discovery, and reverse engineering, so striking a balance between innovation and public interest. Lessons may be derived from international models, particularly the EU Directive and the US Act, both of which provide structured, transparent, and enforceable systems.

In the interim, courts continue to play an important role in evolving trade secrets doctrine. Recent rulings have proven a readiness to impose interim injunctions, pay punitive damages, and direct forensic investigations to secure electronic evidence. However, these remedies depend substantially on the quality of pleadings and evidence adduced by the parties, imposing a weight on litigants to structure their claims precisely. While India’s common law approach to trade secrets gives a fundamental layer of protection, its reliance on equitable principles and contractual agreements is no longer adequate in an era defined by data-driven business models and cross-border commercial transactions. The absence of a dedicated act generates legal ambiguity, reduces enforcement certainty, and potentially deters investment in innovation. There is a compelling need for comprehensive legislative reform to provide clear standards, effective remedies, and procedural safeguards appropriate to the complexities of trade secret protection in the modern economy. Such a step will not only enhance India's intellectual property framework but also align it more closely with global best practices.

ISSN (O): 2584-2196

JUDICIAL TRENDS AND KEY CASE LAWS

One of the earliest and most frequently cited judgments in this area is the ***John Richard Brady v Chemical Process Equipments Pvt Ltd***[14] where the Delhi High Court observed that confidential information developed or acquired by an employer during the course of business, including formulae, designs, and processes, is capable of protection under equity. The Court ordered an injunction to prevent former employees from exploiting such information in a competitive enterprise, even in the lack of a patent or official registration. This decision set the tone for identifying trade secrets as a sort of intellectual asset worthy of legal protection.

Similarly, in ***American Express Bank Ltd v Priya Puri***[15], the Delhi High Court examined the issue between employee mobility and the preservation of important corporate information. The Court held that while an employee is entitled to use their skills and expertise after resignation, they are not permitted to exploit trade secrets or sensitive client information received during the course of employment. However, the Court also highlighted that wide non-compete clauses must be scrutinised against the backdrop of Section 27 of the Indian Contract Act, 1872, which makes agreements in restraint of commerce unlawful. This case reflects the judiciary's effort to achieve a balance between commercial protection and individual liberty.

In ***Navigators Logistics Ltd v Kashif Qureshi & Ors***[16], where the Delhi High Court granted a perpetual injunction against former workers who had misappropriated the plaintiff's proprietary client lists and business ideas. The Court reaffirmed that in order to obtain remedy, the plaintiff must prove that the material was really confidential, not in the public domain, and subject to reasonable means of protection. The Court underscored that even in the absence of a written non-disclosure agreement, courts can infer an obligation of confidence from the nature of the relationship and the circumstances of disclosure.

The Bombay High Court, in ***Zee Telefilms Ltd v Sundial Communications Pvt Ltd***[17], expanded the scope of protection by holding that information shared during preliminary business negotiations—such as concept notes or ideas for television programming—could amount to confidential information, especially where it involved original thought and commercial

[14] (AIR 1987 Delhi 372),
[15] 2006 (3) LLJ 540)
[16] 2018 SCC OnLine Del 12156
[17] 2003 (27) PTC 457 Bom

potential. The Court followed the English standards given down in ***Coco v AN Clark (Engineers) Ltd,*** [18]so reinforcing the international underpinning of Indian trade secret jurisprudence.

In Tata Motors Ltd v State of Bengal (2008), though not centrally about trade secrets, the Supreme Court highlighted the importance of protecting confidential communications and commercially sensitive negotiations, reinforcing the broader judicial sentiment that confidentiality in business dealings must be preserved where legitimate. Notably, courts have also shown a willingness to safeguard digital forms of proprietary information. In ***Indian Farmers Fertiliser Cooperative Ltd v IFFCO Tokio General Insurance Co Ltd***[19], the Delhi High Court recognised that electronically stored data, if proven to be confidential and commercially valuable, warrants the same level of protection as traditional trade secrets. In granting temporary relief, the Court ordered forensic imaging of the defendants' devices, demonstrating the judiciary's openness to adopt technologically responsive remedies. At the same time, judicial interpretation has also drawn boundaries. In ***Bombay Dyeing & Mfg Co Ltd v Meher Mistry & Ors***[20] the Bombay High Court refused to award an injunction based on the worry that proprietary knowledge would be utilised, stressing the requirement for actual evidence of misappropriation. This caution reflects the courts' reluctance to restrict reasonable competition or employment migration in the absence of apparent wrongdoing. Overall, the judicial trend in India demonstrates a progressive increase of trade secret protection, founded in fair ideals yet sensitive to modern commercial realities. Courts have been crucial in establishing the limits of what constitutes confidential information, setting evidentiary criteria for relief, and clarifying the scope of enforcement of post-employment duties. However, these protections remain contingent on factual analysis and the specific pleadings of each case, often leading to contradictory outcomes.

The lack of established terminology and procedural clarity also places an onerous burden on parties to show the existence of trade secrets and the manner of their misuse. This judicial dependence on discretion, while flexible, also shows the limitations of the common law system. It is in this context that the call for a specific trade secrets statute takes significance. A

[18] [1969] RPC 41
[19] 2019 SCC OnLine Del 7949
[20] 2014 SCC OnLine Bom 1972

ISSN (O): 2584-2196

comprehensive legal framework would not only define the standards for protection and exceptions but also guide courts in adopting uniform principles across situations.

CONCLUSION

The protection of trade secrets in India continues to evolve through a common law framework grounded in equitable principles, contract law, and judicial interpretation. Despite the absence of a specific statute, courts have consistently recognised the importance of safeguarding confidential business information, particularly in the context of employment, technological innovation, and commercial competition. Judicial decisions have affirmed that trade secrets, though not statutorily defined, are enforceable through injunctions, breach of confidence claims, and restrictive covenants—provided that the information is proven to be confidential, commercially valuable, and subject to reasonable protection measures. However, the reliance on judicial discretion and the lack of statutory clarity often lead to unpredictability and inconsistent outcomes. This legal vacuum has triggered calls for legislative reform, especially to align Indian law with international standards such as the TRIPS Agreement and the EU Trade Secrets Directive. A dedicated statute would help in defining key concepts, establishing procedural safeguards, and outlining remedies for misappropriation. As India transitions into a knowledge-based economy, the need to foster innovation while balancing employee rights and competition makes trade secret protection a pressing legal imperative. Codifying this area of law would not only strengthen intellectual property protection but also boost investor confidence and global competitiveness.