A COMPARATIVE STUDY OF THE LAWS PERTAINING TO THE PROTECTION OF TRADE SECRETS IN INDIA, U.S., U.K., AND E.U.

Deepthi P D, LL.M in Intellectual Property and Trade Law, Christ (Deemed to be University), Bangalore.[1]

ABSTRACT

Trade secrets constitute a crucial component of intellectual property, offering protection to confidential business information that holds commercial value. With the rise of a knowledge-driven economy, safeguarding trade secrets has gained unprecedented significance, particularly in cross-border contexts where businesses operate under divergent legal regimes. This paper undertakes a comparative analysis of the laws pertaining to the protection of trade secrets in India, the United States, the United Kingdom, and the European Union. It traces the historical evolution and conceptual foundations of trade secrets, examines legislative frameworks, and analyzes judicial interpretations shaping the scope of protection across jurisdictions.

The study adopts a doctrinal and comparative methodology, relying on primary legal sources, case law, and secondary scholarly materials. It addresses four core research questions: the definitional and legislative contours of trade secrets; judicial interpretation in the selected jurisdictions; existing gaps in India's framework; and the best practices that may inform a robust statutory regime for India. The paper suggests the introduction of a comprehensive Indian trade secrets law drawing upon global best practices, explicitly defining key concepts, harmonizing remedies, and ensuring procedural safeguards. Such a framework would align India with international standards, enhance innovation protection, and facilitate cross-border commercial confidence.

Keywords: Trade Secrets, Confidential, Information, Commercial Value.

[1] Student of LL.M in Intellectual Property and Trade Law, Christ (Deemed to be University), Bangalore.

I. INTRODUCTION

The importance of intellectual property in the modern globalized and technology-based economy has grown manifold in regard to its role as an innovation driver, economic driver, and competitive driver. Of all types of IP, trade secrets hold a special status since they guard valuable business information without the procedural formalities and public disclosures that are common with patents, trademarks, or copyrights. Trade secrets typically cover confidential business content, including technical processes, manufacturing techniques, formulas, designs, customer databases, and marketing techniques, the unauthorized linking or exposure of which can damage the competitive position of the business.

The trade secret law in the U.S. became more uniform and federally protected with the passage of the Defend Trade Secrets Act (DTSA) in 2016 to supplement the Uniform Trade Secrets Act (UTSA). The DTSA does allow civil proceedings of misappropriation of trade secrets at the federal level and allows relief such as injunction, damages, and, in certain situations, the property may be seized to ensure its release.

Based on the common law principles of equity and breach of confidence, the United Kingdom revised its system with the Trade Secrets (Enforcement, etc.) Regulations 2018 to harmonize its national legislation with the European Union Directive (EU) 2016/943 on the protection of undisclosed know-how and business information. The Directive achieved harmonization of protection of trade secrets in EU member countries, with new common definitions and remedies, and safeguards, which enhanced commercial operations across borders in the EU.

By contrast, India does not have an independent law on trade secrets. The main sources of protection are the contractual requirements, the just principles of common law, and judicial precedents. Trade secrets have been identified as a set of actionable wrongs of breach of confidence or breach of contract by the courts, but the lack of codification of the law has resulted in disparities in protection, remedies, and methods of protection. The legal gap poses a challenge to businesses that run operations in India, especially in the information technology, pharmaceutical, and manufacturing business sectors, where proprietary information is the basis of competitive advantage.

Furthermore, as a result of globalization and digitalization, there is a high risk of cross-border trade secret misappropriation, and India needs to ensure that its internal system does not

contradict international standards. Jurisdictional comparisons such as the U.S., U.K., and EU provide an invaluable insight into other potential legislative models, enforcement, and judicial practices that India can borrow and/or adapt.

II. HISTORICAL AND CONCEPTUAL FRAMEWORK

Trade secrets are one of the oldest kinds of intellectual property protection, and they existed long before contemporary patenting and copyrighting regimes. The necessity to secure the confidentiality of business information is explained by the economic importance attached to knowledge that enables one to gain a competitive advantage. Mechanisms of early protection were based on equity and contract law, especially under the English common law principle of breach of confidence.[2] Courts realised that a lot of commercial damage could be suffered in the misuse of confidential information acquired under fiduciary relationships, employment contracts, or as mandated by other duties of fidelity. Cures were mostly fair, such as an injunction against disclosure and damages against any loss incurred.[3]

Trade secrets emerged as a legal concept in the United States, starting in the late 19th and early 20th centuries, as courts sought to place limits on what constituted a trade secret and to enforce trade secrets through what was deemed a reasonable effort to maintain confidentiality.[4] Early U.S. jurisprudence focused on trade secrets as a competitive advantage that needed to be preserved by reasonable measures, culminating in the 1979 creation of the Uniform Trade Secrets Act (UTSA) to offer a legal definition of trade secrets, a standard of misappropriation, and civil recovery[5]

In the United Kingdom, trade secrets were historically developed through the doctrine of breach of confidence, an equitable relief developed to deal with the misuse of confidential information.[6] In the United Kingdom, trade secrets were historically developed under the doctrine of breach of confidence, which established three elements of breach of confidence: the information must be confidential, the circumstances under which it was disclosed must impose an obligation of confidentiality, and the misuse of the information must have caused

[2] Coco v. A.N. Clark (Engineers) Ltd., [1969] RPC 41 (UK).
[3] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd., [1948] 65 RPC 203 (UK).
[4] Restatement (First) of Torts §757 cmt. b (1939).
[5] Uniform Trade Secrets Act §§1–7 (National Conference of Commissioners on Uniform State Laws 1979).
[6] Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018/1217 (UK); Directive 2016/943, 2016 O.J. (L 157) 1 (EU).

detriment. Part of this framework was codified into regulations in 2018 as Enforcement Regulations 2018, and includes the European Union Trade Secrets Directive 2016/943, which harmonizes definitions and enforcement measures among EU member states.

Directive 2016/943 was proposed by the European Union as a progression to establish a universal level of trade secret protection in all of the Member States.[7] Directive 2016/943 defines the concept of a trade secret and stipulates its lawful acquisition and use, as well as retaliatory measures against its misappropriation. The goal is to lessen legal uncertainty in cross-border operations and create innovation without excessive focus on the concept of the general will, including whistleblowing and reverse engineering. In the Directive, proportionality also focuses on the process of providing remedies, which means that protection measures should not be used to an unreasonable extent to impede lawful business operations.[8]

Trade secrets, in concept, are not registered and derive value solely through secrecy, which contrasts with patents, which, as a condition of obtaining a time-limited protective monopoly, must be publicly disclosed.[9] In the U.S., the U.K., and E.U. legal systems, trade secrets also generally incorporate the secrecy of the information, commercial value attaching to the secrecy, and reasonable efforts being made to ensure the secrecy. Trade secrets in India are mostly safeguarded by the contract law, equity, and judicial precedent because the country has no statute that is purely concerned with the protection of trade secrets.[10] Trade secret protection has also been developed through judicial precedent, focusing on the rights of the employer, the duties of the employee, and the relationship between the interests of the public. Cases including PepsiCo India Holdings Pvt. Ltd. v. Bharat Industrial Trading Co. and Tata Consultancy Services v. State of Andhra Pradesh provide examples of court enforcement of confidentiality by injunction, damages, and fair remedies.[11]

III. LEGISLATIVE FRAMEWORK IN INDIA, U.K., U.S., AND E.U.

- **INDIA:**

At present, a statutory regime on trade secrets does not exist in India. It is believed that

[7] Directive 2016/943, 2016 O.J. (L 157) 1 (EU).
[8] Id.
[9] Milgrim, Trade Secrets and Unfair Competition §1.01 (2022).
[10] PepsiCo India Holdings Pvt. Ltd. v. Bharat Industrial Trading Co., 2011 (44) PTC 209 (Del).
[11] Tata Consultancy Services v. State of Andhra Pradesh, 2006 (32) PTC 337 (AP).

protection of confidential business information is based mainly on the principles of common law, contractual obligations, and equitable remedies that ban employees from sharing any proprietary information with their competitors. Trade secrets are safeguarded through non-disclosure agreements (NDAs), employment contract confidentiality, and restrictive covenants.

Statutory protection is also provided as indirect protection. Violation of contractual duties that result in unauthorized disclosure of confidential information is a liability under the Indian Contract Act, 18723. On the same note, the Information Technology Act, 2000, prohibits unauthorized access, copying, or sharing of electronic data and thus offers secondary protection to digital trade secrets. These safeguards have been strengthened in the courtroom by judicial precedents. To take a typical example, in PepsiCo India Holdings Pvt. Ltd. v. Bharat Industrial Trading Co.,[12] the Delhi High Court affirmed injunctions and damages in cases of violation of confidentiality, and in Tata Consultancy Services v. State of Andhra Pradesh,[13] the court pointed out fair remedies in order to protect proprietary business information. Even with such measures, India tends to adopt greater reliance on case law and contracts, which results in inconsistency and uncertainty, especially in cross-border or technologically challenging cases.

- **UNITED KINGDOM**

Trade secrets in the U.K. are mainly safeguarded by the doctrine of breach of confidence at common law, which provides fair remedies in cases where confidential information has been disclosed, and the disclosure has resulted in detriment *Coco v. A.N. Clark Engineers Ltd*.[14]. It was determined that the three-pronged test of breach of confidence is: (i) must be of sufficient quality of confidence, (ii) must have been imparted in a situation which created an obligation of confidence, and (iii) must have caused detriment.

To extend the scope of statutory protection, the Trade Secrets (Enforcement, etc.) Regulations 2018 were introduced to enforce the EU Trade Secrets Directive 2016/943.[15] These regulations define the lawful acquisition and use of trade secrets and disclosure and provide remedies such as injunction, damages, and remedial action. The UK framework, therefore, incorporates both loose fair principles and statutory codification to provide businesses with a more certain legal

[12] Information Technology Act, No. 21 of 2000, §§ 43, 66.
[13] Tata Consultancy Services v. State of Andhra Pradesh, 2006 (32) PTC 337 (AP).
[14] Coco v. A.N. Clark (Engineers) Ltd., [1969] RPC 41 (UK).
[15] Directive 2016/943, 2016 O.J. (L 157) 1 (EU).

framework, especially in cases involving international transactions.

- **UNITED STATES**

The US has one of the most established statutory legislations regarding trade secrets. Most states have adopted the Uniform Trade Secrets Act (UTSA), 1979,[16] which defines trade secrets, provides rules on misappropriation, and describes civil remedies such as injunctions, damages, and exemplary damages in cases of willful violation. The UTSA points out that the information should be economically valuable by virtue of its secrecy and that the owner should exercise reasonable efforts to ensure the information is kept confidential.

In 2016, a new cause of action, the Defend Trade Secrets Act (DTSA), was enacted, which allowed owners of trade secrets to initiate a suit in a federal court and obtain such remedies as ex parte seizure and statutory damages. To strike a balance between trade secret protection and employee mobility and competition, federal courts have continually interpreted these statutes. In the case *Kewanee Oil Co. v. Bicron Corp.*,[17] the Supreme Court had acknowledged the economic worth of trade secrets and had found that protection of trade secrets at the state level was justified, but in PepsiCo, Inc. v. Redmond,[18] the court had demonstrated how the courts can prevent employee misuse of information and still support a free labor market. The U.S. framework also protects whistleblowers and disclosure of the public interest, so that the enforcement of trade secrets does not hamper good-faith reporting of misconduct.

- **EUROPEAN UNION**

The Trade Secret Directive 2016/94317 is the first harmonized system of protection of trade secrets in all EU Member States. A trade secret is a type of information that is secret, has a commercial value owing to its secrecy, and is the subject of reasonable efforts to keep it confidential.[19] The Directive itself outlaws unlawful acquisition, use, or disclosure of trade secrets and provides remedies such as injunctions, damages, and corrective measures. The application of the Directive in national laws by 20 Member States, including the U.K. prior to Brexit, brings consistency in the protection standard, as well as in balancing overall public

[16] Uniform Trade Secrets Act §§1–7 (National Conference of Commissioners on Uniform State Laws 1979).
[17] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).
[18] PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).
[19] Directive 2016/943, 2016 O.J. (L 157) 1 (EU).

interests, including whistleblowing, freedom of expression, and reverse engineering.

- **Comparative Insights**

There are major differences and similarities as a comparative analysis demonstrates:

The U.S. and E.U. offer codified statutory frameworks that have specific definitions, remedies, and enforcement tools.

The U.K. has integrated the principles of flexible common law with statutory laws that are based on EU directives.

India is a country of contract and judicial precedents with no specific law addressing the issue of trade secrets, which creates legal loopholes in clarity, predictability, and enforcement.

The differences highlight why India ought to think about codifying the protection of trade secrets in a broad statute. Such a law might have aspects of U.S. federal, EU harmonization, and U.K. equitable flexibility, thus giving definite definitions, remedies, and enforcement systems of business that is conducted within the country and abroad.

IV. JUDICIAL INTERPRETATIONS

Trade secrets protection is mostly enforced by means of equitable remedies and contractual obligations in India, since there is no independent statute. The breach of confidentiality and contractual limitations has been used in courts as a measure to protect confidential business information. An example of this is *PepsiCo India Holdings Pvt. Ltd. v. Bharat Industrial Trading Company*,[20] where the High Court of Delhi passed injunctions to prevent the misuse of PepsiCo's confidential information, the court observed that commercial secrecy is vital. On the same note, in Tata Consultancy Services v. State of Andhra Pradesh, [21] the court stressed that the employers have the right to injunctions and damages in such cases when disclosure of proprietary information or trade secrets was made without proper permission.

F. Hoffmann-La Roche Ltd. v. Cipla Ltd.,[22]is another case that the Delhi High Court has upheld, in which trade secrets in the form of confidential pharmaceutical formulae were found to have

[20] PepsiCo India Holdings Pvt. Ltd. v. Bharat Industrial Trading Co., 2011 (44) PTC 209 (Del).
[21] Tata Consultancy Services v. State of Andhra Pradesh, 2006 (32) PTC 337 (AP).
[22] F. Hoffmann-La Roche Ltd. v. Cipla Ltd., CS (OS) No. 1524/2008 (Delhi High Court).

economic and competitive importance. Indian courts have always maintained a balance between the proprietary interests of the employer and the right of mobility of the employee. It is rather argued that the misuse of information is not a matter of knowledge per se.

In the U.K., there is a strong history of safeguarding trade secrets using fair principles via the doctrine of breach of confidence. In the legendary case of *Coco v. A.N. Clark Engineers Ltd*.[23], it was found that the three-part test required the information to be: secret, it must have been taught in such a situation that it is subjected to an obligation of secrecy, and abuse must lead to harm.[24] In *Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd*.,[25] the court emphasized that the employees or the former business associates should not misuse the confidential technical information acquired during the employment or in the course of the contract. These principles were later codified in the Trade Secrets (Enforcement, etc.) Regulations 2018, which incorporate the EU Trade Secrets Directive 2016/943 standards, and give statutory support to equitable remedies, including injunctions, damages, and corrective action.[26]

The United States offers extensive judicial protection to trade secrets pursuant to the Uniform Trade Secrets Act (UTSA) and the Defend Trade Secrets Act (DTSA). The importance of secrecy, reasonable protective measures, and misappropriation prevention has been stressed in courts.[27] In *Kewanee Oil Co. v. Bicron Corp.,*[28] the Supreme Court acknowledged that trade secrets were a valuable type of intellectual property worth protection, and that the trade secret law promoted innovation without undermining healthy competition. The doctrine of inevitable disclosure was used by the Seventh Circuit in *PepsiCo, Inc. v. Redmond*,[29] where a former employee was prohibited from taking over a competitor, in which his awareness of confidential information could be inalienably used against the competitor.

In the same way, in *Douglas Dynamics, LLC v. Buyers Products Co*., the court expanded the UTSA definition of misappropriation and strengthened remedies such as injunctive relief, damages, and attorney fees in case of willful breach. Another power granted to the owners of

[23] Coco v. A.N. Clark (Engineers) Ltd., [1969] RPC 41 (UK).
[24] Id.
[25] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd., [1948] 65 RPC 203 (UK).
[26] Directive 2016/943, 2016 O.J. (L 157) 1 (EU).
[27] Uniform Trade Secrets Act §§1–7 (National Conference of Commissioners on Uniform State Laws 1979).
[28] Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974).
[29] PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).

trade secrets by the DTSA is to seek federal relief and ex parte seizure to demonstrate to the court that they have a sound judicial system to protect them.

Courts in the E.U. have been relying on Directive 2016/943 to harmonize the definitions of trade secrets, their acquisition terms, and remedies across the board. The E.U. framework, which balances precariously between the protection of trade secrets and exceptions applied to the protection of the popular interest, such as whistleblowing, the disclosure of investigative information, and the disclosure of regulatory information.[30]

India is based on fair remedy and contract law, and by precedent, courts are slowly developing trade secret protection. The U.K. is a statutory codification of common law based on EU standards. The U.S. enjoys an excellent statutory regime with federal and state relief (injunctions, damages, ex parte). The EU balances the interests of businesses against the policy exception by harmonizing the protection of trade secrets across Member States. Finally, these interpretations point to the value of written protection, judicial certainty, and binding solutions, and this can lead to the suggestion that India could benefit by adopting a statutory model that incorporates good practice in these jurisdictions.

V. GAPS IN THE INDIAN LEGAL FRAMEWORK

The result of this deficiency is legal ambiguity, in particular, the meaning of the trade secrets, the procedure of remedies, and the conceptualization of the relevant procedural rules to adhere to when enforcing the remedies.

There is no statutory protection of trade secrets in India. As opposed to the U.S. and the Defend Trade Secrets Act of 2016, or to the EU and the Directive 2016/943, India is based on contractual duties, fair principles, and ancillary statutes. The Indian law protects the trade secrets primarily on the basis of contractual agreements and fair remedies. It is common in a country like India, where businesses are uncertain of the misuse of their confidential data, particularly in foreign business dealings or in the hands of technologically endowed sectors.

That narrow scope can also threaten the commercial value of proprietary information, as the law does not always offer relief in cases of misuse by third parties who do not themselves enter into the contract. As a result, this has resulted in protection being provided to parties that have

[30] Directive 2016/943, 2016 O.J. (L 157) 1, pmbl.

expressly signed confidentiality agreements at the expense of other possible breaches, including disclosure by former employees or non-parties under a contract, which is poorly covered. This kind of ambiguity affects businesses that would like to claim a proprietary right on some proprietary process, formula, or technical knowledge because various courts may interpret various information as a secret or commercially valuable information.

There is no statutory definition of trade secrets in India, and this has led to varying judicial interpretations. Protection is determined on an ad hoc basis by the courts based on breach of confidence principles or on contractual clauses.

India does not have an easy way out on the enforcement of trade secret protection. Injunctions or damages are usually granted by the courts, and such things as ex parte seizure or protection orders are not allowed in the U.S., as they are with the DTSA. The cost of waiting to pursue a legal case can cause potential commercial damage that is irreparable to the business, as firms may struggle to stay in the competitive spotlight while awaiting the legal decision.

The existing Indian laws do not explicitly deal with trade secret misappropriation, industrial espionage, or trade secret theft via the Internet. Whereas the Information Technology Act, 2000, affords to some degree the protection against unauthorized access, it is not designed to specifically address trade secrets and commonly lacks the capacity to combat highly technological or Web-related violations.

The compensatory damages and injunctions awarded by Indian courts mainly concern misappropriation, but punitive or exemplary damages are not provided by statute. Unless there are deterrence controls, deliberate or systematic misappropriation can go unchecked, making it less appealing to the company to invest in innovation, or their own-resourced research.

VI. SUGGESTIONS AND BEST PRACTICES

India needs to implement a complete statutory law specially designed to safeguard trade secrets. Trade secrets should be spelled out under this law, misappropriation acts identified, and remedies put in place that are enforceable. According to the U.S. DTSA and EU Directive 2016/943, the law can provide clarity and predictability, and companies can be confident that their proprietary data is safeguarded in court. A codified law would also harmonize judicial interpretations and would avoid the use of ad hoc equitable remedies and inconsistent

enforcement of contracts.

To increase its implementation, India must implement enforcement strategies such as ex parte injunctions, protective orders, and accelerated hearings. Like the options offered by the U.S. DTSA, these measures would enable companies to avoid irreparable commercial damage when litigation is pending. Rapid delivery systems are especially relevant to time-sensitive proprietary data, including technological breakthroughs or research information.

The Act must also clearly cover cyber theft, industrial espionage, and online trade secret disclosure. India can guarantee that digital and technological misappropriation is effectively avoided by combining the provisions related to the Information Technology Act, 2000, with the trade secret-related provisions. Businesses increasingly reside online, and effective cyber defences are critical to protecting competitive advantage.

To discourage deliberate misappropriation, India needs to include remedies like compensatory damage, exemplary or punitive damage, and the reimbursement of profits. The U.S. and EU experience shows that civil remedies can be reinforced with deterrent approaches as a way to improve the level of compliance and minimize litigation. The availability of statutory guidelines on damages and equitable remedies will foster investment in research and innovation by businesses.

The law must find a balance between preserving trade secrets and the freedom of movement of employees. The U.S. inevitable disclosure doctrine of best practice and the U.K. doctrine of breach of confidence may be relevant to inform Indian laws in ensuring that former employees do not use confidential information to the disadvantage of the company, and that it does not constrain career mobility. Whistleblower provisions should be clearly written so that the interests of the population are not jeopardized.

India must be able to harmonise its trade secret regime with global best practices, in terms of definitions, enforcement systems, and procedural protections. Such harmonization would ease business operations across borders, promote foreign investments, and improve the image of India as a safe haven for innovation-driven sectors. Compliance with U.S., U.K., and EU regulations will also assist Indian firms in securing their intellectual property rights across international borders.

Finally, India must promote the sensitisation of companies and employees concerning the protection of trade secrets. To prevent inadvertent disclosure, companies are encouraged to implement internal compliance practices, regular training, and robust NDAs. With statutory enforcement coupled with legal literacy, the culture of proactive confidentiality and accountability in corporate India will be developed.

VII. CONCLUSION

The protection of trade secrets can be recognized as one of the most significant issues as far as the promotion of innovations, protection of the economic interests, and competition in the strongly knowledge-based global economy are concerned. This paper has revealed that although India offers certain protection in the form of contractual obligations, equitable remedies, and ancillary legislation like the Indian Contract Act, 1872, and the Information Technology Act, 2000, no unified statutory framework exists to offer a clear, enforceable, and deterrent basis.

As can be proved by comparative law, there exists effective protection in such jurisdictions as the United States, the United Kingdom, and the European Union because laws, procedures of redress, and harmonized procedures of enforcement are codified. The U.S. DTSA makes federal remedies, ex parte seizure, and whistleblower protection clear and predictable. The U.K. has common law principles codified by statute under the Trade Secrets (Enforcement, etc.) Regulations 2018, and the EU Directive 2016/943, achieve a balance between commercial confidentiality and exceptions to the public interest by harmonizing the protection of trade secrets between Member States.

Through judicial rulings, Indian courts have, over time, interpreted the protection of trade secrets and have shown that the judiciary is capable of developing fair solutions. However, the problems of enforcement, absence of specifications in legislation, vulnerability of the Internet, and absence of preventive schemes reveal the significance of a legal statutory framework. It is proposed by the study that India needs a complete trade secret law, with clear definitions, enforceable solutions, procedural improvements, including ex parte injunctions, online safeguards, and remedies against misuse to prevent theft. Moreover, the harmonization of the practices, equitable protection of the mobility of the employees, and corporate compliance will have to be organized internationally to establish the environment that will trigger the innovations and foreign investments.

Finally, the reinforcement of the Indian trade secret system is not only a legal requirement but also an economic one. Through best practice adoption in the top performers. In India, jurisdictions can help businesses enjoy predictable, efficient, and enforceable proprietary information protection, thus enhancing business and global innovation, competitiveness, and sustainable growth.