



Trade Secrets as a Form of Intellectual Property Right (IPR)

*Jaykumar Pansuriya¹, Arjun Dudhatra¹, Sanjay Chandapa¹, Jay Patoliya², Anand Kavar²,
Ranjit Modhvadiya², Fenil Patel³, Yuvaraj Bheda⁴ and Dr. H. B. Limbani⁵

¹PG Scholar (Genetics and Plant Breeding), College of Agriculture, JAU, Junagadh

²PG Scholar (Seed Science and Technology), College of Agriculture, JAU, Junagadh

³PG Scholar, Department of Entomology, College of Agriculture, JAU, Junagadh

⁴PG Scholar, Department of Biochemistry, College of Agriculture, JAU, Junagadh

⁵Assistant Professor, Department of Genetics and Plant Breeding, College of
Agriculture, JAU, Junagadh, Gujarat, India

Corresponding Author's email: pansuriyajay007@gmail.com

Trade secrets represent a cornerstone of modern industrial asset protection, offering corporate enterprises an alternate, indefinite mechanism for safeguarding high-value innovations outside standard patent systems. This review paper provides a structured and granular overview of the legal definitions, structural parameters and institutional criteria determining trade secret validity under international frameworks such as the TRIPS Agreement, the US Defend Trade Secrets Act (DTSA) and the EU Trade Secrets Directive. Crucially, this paper synthesizes emerging operational dynamics from the 2025-2026 landscape, mapping a historic 20% surge in litigation, heightened judicial scrutiny requiring precise identification of misappropriated information and existential threats posed by generative AI models through prompt injection attacks and permanent data encoding. Finally, it addresses the expanding geopolitics of cyber-espionage targeting agricultural seed technology and R&D. The paper concludes with an integrated review layout mapping future directions for intellectual property strategy.

Keywords: Trade Secrets, Intellectual Property Rights, TRIPS Agreement, Generative AI, Cyber-Espionage, Seed Technology, Comparative Jurisprudence.

Introduction

Intellectual Property Rights (IPR) are structural tools that incentivize innovation and secure global commercial market shares. While patents, trademarks and copyrights have historically dominated formal institutional registries, trade secrets have emerged as an equally potent and strategically dynamic legal mechanism. A trade secret represents any form of confidential business information that provides an enterprise with a distinct, measurable competitive advantage over market rivals.

Unlike patent protection, which mandates strict public disclosure of an innovation in exchange for a time-bound legal monopoly, trade secret protection operates through a framework of continuous operational confidentiality. Consequently, trade secrets require no centralized state registration, bypass fixed legal expiration horizons and apply across an expansive, non-standardized array of proprietary methodologies, algorithms, economic datasets and negative know-how. This review examines the doctrinal criteria governing trade secrets, evaluates their strategic utility against patents and delineates the legal vulnerabilities arising from recent technological shifts between 2025 and 2026.

Legal Criteria and Jurisdictional Definitions

To achieve legal protection and qualify for actionable judicial remedies under global tort, contract or statutory law, proprietary information must rigorously satisfy structural criteria. Under Article 2 of the European Union Trade Secrets Directive (2016/943), undisclosed information must comprehensively meet three concurrent thresholds to be legally categorized as a trade secret:

Objective Secrecy: The subject matter must be secret in the sense that it is not generally known among or readily accessible to persons within the specialized professional circles that normally handle the specific information type.

Derived Economic Value: The asset must possess explicit or latent commercial value precisely because it is kept confidential, meaning its exposure to competitors would immediately erode the owner's economic advantage.

Reasonable Protection Measures: The lawful controller must have actively implemented reasonable, systematic steps under the prevailing circumstances to ensure the information remains classified.

Parallel statutory rules are codified in the United States under the Defend Trade Secrets Act of 2016 (DTSA). The DTSA demands that the corporate owner employ active, verifiable internal and external “reasonable measures” to maintain structural secrecy. If an organization fails to demonstrate adequate physical, digital or contractual safeguards, courts will deny legal protection and rendering the technical asset public domain.

Taxonomy of Protectable Subject Matter

The informational criteria protectable under trade secret regimes are remarkably diverse, cutting across technical, financial and operational sectors. Broadly, these assets are classified into five core industrial domains:

Chemical Formulas and Recipes: Industrial compounds, soft drink concentrates (e.g., the iconic Coca-Cola Merchandise 7X formula) and cosmetic material mixtures.

Industrial Processes and Methods: Proprietary metallurgy steps, distinct manufacturing workflow speeds, specialized refining techniques and unpatented engineering procedures.

Digital Architectures and Algorithms: Unpublished software source code, unique proprietary search logic, neural network weighting matrices and trading automation scripts.

Commercial Intelligence and Compilations: Structured consumer databases, specialized procurement lists, unannounced corporate pricing tables and private distribution networks.

Negative Know-How: Documentation charting research and development dead-ends, failed experimental equations or defective material combinations. Negative know-how holds massive commercial value by allowing an entity to bypass redundant, multi-million-dollar R&D paths already pursued and eliminated by competitors.

Comparative International Legal Frameworks

Global compliance and baseline minimum definitions are anchored by key international conventions, though enforcement mechanisms remain fractured across individual states.

Table 1. Summarizes the core global instruments governing trade secret validation.

Regulatory Instrument	Primary Sovereign Scope	Core Enforcement & Jurisprudential Impact
TRIPS Agreement	Global (WTO Members)	Establishes the foundational international baseline for protecting undisclosed data against unfair competition.
EU Directive 2016/943	European Union Member States	Harmonizes regional judicial definitions, structures uniform civil remedies and legally safeguards reverse engineering.
US DTSA (2016)	United States (Federal)	Creates an expansive federal civil cause of action, enabling nationwide injunctions and ex part property seizure rules.

Indian Common Law Matrix	Republic of India	Lacks standalone statutory trade secret acts; relies on equity, tort law and Section 27 of the Indian Contract Act.
--------------------------	-------------------	---

Strategic Intellectual Property Bifurcation

A critical operational challenge for corporate management is deciding whether to pursue patent registration or maintain an asset as a trade secret. This structural choice alters an organization's competitive profile.

Table 2. Provides a comprehensive strategic matrix.

Strategic Dimension	Patent Protection Pathway	Trade Secret Protection Pathway
Legal Mechanism	State-sanctioned exclusive rights in exchange for explicit public disclosure.	Continuous structural confidentiality; no state disclosure required.
Temporal Duration	Strictly limited to a fixed term (typically 20 years from filing date).	Potentially infinite; exists as long as secrecy is operationally maintained.
Financial Outlays	High upfront filing, examination and recurring sovereign annuity fees.	Negligible filing fees; variable long-term cybersecurity/compliance costs.
Reverse Engineering	Prohibited; patent claims block independent development.	Perfectly legal if achieved through honest, proper analytical means.
Sovereign Registries	Requires comprehensive examination by government patent offices.	Bypasses all state registration, testing and public notice mandates.

Contemporary Disruptions and Global Trends (2025-26)

1. Surge in Litigation and Judicial Skepticism

The period between 2025 and 2026 marked an inflection point in trade secret enforcement. Empirical tracking of United States federal filings recorded a historic 1,552 trade secret cases in 2025—a 20% year-on-year escalation since the baseline trends of 2024. This surge is driven by increased employee mobility, hybrid decentralized remote work models and rapid cloud-based digital file dissemination. Concurrently, the judiciary has pushed back against ambiguous claims. Corporate litigants in 2025 face severe skepticism from judges who increasingly reject overly broad complaints. The prevailing legal precedent requires companies to identify their trade secrets with technical precision early in the discovery phase or risk immediate case dismissal (Greenberg Traurig, 2026).

2. Generative AI and Algorithmic Secrecy Crises

Generative Artificial Intelligence (AI) has introduced complex vulnerabilities to proprietary data. Two landmark judicial cases from 2025 highlight this legal frontier:

Permanent Model Encoding: In *Intercept Media, Inc. v. OpenAI, Inc.* (S.D.N.Y. 2025), the court observed that when proprietary datasets are used to train large-scale neural networks, the underlying data points become permanently encoded within the non-linear weights of the final model memory. This makes extraction or deletion virtually impossible, transforming inadvertent data ingestion into an un-remediable, permanent leak.

Adversarial Prompt Injection: In *Open Evidence, Inc. v. Pathway Medical, Inc.* (D. Mass. 2025), the judiciary evaluated whether advanced prompt injection attacks—where external actors engineer malicious input queries to extract hidden system prompts or underlying training metrics—constitute actionable “improper means” under trade secret statutes.

3. Geopolitical Cyber-Espionage in Agribusiness and Seed Technology

Beyond software industries, the agricultural sector has emerged as a high-stakes battleground for trade secret misappropriation. Sophisticated, state-backed cyber-espionage groups have shifted focus toward corporate seed research, elite crop genetics and automated phenotyping

datasets. Rather than navigating lengthy regional patent applications, adversarial nation-state actors target highly sensitive agricultural intellectual property directly from R&D servers to circumvent global regulatory frameworks. This has forced major agribusinesses to reallocate capital toward operational security, secure supply chains and international compliance measures (Cybersecurity Dive, 2025).

4. Chinese Rights-Protective Judicial Reforms

Concurrently, China's Supreme People's Court (SPC) Intellectual Property Tribunal has executed strategic shifts in its 2025 civil jurisprudence. Across several published landmark rulings, the SPC demonstrated an aggressive, rights-protective framework characterized by a sharp escalation in statutory punitive damages, a systematic relaxation of the burden of proof for plaintiff innovators and severe evidentiary sanctions penalizing corporate defendants for data and evidence spoliation (China IPR, 2026).

Structural Challenges and Limitations

The primary weakness of trade secret protection lies in its absolute fragility. If a secret is made public-whether through a targeted cyber breach, employee negligence or public disclosure-all statutory legal protection terminates immediately. Once the information is unprotected, it cannot be pulled back or restored to a proprietary state. Furthermore, independent parallel innovation and reverse engineering remain entirely lawful. Consequently, entities operating in hyper-competitive markets face structural risks when relying solely on trade secrets, particularly as automated decompilation, edge-computing extraction and generative AI models accelerate.

Conclusion and Future Recognitions

As the global knowledge economy shifts toward rapid digital integration and algorithmic development, trade secrets have become essential elements of organizational value. The legal dynamics of 2025-2026 show that traditional confidentiality steps are no longer sufficient against modern technological challenges. Moving forward, enterprises must integrate rigorous legal contracts with proactive cybersecurity measures-especially when deploying artificial intelligence tools and safeguarding specialized agricultural technologies. To maintain actionable protection in courts worldwide organizations must treat trade secret governance as a dynamic, continuous operational process rather than a passive legal status.

References

1. Benesch, Friedlander, Coplan & Aronoff LLP. (2026). Trade secret and restrictive covenant: 2025 year in review. *Benesch Law Insights*.
2. Berkeley Technology Law Journal. (2026). From patents to privacy: The strategic turn toward trade secrets in the AI era. *BTLJ Analysis*, **41(2)**: 112-129.
3. China IPR. (2026). Analyzing trade secret protections: 2025 civil trends in China's Supreme People's Court IP Tribunal. *China IPR Legal Blog*.
4. Cybersecurity Dive. (2025). Food and agriculture sector faces elevated threat landscape from nation-state trade secret espionage. *Cybersecurity Dive Reports*.
5. EU Trade Secrets Directive. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8th June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *EUR-Lex*.
6. Greenberg Traurig LLP. (2026). Trade secrets 2025 in review: Judicial skepticism and precision trends. *GT Insights*.
7. TRIPS Agreement. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights, Article 39, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization.