ANALYSING LEGAL CHALLENGES IN ENFORCING TRADE SECRETS AND AI

Muthulakshmi B, Sastra Deemed to be University, Thanjavur

Vahitha Parveen A, Sastra School of Law

ABSTRACT

The increasing integration of artificial intelligence (AI) technologies into business operations has significantly impacted the development, safeguarding and potential misappropriation of trade secrets. Determining precisely what qualifies as a trade secret frequently depends heavily on the knowledge and inventiveness of business legal advice. This results in a broad interpretation that goes beyond the conventional limits of what constitutes a trade secret. This study examines the meaning and significance of trade secrets in the business world, especially in light of advancements in artificial intelligence. Proprietary models, training data, and algorithms are examples of trade secrets, which give businesses significant competitive advantages. Enforcing these rights, particularly within the Indian legal framework, is made more difficult by the quick development of AI. Businesses need to foster a culture of understanding about the importance of trade secrets and make sure that every employee knows their part in protecting confidential data. The current legal systems controlling trade secrets in the US and India are both examined in this paper. The study emphasises the challenge it is to uphold trade secret rights in the face of developing AI technology. Ultimately, this research aims to provide insights into best practices for safeguarding trade secrets in AI-driven sectors. By fostering collaboration among legal experts, technologists, and policymakers, businesses can better navigate the complexities of trade secret enforcement in an increasingly AI-centric landscape.

Keywords: Trade Secrets, Artificial Intelligence, Algorithms, Confidentiality, Legal framework.

I. INTRODUCTION

Business operations have been transformed by the incorporation of artificial intelligence (AI) technology, which have increased productivity and creativity in a number of industries. But this quick development also brings up important legal issues, especially with regard to trade secret enforcement. In an AI-driven environment, trade secrets—defined as exclusive business knowledge that gives an advantage—are more susceptible to theft. The complex relationship between artificial intelligence (AI) and trade secrets is examined in this paper, with particular attention paid to how definitions and perceptions of what qualifies as a trade secret have changed in response to technical developments. With increasing sophistication, AI systems may now analyse large databases and produce insights that could unintentionally reveal confidential information.

Businesses now have to deal with the possibility that AI will comprehend or duplicate their exclusive processes and algorithms, which confuses the conventional concept of trade secrets. Examining current laws and their efficacy in safeguarding confidential data is crucial since the legal frameworks governing trade secrets in the US and India are having difficulty keeping up with these developments. Furthermore, it's critical to cultivate an organisational culture that recognizes the value of trade secrets. Workers must be aware of their responsibilities to protect sensitive information, especially when using AI tools that might not sufficiently filter it. In order to successfully negotiate the complexity of trade secret enforcement, this study intends to shed light on best practices for trade secret protection in AI-driven industries while emphasising the necessity of cooperation between legal professionals, engineers, and legislators. In conclusion, it is critical to comprehend the implications for trade secret protection as companies depend more and more on AI technologies. This paper will examine the legal issues raised by advancements in artificial intelligence and offer solutions for improving trade secret protection in a constantly changing digital environment.[1]

II. LITERATURE REVIEW

The paper titled "**Into Uncharted Waters: Trade Secrets Law in the AI Era" by Burcu Kilic**, explores the expanding use of trade secrets law to protect AI algorithms, highlighting how this can limit transparency and accountability. Companies increasingly shield AI source code, algorithms, and training data as trade secrets, creating "black boxes" that

[1] Kilic, B. (2024). *Into uncharted waters: Trade secrets law in the AI era* (No. 295). CIGI Papers.

restrict public and regulatory access. This broad protection conflicts with public interest, especially in sectors like health and safety where transparency is critical. The paper argues for balanced legal reforms to allow necessary public scrutiny of AI while protecting legitimate business secrets, suggesting that trade secrets laws need clearer boundaries to accommodate AI's unique transparency challenges.[2]

The paper titled **"Untangling the Legal Complexities of Trade Secrets And AI" by Joshua Lerner and Nora Passamaneck** examines the suitability of trade secret law for protecting innovations in generative artificial intelligence (AI). It highlights challenges faced by generative AI under traditional intellectual property laws like patents and copyrights, which often require human inventorship and specific thresholds for eligibility. In contrast, trade secret law—particularly under the U.S. Defend Trade Secrets Act (DTSA)—offers broader applicability by encompassing various forms of information and does not require human authorship. However, leveraging trade secret protection for AI is fraught with challenges. The authors discuss three primary requirements for trade secrets: specificity in identification, reasonable measures to ensure secrecy, and deriving independent economic value from being unknown. The dynamic and complex nature of AI systems, such as evolving algorithms and training data, complicates compliance with these criteria. The authors also emphasize that companies must adopt context-specific measures to protect trade secrets, including tailored confidentiality agreements and security practices, as generic solutions are insufficient for AI's unique demands. The article enriches ongoing debates about the intersection of AI and intellectual property law. It bridges gaps in existing frameworks by proposing a nuanced approach to using trade secrets for AI innovations, recognizing the limitations of patents and copyrights in this domain. Future research might explore alternative protection mechanisms or adapt existing laws to better address AI's complexities[3].

The paper titled **"Keeping ChatGPT a Trade Secret While Selling It Too" by Camilla A. Hrdy** explores how companies, like OpenAI with ChatGPT, protect AI algorithms as trade secrets while making them widely available to the public. By using closed-source structures and restrictive terms of use, companies prevent users from accessing or reverse-engineering the underlying models. These contracts often contain anti-reverse engineering

[2] Kilic, B., 2024. *Into uncharted waters: Trade secrets law in the AI era* (No. 295). CIGI Papers.
[3] Joshua Lerner & Nora Passamaneck, *Untangling the Legal Complexities of Trade Secrets and AI*, Law360 (Mar. 26, 2024).

and non-compete clauses, creating legal barriers that extend beyond traditional contract law into trade secret protections. However, the author argues that once an AI product becomes easily reverse-engineered by the public, trade secret protections should no longer apply, advocating for clearer boundaries in trade secrets law to balance transparency with business confidentiality.[4]

The paper titled "**My AI, my code, my secret. How trade secrets (will) impact the right to effective review under the EU's AI Liability Directive Proposal" by Ljupcho Grozdanovski,** discusses the EU's AI Liability Directive (AILD), which allows victims of harm from high-risk AI systems to request evidence in court but also protects AI algorithms as trade secrets. This creates a tension between ensuring transparency for fair trials and maintaining companies' competitive edge. The AILD aims to balance these interests by enabling limited disclosure of evidence while protecting trade secrets, thus addressing both the need for judicial transparency and market fairness.[5]

III. RESEARCH PROBLEM

The primary research problem is the inadequacy of existing legal framework to effectively govern the use of AI algorithms as trade secrets.

IV. RESEARCH OBJECTIVES

1. To Assess the gaps in existing legal framework related to trade secret.
2. To Recommend best practices for combating challenges faced by artificial intelligence in trade secrets.

V. RESEARCH QUESTIONS

1. How do current legal frameworks address issues related to trade secrets?
2. What recommendations can be made to improve the legislative framework to combat the challenges faced by the artificial intelligence in trade secrets?

VI. RESEARCH METHOD

The research methodology is based on the doctrinal research. The most relevant secondary data had been collected from authentic sources. The data used here has been collected from

[4] Hrdy, C.A., 2024. Keeping ChatGPT a Trade Secret While Selling It Too. *Berkeley Technology Law Journal (forthcoming 2025)*.
[5] Grozdanovski, L., My Ai, My Code, My Secret.

different books, articles, journals and legislations.

VII. DEFINITION OF TRADE SECRETS

A trade secret is a kind of intellectual property that gives a business a competitive edge and is made up of exclusive business knowledge. Trade secrets, as opposed to patents or trademarks, are not registered and depend on the owner's efforts to keep them private. Proprietary algorithms, designs, procedures, and formulas are typical examples. Laws such as the Defend Trade Secrets Act in the United States provide legal protection for trade secrets, allowing firms to function without worrying about their private information being revealed. Commercial value and confidentiality through nondisclosure agreements and restricted access are prerequisites for knowledge to be considered a trade secret. Trade secrets are crucial for promoting economic growth and innovation because they enable businesses to develop new concepts and technologies without worrying about being copied right away, giving them a competitive edge in the market.[6]

VIII. LEGAL FRAMEWORK FOR TRADE SECRETS

1. US legal framework for trade secrets

The intersection of artificial intelligence (AI) and trade secrets has become a pivotal topic due to AI's growing influence and the inadequacy of traditional intellectual property protections like patents and copyrights. The Defend Trade Secrets Act (DTSA), can offer protection for AI innovations without the human authorship requirement demanded by patents and copyrights (Trade Secrets and AI). AI’s unique aspects, such as dynamic learning algorithms, evolving data sets, and difficulty in pinpointing specific trade secrets, pose challenges under trade secret law. The document underscores the requirement for companies to adopt tailored measures—like confidentiality agreements and restricted access policies—to protect AI assets effectively (Trade Secrets and AI). Overall, the emphasis on AI in the trade secret domain highlights its potential for broad applicability while addressing nuanced challenges of information secrecy and economic value derivation. For AI, these laws may need to evolve further to address its unique dynamic nature. All things considered, the focus on AI in the trade secret space emphasises its potential for wide use while tackling the complex issues of information confidentiality and

[6] Kumar, A. and Mishra, A., 2015. Protecting trade secrets in India. *The Journal of World Intellectual Property*, *18*(6), pp.335-346.

determining economic worth. These rules might need to change further for AI in order to account for its special dynamic character.

The legal concept of a trade secret is broad and can vary depending on the jurisdiction, but the Defend Trade Secrets Act (DTSA),2016 and most state laws offer similar definitions. A trade secret pertains to any information that holds economic value (either actual or potential) due to not being widely known or readily discoverable by others who could gain from its disclosure or application. It includes information that is actively safeguarded to maintain its confidentiality. This definition encompasses various types of information such as manufacturing processes, business plans, customer and supplier lists, software and algorithms, marketing strategies, research and development data, and the misappropriation of trade secrets.

1.1 MISAPPROPRIATION

The essence of safeguarding trade secrets revolves around thwarting misappropriation, which transpires when a trade secret is obtained, revealed, or employed by an individual without the proprietor's authorization and utilizing improper methods. Improper Means Acquisition pertains to acquiring a trade secret through illicit or unethical practices. Misappropriation can manifest in various ways[7].

1.1.1 Theft

One of the simplest and most visible methods of stealing trade secrets is theft. It happens when someone illegally obtains digital or tangible property that holds private or secret company data. Documents, physical prototypes, blueprints, computer files, and any other type of trade secret information could be stolen in this way.

1.1.2 Bribery

Bribery is the practice of providing cash, presents, or other rewards to workers, subcontractors, or other people who have access to a business's trade secrets in return for their use or disclosure. This kind of misappropriation frequently happens when a rival or an individual tries to obtain private knowledge illegally in order to avoid the time, expense, and effort required to establish their own proprietary knowledge.

[7] Nomani, M.Z.M. and Rahman, F., 2011. Intellection of trade secret and innovation laws in India.

1.1.3 Espionage

Espionage, often known as industrial espionage, is the practice of surreptitiously obtaining trade secrets from rival companies or other enterprises by clandestine or unlawful means. It frequently entails spying operations that go beyond straightforward theft with the goal of obtaining private company data for financial gain or to hurt a rival.

1.1.4 Deception

Fraud is when someone uses dishonest or misleading methods to get a company's trade secrets. In contrast to theft or bribery, fraud typically entails lying, deception, or some other kind of misrepresentation in order to get access to private data.

1.2 DISCLOSURE OR USE OF TRADE SECRETS

Misappropriation also includes using or disclosing a trade secret without the owner's permission once someone has obtained it illegally. A competitor who obtains access to a company's trade secrets through illegal means (such as hacking or bribery) and uses that information to create competing products is also guilty of misappropriation, as is an employee who quits their job and gives confidential information to a rival company or uses it to launch their own rival company.

1.3 BREACH OF DUTY TO MAINTAIN SECRECY

Violating a duty of confidentiality is also considered misappropriation. In certain situations, people or organisations have an obligation to protect the privacy of specific information. They may be held accountable for misappropriation if they violate that obligation by revealing or utilising trade secrets.

1.4 REMEDIES FOR TRADE SECRET MISAPPROPRIATION

The Defend Trade Secrets Act (DTSA) and state laws provide the victim corporation with a number of legal remedies. The goals of these remedies are to halt the theft, pay damages to the victim, and discourage such offences in the future.

1.4.1 Injunctions

An injunction, which is a court order that prevents the defendant from using or disclosing the trade secret going forward, is one of the main remedies for trade secret misappropriation. Different kinds of injunctions exist, including Preliminary Injunction to stop additional injury, a temporary injunction is granted early in the case, frequently prior

to the trial. A permanent injunction was issued that forbade the defendant from exploiting the trade secret going forward. Because they can stop the abuse of the private information, injunctions are especially crucial in preventing additional harm to the trade secret holder's company.[8]

1.4.2 Damages

The owner of the trade secret may be entitled to compensatory damages for the losses incurred as a result of the trade secret's unauthorised use or disclosure, in addition to halting the misappropriation. These may consist of:

Actual Damages: The real monetary losses brought on by the theft, such as missed revenue, market share, or commercial prospects.

Unjust Enrichment: Even if the owner of the trade secret is unable to demonstrate the precise extent of their injury, they may still be able to recoup the profits they made from employing the trade secret.

Exemplary Damages (Punitive): A court may grant exemplary penalties, sometimes referred to as punitive damages, in some circumstances, particularly when the misappropriation was deliberate or malicious, in order to penalise the defendant and discourage future occurrences of the same behaviour.[9]

1.4.3 Legal Fees

In extreme circumstances, the victorious party in a trade secret litigation may also be eligible to receive attorney's fees under the DTSA. This usually occurs if the court determines that the trade secret owner's legal claims were baseless or presented in poor faith, or if the misappropriation was determined to be wilful and malicious.

1.4.4 Criminal Responsibility

The Economic Espionage Act (EEA) of 1996 permits the criminal prosecution of trade secret theft, even though the DTSA mostly handles civil cases. People or organisations that steal trade secrets for the benefit of foreign governments or businesses may be prosecuted by the government under the EEA, and they may face severe fines and even jail time.

[8] Nashkova, S., 2023. Defining Trade Secrets in the United States: Past and Present Challenges–A Way Forward?. *IIC-International Review of Intellectual Property and Competition Law*, *54*(5), pp.634-672.
[9] Varadarajan, D., 2017. The trade secret-contract interface. *Iowa L. Rev.*, *103*, p.1543.

2. Indian legal framework for trade secrets

Trade secrets basically refer to confidential business information that provides a competitive edge over other companies. No Indian statute exclusively deals with protection of trade secrets. However, various enactments collectively form a safe haven for them. As part of this context, we will discuss some of the aspects and sources for trade secret protection in India: common law principles, contractual obligations, and statutory sources.

1.Common Law Principles

Trade secret law in India is significantly based on common law principles that have evolved over the years through judicial precedents.

1.1 Confidentiality: Indian courts recognize the existence of a duty of confidence, which arises out of the nature of the relationship existing between parties, for example, employer-employee or between partners in business. A party to a confidential relationship cannot disclose sensitive information. An example is where an employee has access to proprietary formulas or processes. Disclosure to a competitor will lead to legal consequences. In general, courts have upheld the owner's right to take action against those who disclose such confidential information without permission.

1.2 Equity: In addition to common law, equity principles provide a route to protection for trade secrets. In the event of a dispute relating to trade secrets, courts will possibly consider whether there has been a breach of good faith and fair dealing. If one party misappropriates trade secrets and uses it to his advantage, the other party can seek equitable remedies by way of an injunction according to equity principles.

2. The Indian Contract Act, 1872: This Act governs all contracts in India, including those aimed at protecting trade secrets. It provides the framework for drafting enforceable NDAs and other agreements protecting trade secrets, emphasising the importance of lawful consideration and the mutual agreement of parties.

Contract Obligations

Non-disclosure agreement: NDAs are probably the most popular mechanism of safeguarding trade secrets. NDAs are legal agreements between parties whereby one or more parties agree to maintain certain information confidential. NDAs can be drafted according to the specifications of the parties involved and generally include the nature of the information deemed confidential, the duration of the obligation, and consequences of

breaching that obligation. Violations of NDAs can lead to civil lawsuits, wherein the owner of the trade secret can seek damages and injunctions to prevent further disclosure.

Employment Agreements: Many employment contracts include confidentiality clauses to protect an employer's trade secrets. Employees are often explicitly prohibited from disclosing any proprietary information they come in contact with during their employment.

Several statutes in India provide a framework for the protection of trade secrets and confidentiality:[10]

3. The Information Technology Act, 2000: This Act addresses issues pertaining to electronic records and data, including unauthorised access and theft of digital information. Section 43 of the Act imposes liability for damage caused by an individual who accesses or downloads data without permission, which can extend to trade secrets held electronically.[11]

4. The Copyright Act, 1957: Although primarily aimed at protecting creative works, the Copyright Act can indirectly safeguard trade secrets, especially in software development. For instance, source code may be considered the expression of an idea and is therefore covered under this law. Unauthorised reproduction or distribution of such software containing trade secrets may result in legal action.[12]

5. The Competition Act, 2002: This statute promotes fair competition within India and prohibits practices that can harm competition. Misappropriation or theft of trade secrets that gives one business an unfair competitive advantage can be scrutinised under this act. The Competition Commission of India (CCI) can take action against companies engaged in conduct that undermines fair competition.[13]

IX. AI TECHNOLOGIES AND TRADE SECRETS

Advanced data analysis, automation, and decision-making processes made possible by AI technology are transforming entire industries. A company's competitive advantage generally depends on proprietary algorithms, data sets, and models that are at the heart of

[10] Graves, C.T. and DiBoise, J.A., 2006. Do strict trade secret and non-competition laws obstruct innovation?. *Entrepreneurial Bus. LJ*, *1*, p.323.
[11] Maurer, S.D. and Zugelder, M.T., 2000. Trade secret management in high technology: a legal review and research agenda. *The Journal of High Technology Management Research*, *11*(2), pp.155-174.
[12] Arora, J.K., 2023. *COPYRIGHT, PATENTS, TRADEMARKS AND TRADE SECRETS LAWS*. Jagdish Krishanlal Arora.
[13] Sprankling, J.G., 2024. TRADE SECRETS IN THE ARTIFICIAL INTELLIGENCE ERA. *Available at SSRN 4847813*.

these breakthroughs. For organisations to be competitive and promote innovation, these components must be protected as trade secrets. AI systems' underlying algorithms as well as special techniques for gathering, processing, and analysing data can be considered trade secrets. The privacy of training datasets is equally crucial in light of the growing dependence on insights derived from data. The loss of competitive advantage and large financial losses can result from unauthorised access to or publication of these trade secrets.[14]

1. Algorithm

In AI, an algorithm is a set of mathematical procedures and computational techniques that explain how data is processed and analysed to yield some sort of output. This could include decisions of how a particular thing is handled with certain data types, structures, or complex patterns. An application such as natural language processing, image recognition, and predictive analytics have functionalities powered by algorithms. Often, the source code from which an algorithm is developed is proprietary. Such organisations invest a lot in research and development to create proprietary algorithms that have better performance efficiency than competitors. A company holding such proprietary algorithms confidential thus has a competitive advantage on the marketplace. When accessed by competitors, they probably replicate the technology or engineer similar capabilities, thus damaging the original company's investments. [15]

2. Training data

The datasets used to train AI models are referred to as training data. An AI system's performance is largely determined by the calibre, volume, and applicability of this data. It takes a lot of money, effort, and experience to curate and gather high-quality training data, especially when it comes to making sure that the datasets are impartial and representative. If the training data compilation is valuable, not widely known, and is protected by reasonable measures to keep it secret, it may be regarded as a trade secret. Proprietary datasets can provide significant competitive benefits for AI applications; the data's uniqueness can result in the creation of models that outperform those trained on publicly

[14] Greer, G.G., 2021. Artificial Intelligence and Trade Secret Law. *UIC Rev. Intell. Prop. L.*, *21*, p.i.
[15] Hrdy, C. A. (2024). Keeping ChatGPT a Trade Secret While Selling It Too. *Berkeley Technology Law Journal (forthcoming 2025)*.

accessible datasets. Potential trade secret examples Data Labelling Methods, Curated Datasets, dynamic data updating.

3. Models

An AI model represents the encoded information obtained from particular datasets once it has been trained on them. This covers not only the model's architecture (its structure), but also its learnt weights (the particular values allocated to various connections within the model) and hyperparameters (the settings that control the learning process). The actual trained models themselves may be considered trade secrets, especially if they represent special knowledge or practical benefits. Businesses can safeguard their models by limiting access to the parameters and underlying structure, particularly if these are the outcome of intensive testing and refinement. Additionally, performance-enhancing ensemble approaches or model optimisation may have proprietary components. Potential trade secret examples Transfer learning strategies, model architecture, and hyperparameter settings.

XI. CHALLENGES IN IDENTIFYING AI TRADE SECRETS

The protection of trade secrets related to artificial intelligence (AI) technology is crucial as businesses depend more and more on these advancements. However, a number of obstacles make it more difficult to identify and preserve trade secrets in the field of artificial intelligence. Difficulties in Recognizing AI Trade Secrets

1. Requirements for Specificity

According to trade secret legislation, information must be sufficiently detailed to be eligible for protection. The intricacy of algorithms and models frequently makes it difficult to express AI-related trade secrets in tangible words, making this necessity a major obstacle. Courts have stressed that plaintiffs must give thorough explanations that disclose the true secrets involved; simply labelling something as "AI" or "machine learning" is not enough. This clarity is essential for both enforcing the law and putting in place appropriate safeguards.

2. Reverse Engineering

Production-deployed AI systems are susceptible to reverse engineering, in which rivals can examine and duplicate the underlying models and algorithms. Since information obtained through reverse engineering is not covered by trade secret laws, this capability compromises the confidentiality necessary for trade secret protection. Particularly in

competitive marketplaces, the ease with which AI systems can be deconstructed poses serious concerns about confidentiality.

3. Transparency in Algorithms

Maintaining trade secrets is made more difficult by the drive for explainability and transparency in AI systems, particularly in regulated businesses. Companies may have to reveal some parts of their algorithms in order to meet legal requirements or industry norms, which reduces their ability to keep some parts secret. Businesses may face operational and legal challenges as a result of this conflict between regulatory requirements and the demand for confidentiality.[16]

4. The Changing Character of AI

Because AI technologies are developing so quickly, the definition of a trade secret is subject to quick changes. Businesses find it challenging to properly define and safeguard their private information due to the constant emergence of new methods and systems. Compliance efforts are made more difficult by the changing context, which calls for constant evaluations of what constitutes a trade secret.[17]

5. Mobility of Employees

Significant staff mobility across firms is a result of the strong demand for qualified AI workers. This mobility raises the possibility of trade secret misappropriation since departing employees could purposefully or unintentionally provide competitors critical information. Businesses must put strong safeguards in place to reduce this risk, such as non-disclosure agreements and leave interviews that highlight confidentiality commitments.

XII. BEST PRACTICES FOR PROTECTING TRADE SECRETS INVOLVING AI

1. Restricted Access to Sensitive Information

In order to guarantee that only authorised individuals can view or handle sensitive material, trade secret access must be restricted. Organisations should take a number of important steps to accomplish this. To ensure that workers only have access to the data required for

[16] John, A., 2023. Assessing the International Efficacy of Legal Safeguards for Software and Algorithms: Comparative Analysis Between India and the UK. *Available at SSRN 4689534*.
[17] Greer, G.G., 2022. Artificial Intelligence and Trade Secret Law, 21 UIC Rev. Intell. Prop. L. 252 (2022). *UIC Review of Intellectual Property Law*, *21*(3), p.2.

their jobs, they can first implement Role-Based Access Control (RBAC), which assigns permissions according to job duties. Data classification is also essential; companies should group data based on the degree of sensitivity, explicitly identify trade secrets, and make sure the right security measures are in place while handling them. Last but not least, regular access reviews are essential for security; they assist ensure that only current employees who need access to certain trade secrets keep it, reducing the possibility of unapproved exposure.

2. Implementation of Robust Security Measures and Monitoring Protocols

Organisations should implement sophisticated security procedures that make use of contemporary technologies in order to shield sensitive data from breaches and illegal access. Using robust encryption techniques for data in transit and at rest is essential because it guarantees that, even in the event of interception, the data cannot be decrypted without the right decryption keys. Furthermore, security may be greatly improved by putting AI-driven anomaly detection systems into place. These systems keep an eye on user behaviour and data access patterns to spot odd activity that might point to possible security breaches. AI can swiftly identify departures from typical behaviour by evaluating enormous datasets in real time, allowing for proactive reactions to dangers. In order to reduce vulnerabilities that can reveal trade secrets, companies should also use safe development techniques when developing AI systems. [18]

3. Regular Audits to Detect Unauthorised Access

It is essential to carry out routine audits in order to spot possible weaknesses and illegal access to trade secrets. To determine whether trade secret protection policies are being followed and how well the current security measures are working, organisations should plan internal security audits. These audits aid in making sure that procedures are being followed and that any systemic flaws are quickly fixed. Furthermore, hiring outside cybersecurity specialists to conduct third-party assessments can offer an unbiased assessment of the company's security posture and reveal possible threats that would not be apparent from within. Additionally, by simulating data breaches or unauthorised disclosures through incident response drills, staff are better equipped to handle real-world scenarios, increasing the organisation's overall preparedness to safeguard its trade secrets.

[18] Pooley, J., 1997. The Top Ten Issues in Trade Secret Law. *Temp. L. Rev.*, *70*, p.1181.

When combined, these procedures offer a thorough method for protecting private data.[19]

Legal Strategies for Enforcement

Organisations must be ready to take swift legal action when misuse of trade secrets is suspected. Organisations must take prompt action when they discover a possible violation by consulting with intellectual property law experts to decide on the best course of action. Sending cease-and-desist letters to people or organisations accused of stealing trade secrets is one way to do this, formally asking them to stop using or disclosing private information without authorization. Furthermore, gathering proof is essential for supporting allegations of trade secret theft. Businesses should keep thorough records that specify what qualifies as a trade secret, along with thorough descriptions and usage instructions. This endeavour can be further aided by using security system monitoring logs, which keep track of sensitive information access and assist in identifying any unauthorised access or questionable activity that might point to misappropriation. When combined, these preventative actions guarantee that businesses are prepared to successfully protect their confidential data.[20]

XIII. SCOPE

This research paper will explore the intersection of trade secrets and artificial intelligence (AI), focusing on the legal frameworks, challenges, and best practices for protecting proprietary information in a digital environment. It examines how businesses might protect trade secrets while addressing issues around AI transparency by utilising cutting-edge security measures and legal tactics.

XIV. LIMITATION

This study only focused on doctrinal view point. The author only relied on secondary sources. As the research was completed in a short time it was not able to be further expanded. So future researchers can expand their scope.

XV. CONCLUSION

Protecting trade secrets in an AI-driven future has grown more and more important, especially in light of Indian law's particular circumstances. Strong security measures are required as the risks of trade secret theft increase when companies use AI technologies to

[19] Chauhan, A. and Singh, K., Intellectual Property Rights and Artificial Intelligence: A Path to the Future.
[20] Dhir, M. and Verma, S., 2024. *AI for good: India and beyond*. Notion Press.

improve their operations. Although court decisions have confirmed the significance of trade secrets, Indian law does not yet have a thorough framework that addresses them expressly. Organisations must thus take a diversified approach that incorporates cutting-edge security procedures, staff education, and legal protections catered to the intricacies of artificial intelligence.

Businesses may successfully negotiate the changing terrain of trade secret protection and guarantee that their private information stays safe in the face of rapid technology breakthroughs by encouraging collaboration among legal experts, technologists, and policymakers. In addition to protecting competitive advantages, this proactive approach will support innovation in the Indian market.

XVI. RECOMMENDATIONS AND FUTURE DIRECTIONS

Evolving Legal Landscape in India

It is anticipated that India's legal system would change as AI technology develops to handle new issues pertaining to trade secret protection:

1. **Proposed "Protection of Trade Secret Bill 2024":** A thorough trade secret law that would offer a uniform and transparent framework for the detection, safeguarding, and enforcement of trade secrets—including those pertaining to artificial intelligence (AI) technologies—is presently being contemplated by the Indian government. As AI technologies continue to advance, the legal landscape in India is expected to evolve to address emerging challenges related to trade secret protection.
2. **The significance of codified laws:** India's lack of a specific trade secret legislation has resulted in a hodgepodge of common law rules, contractual duties, and other laws. The intricacy of AI systems, the dangers of reverse engineering, and the effects of generative AI technologies are only a few of the particular difficulties that may be addressed with codified trade secret regulations.

Collaboration Among Stakeholders

Multiple stakeholders will need to work closely together to protect trade secrets in the AI era, including:

Legal experts: Lawyers and legal scholars who can offer advice on how the law is changing, create efficient enforcement plans, and push for legislative changes.

Technologists: Engineers, Security experts, and AI researchers who can assist in identifying and putting into practice strong technical safeguards for trade secrets as well as in creating new technologies to improve trade secret protection.

Policymakers: Lawmakers and government representatives who can assist in developing the laws and rules pertaining to trade secrets and making sure they stay up with the quick development of artificial intelligence (AI) technologies.

The technological and legal obstacles to safeguarding trade secrets connected to artificial intelligence can be more successfully overcome by encouraging collaborations and candid communication among these important parties. As the AI landscape develops further, this cooperative approach will be essential to guaranteeing that the legal framework stays applicable and flexible.

REFERENCES

1. Kilic, B. (2024). *Into uncharted waters: Trade secrets law in the AI era* (No. 295). CIGI Papers.
2. Hrdy, C. A. (2024). Keeping ChatGPT a Trade Secret While Selling It Too. *Berkeley Technology Law Journal (forthcoming 2025)*.
3. Lin, C.F., 2019. Public Morals, Trade Secrets, and the Dilemma of Regulating Automated Driving Systems. *Artificial Intelligence and International Economic Law: Disruption, Regulation, and Reconfiguration (Cambridge University Press 2021) Chapter*, *12*.
4. Grozdanovski, L., My Ai, My Code, My Secret.
5. Rissland, E.L. and Ashley, K.D., 1987, December. A case-based system for trade secrets law. In *Proceedings of the 1st international conference on Artificial intelligence and law* (pp. 60-66).
6. John Villasenor, *Artificial Intelligence, Trade Secrets, and the Challenge of Transparency*, 25 N.C. J.L. & Tech. 3 (2024),
7. *Navigating the Legal Complexities of Artificial Intelligence in Global Trade Agreements*, ResearchGate (2024),
8. R. Mark Halligan, *Artificial Intelligence and Trade Secrets*, Reuters (Dec. 11, 2023)