INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE AND TRADE SECRET PROTECTION: EMERGING LEGAL RISKS AND REGULATORY CHALLENGES

AUTHORED BY - ALEENA B ALEX

ABSTRACT

Artificial Intelligence (AI) is revolutionizing the modern business world by using automation, prediction-based analysis, and decision-making processes based on algorithms to transform many industries. The commercial value of AI systems is generated from proprietary algorithms, training datasets, source codes, and model architecture, many of which qualify as trade secrets. Unlike patents, which require public disclosure, trade secret protection gives businesses the benefit of protecting their confidential business information from being used by competitors or disclosed to the public, therefore ensuring a competitive advantage. At the same time, there is an unprecedented risk of legal vulnerability due to the digital and data-intensive nature of AI systems, and therefore AI systems face challenges to all traditional doctrines concerning trade secret protection. These new types of challenges consist of algorithmic transparency requirements, model inversion and extraction attacks, employee-transferred, non-competition agreements, cross-border data processing, and cybersecurity. The above will raise serious questions with respect to the current legal framework. On an international level, Article 39 of the TRIPS Agreement requires that member countries protect undisclosed information from any form of unfair competition. In the United States, the Defend Trade Secrets Act provides federal civil remedies for the protection of trade secrets; while India does not have a stand-alone trade secret statute, it primarily relies on contract law and equitable remedies. This article critically examines how trade secrets and AI technology are evolving, finds legal loopholes pertaining to these matters, and assesses regulatory obstacles. The author makes the case that current trade secrets rules need to be changed to properly safeguard companies' private knowledge in the current digital economy and to reflect the new realities of AI-driven innovation.

Keywords: Artificial Intelligence, Trade Secrets, Misappropriation, Algorithmic Transparency, Reverse Engineering, Regulatory Gaps, Digital Economy.

ISSN: 2582-6433

INTRODUCTION

The use of artificial intelligence (AI) in the digital economy has led to a rapidly changing global economy with new opportunities for businesses to create competitive advantages. AI systems are impacting all industries including finance, healthcare, e-commerce, manufacturing, and government by improving operational efficiencies and enabling more innovative strategies. Much of the commercial value associated with AI stems from certain proprietary development assets; not necessarily from the physical components (namely, hardware and software), but rather from algorithms, data used to develop the algorithms (commonly referred to as training data), architecture of the neural networks used to build AI, predictive analytics, and optimization techniques. These intangible assets are often subject to trade secret protection as they can represent confidential business information, which, in turn, provides an organization with significant competitive advantages. Organizations have historically relied on trade secret protection to protect their proprietary information. In contrast to patents that require an inventor to publicly disclose their invention and only provide a right to exclude others from using an invention for a limited period of time, trade secrets can be indefinitely protected as long as trade secret law requirements are satisfied. The foundation for protecting confidential information is found in the international legal framework of Article 39 of the TRIPS Agreement. Article 39 of TRIPS prohibits WTO member countries from unfairly utilizing undisclosed information. Numerous jurisdictions have put forth comprehensive statutory schemes to operate the protection of these trade secrets.

However, fundamental flaws in conventional trade secret theories have been revealed by the incorporation of AI technology into corporate processes. There are more complexity in the Indian legal system. There isn't a separate trade secret law in India. Contractual duties, equitable principles, and judicial interpretation of breach of confidence are the main sources of protection. In Niranjan Shankar Golikari v. The Century Spinning and Manufacturing Company Ltd[1], the Supreme Court acknowledged the validity of maintaining secret information while an employee is employed. This is only one example of how courts have treated confidentiality concerns in employment situations. However, the lack of established guidelines raises questions about the extent of protection, potential remedies, and the level of "reasonable efforts" necessary to preserve confidentiality in technologically sophisticated settings. The main goal of this study is to investigate how AI technologies and trade secret

[1] . AIR 1967 SC 1098

ISSN: 2582-6433

protection interact. In order to ensure that trade secret law reflects current realities in an increasingly digital economy, it will assess potential legal liability risks associated with the growing convergence of AI and trade secrets, assess how well existing domestic and international frameworks will continue to provide sufficient safeguards for trade secrets, and suggest potential regulatory changes, particularly with regard to India. This paper suggests that, in the rapidly evolving field of artificial intelligence, updating trade secret jurisprudence is essential to maintaining innovation through an equitable legal framework.

OBJECTIVES

In addition to investigating the national and international legal frameworks that govern trade secret protection, the current study aims to i) analyse the effects of artificial intelligence on the features and security of sensitive corporate information. ii) To ascertain whether a comprehensive legal framework is required for the efficient protection of technology-driven trade secrets; iii) to recognize and assess the new legal risks that AI technologies pose to trade secrets; and iv) to critically evaluate the suitability of the current Indian legal system.

RESEARCH QUESTIONS

This research aims to answer a number of important questions: Which are the main national and international legal frameworks that govern trade secret protection, and how well do they adjust to technological advancements? When AI technologies are used and implemented in corporate settings, what new legal dangers arise? Furthermore, does the current Indian legal system adequately protect technology-driven trade secrets, or does it require extensive statutory reform?

RESEARCH HYPOTHESIS

The study is based on the idea that developments in artificial intelligence technology have fundamentally changed the character and susceptibility of confidential business information, exposing trade secrets to novel and intricate legal concerns. Additionally, it is argued that whereas foreign frameworks offer an organized method for identifying trade secret protection, the current Indian legal system lacks a comprehensive legislative process that may successfully address theft related to artificial intelligence. Legislative reform is necessary in this case to guarantee more robust and transparent protection.

ISSN: 2582-6433

RESEARCH METHODOLOGY

The Research methodology used in this study is doctrinal and analytical, with an emphasis on qualitative investigation of the legal rules regulating trade secret protection in light of technological developments. The study's secondary sources include books, scholarly papers, policy reports, international treaties, judicial decisions, and statutory provisions. In order to analyze national and international legal frameworks and evaluate how well they handle new threats to technology-driven trade secrets, a comparative method is also utilized. There is no empirical data collection involved; the study is theoretical in nature.

LITREAURE REVIEW

For a long time now, the protection of trade secrets has been looked at as an important aspect of intellectual property law and something unique from trademark law. Trade secrets do not receive their protection from registration like other types of intellectual property (such as a patent or copyright) but rather will only be protected if they are kept secret and there are reasonable precautions taken to keep the information confidential. According to David S. Almeling, trade secret law can be a valuable tool when protecting your competitive advantage, especially in an industry where innovating is not easily patentable. Likewise, Sharon K. Sandeen puts forth the argument that the basic premise of trade secret law is based on fairness in commercial transactions rather than on exclusive rights to ownership. With respect to international standards, the provisions within Article 39 of the TRIPS Agreement set the minimum standard for the protection of undisclosed information. However, many scholars have noted that due to the broad wording of Article 39, the minimum standard is often implemented in a manner that is inconsistent across countries.

Scholars of comparative law draw attention to how strong the Defend Trade Secrets Act in the United States is as an example of a statute that provides a single national cause of action and also clearer remedies for misappropriation. India has historically relied mostly on a mixture of contract law and equitable principles to provide for the protection of trade secrets. Judicial decisions throughout India, including John Richard Brady v Chemical Process Equipment's Pvt Ltd., have recognised that confidential information and technical know-how qualify for protection even if there is no statute that expressly provides for such protection. Nonetheless, many scholars believe that the continued reliance on judicial rulemaking creates uncertainty, particularly in industries with rapidly advancing technology where the law needs to provide more clarity regarding evidentiary burdens and enforcement methods. There has been an

ISSN: 2582-6433

increase in academic literature describing the challenges posed by AI to traditional trade secret law. Authors such as Mark A. Lemley note that digital technologies make it harder to determine the boundaries of secrecy, especially with proprietary algorithms and datasets that can be replicated or reverse-engineered using technology. Because AI systems rely on confidential training data, source code and model architecture-development, all of which are at risk from cyber-intrusion, model extraction, and the flowing of data across borders, it's important to analyse the legal protections afforded by trade secrets in the current and developing regulatory environments surrounding AI and data. There is much work being done to develop governance structures and regulate data usage in AI; however, little has been done to provide an integrated analysis of how existing trade secret laws (e.g. India) provide protection against risks of technology. These gaps highlight the need for a broader perspective in analysing whether the current legal framework will be adequate to protect innovation within the digital economy, or if further statutory reform will be necessary.

RESEARCH AND ANALYSIS

1. CONCEPT AND NATURE OF TRADE SCERET

Trade secrets are a special type of intellectual property that safeguards commercially valuable information that isn't made public. Trade secrets are independent of state registration or formal issuance, unlike patents, copyrights, or trademarks. Their protection arises from the confidential character of the information and the legal obligation imposed upon those who receive it in confidence. The essence of a trade secret lies in three foundational elements: (i) the information must be secret; (ii) it must possess independent commercial value because of its secrecy; and (iii) reasonable steps must have been taken to maintain its confidentiality.

The economic rationale for trade secret protection stems from two sources: reducing the risk of unfair competition and fostering new ideas. The law provides businesses that have developed valuable trade secrets—their proprietary business information, such as product formulas or designs; technical processes; manufacturing methods; marketing plans; customer lists; and computer source code—with an incentive to create more innovative products through R&D by reducing the chances they will lose them because someone else has copied or disclosed them without authorization. According to many researchers, trade secret protection provides a solution to a problem created by the gaps left by patent protection and also provides another tool to protect knowledge that does not meet patentability requirements and/or that has other

ISSN: 2582-6433

restrictions that make it cost-prohibitive to obtain patent protection through registration[2].

2. INDIAN LEGAL POSITION ON TRADE SECRET PROTECTION

Currently, there is no single trade secret law in India; however, trade secret law is governed by contractual obligations, equity principles, and judicial precedents. The Indian Contract Act, 1872, gives the basis for enforcement of trade secrets, specifically in relation to agreements concerning confidentiality and non-disclosure. Courts have consistently held that if a party discloses confidential information to another party in the scope of their employment or in the course of conducting business with one another, they have a legal duty not to disclose that confidential information without authorization. The equitable doctrine of breach of confidence plays an integral role in the development of Indian law. The courts use their powers of equity to restrict the misuse of confidential information on grounds of good faith and commercial morality rather than on the basis of absolute proprietary rights. In the case of John Richard Brady v. Chemical Process Equipment Pvt. Ltd., (Delhi) it was held that even in the absence of specific statutory provisions protecting confidential information or technical know-how, they can be protected under Indian law. In this regard, the court recognised that equity requires that an employee/contractor be protected from the misuse of trade secrets which he or she has acquired during employment/contractual relationship[3]

In American Express Bank Ltd. v. Priya Puri[4] , the High Court of Delhi distinguished between the general skills that employees acquire during their employment and their employer's confidential customer information. The Court held that while an employee may utilize their general knowledge and experience, they are prohibited from using their employer's proprietary customer data and other confidential business practices. In doing so, the courts have made specific distinctions between the protection of trade secrets and employee mobility and the right to earn a living. The Indian Judicial System has also addressed the enforceability of restrictive covenants included in employment agreements under Section 27 of the Indian Contract Act, 1872. This section declares agreements that restrain individuals from engaging in a trade unlawful. However, the courts of India have determined that reasonable restrictions can be enforced for protecting confidential information during the employee's employment

[2] David S. Almeling, "Four Reasons to Enact a Federal Trade Secrets Act," 19 Fordham Intellectual Property, Media & Entertainment Law Journal 769 (2009).
[3] John Richard Brady v. Chemical Process Equipment's Pvt. Ltd.
[4] (2006) III LLJ 540 (Del)

ISSN: 2582-6433

period. In the case of V.F.S Global Services Pvt Ltd v Suprit Roy[5], the Bombay High Court granted injunctive relief to stop the misuse of confidential databases and proprietary data, thus affirming the significance of protecting commercially sensitive information.

Although there have been some recent court cases regarding trade secrets, they still present a number of challenges in India. First, there is no clear statutory definition for what constitutes a trade secret so Indian courts will have to rely on their own definitions based on case law. Secondly, there are not as many procedural safeguards available to protect the confidentiality of information during litigation in India compared to the US and UK. Third, there are only a few enforcement mechanisms against cyber theft, digital duplication, and cross-border data theft. Although the Information Technology Act provides some remedies for unauthorized access and/or data theft, it does not deal directly with trade secrets[6]

Many commentators believe that the Indian approach, while providing for some flexibility, does not have the certainty and uniformity found in the codified approach of other countries. The increased reliance on digital technology, AI, and data-driven business models exposes the inadequacies of relying solely on breach of contract and/or equitable remedies. In light of this, there is an increasing level of academic support for the enactment of a dedicated trade secret statute that will provide clear definitions, identified remedies, and stronger enforcement mechanisms consistent with global norms.

3. INTERNATIONAL LEGAL FRAMEWORK GOVERNING TRADE SECRET PROTECTION

International trade secret laws are not controlled by a single uniform law but are directed by multiple trade and harmonization agreements. For example, the major BGIE (the governing law of international trade) is Article 39 of the TRIPS Agreement, which was created by the World Trade Organization (WTO). Article 39(2) requires all TRIPS Member States to protect certain non-disclosed information against improper commercial use if that information is secret and has commercial value because of its secrecy and there have been appropriate steps to keep the information secret[7].

[5] (2008) 2 Bom CR 446 (Bom HC)
[6] The Information Technology Act, 2000, §§ 43, 72
[7] Agreement on Trade-Related Aspects of Intellectual Property Rights, 1994, Art. 39(2).

ISSN: 2582-6433

The protection of trade secrets in the TRIPS Agreement has resulted in an important improvement in international intellectual property legislation. Before the TRIPS Agreement, the protection of confidential business information was only governed by national unfair competition contracts & law laws and lacked any kind of established multilateral standard. The TRIPS Agreement provides multilateral minimum obligations for the protection of trade secrets and elevates the protection of trade secrets to the same level as other internationally recognized categories of intellectual property protections like Patents, Trademarks and Copyrights. However, Scholars like Daniel Gervais believe that Article 39 of the TRIPS Agreement establishes only baseline requirements for the protection of trade secrets and gives member states wide discretion in the definition of the scope of trade secrets, the types of remedies available and the enforcement of trade secret laws; thus, many states interpret and enforce trade secret laws differently creating inconsistencies in cross-border enforcement and legal certainty about the enforcement of trade secret laws. In addition to the TRIPs Agreement, there are also regional instruments that have contributed to the advancement of the international regulation of trade secrecy (e.g., the EU Trade Secrets Directive 2016/943, which aims to harmonize the protection of trade secrets for all EU member states, by establishing uniform definitions of a trade secret, defining the lawful and unlawful means of obtaining trade secrets, and by establishing additional procedural safeguards for confidentiality in relation to litigation involving trade secrets[8]) .Some legal scholars believe that the Trade Secrets Directive is an indication of a global trend toward codification and harmonization of trade secrets laws, particularly due to increased digital theft of information and industrial espionage.

Additionally, international discussions on digital trade and cybersecurity are impacting trade secret protections through their intersection with business confidential information, as e-commerce and cross-border data flows become increasingly more important. As more data becomes digital, the risks of transnational data theft, cyber-espionage, and unauthorized replication of technology are increasing. Some legal scholars have indicated that while the international trade law recognizes the need for protection of undisclosed information, enforcement of such protections tends to be within a single country jurisdiction and can create complications in obtaining remedies in international cases involving multinationals and/or

[8] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure

ISSN: 2582-6433

cloud-computing[9]. Even with these advancements, the international framework continues to be disjointed. The TRIPS Agreement establishes basic obligations and provides minimum standards, while regional and national legal systems seek to harmonize the way in which countries will comply with their international responsibilities.

4. EMERGING CHALLENGES IN THE AGE OF ARTIFICIAL INTELLIGENCE

The fast development of AI (artificial intelligence) technology has changed how trade secrets and their vulnerability are defined. Proprietary algorithms, machine learning models, training data sets, predictive analytics systems, and source code used in the digital economy all represent valuable commercial assets that derive their economic value from secrecy. Scholars have commented that trade secret law has become the dominant method for protecting software-driven innovations when it is unclear whether patent protection exists for software or when it is commercially undesirable to disclose software[10].

One of the most significant issues facing the industry today is model extraction and reverse engineering. Research has shown that by querying a trained AI model multiple times, the model can be replicated or approximated based on the entity's analysis of the outputs if the entity does not have access to the source code[11].These reverse engineering and approximation techniques cause confusion between permissible reverse engineering under existing trade secret law and impermissible misappropriation of trade secrets. While traditional trade secret principles permit trade secret owners to independently develop, or to reverse engineer a trade secret through lawful means, the use of advanced computational modelling tools raises the question of whether currently applicable legal standards are sufficient protection for technological copyists.

Another serious issue concerns the requirement of training datasets and/or the way in which these datasets are aggregated. AI systems rely heavily on structured, curated datasets that often contain confidential (i.e., proprietary) business-related information. The main risk to datasets that provide AI capability comes from unauthorized data scraping and cyber-attacks as well as insider exfiltration. While general cybersecurity protocols may protect against unauthorized

[9] Sharon K. Sandeen & Elizabeth A. Rowe, "Trade Secret Law and International Harmonization," 45 Vanderbilt Journal of Transnational Law 729 (2012).
[10] Mark A. Lemley, "The Surprising Virtues of Treating Trade Secrets as IP Rights," 61 Stanford Law Review 311 (2008).
[11] Nicholas Carlini et al., "The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks," 28th USENIX Security Symposium (2019); see also Florian Tramèr et al., "Stealing Machine Learning Models via Prediction APIs," 25th USENIX Security Symposium (2016).

ISSN: 2582-6433

access, the commercial secrets / proprietary nature of AI training data is not a primary consideration in most general protections. The challenges posed by the globalisation of cloud storage make it much more difficult to enforce protections, as the misappropriation of proprietary or confidential datasets can occur from multiple jurisdictions, creating issues of territoriality and jurisdiction under current trade secret law. The increasing demand for algorithmic transparency and explainability creates additional legal tensions. Across the globe, there are numerous regulatory initiatives that require or encourage the disclosure of decision-making processes associated with AI applications, particularly those used in sensitive sectors. However, there are conflicts between the mandatory obligations of transparency, under the regulatory regimes, and the ability of proprietary algorithms to be protected as confidential business information. Article 39 of TRIPS requires the protection of undisclosed information; however, it does not clearly define how such protections balance against transparency obligations. As a result, many scholars believe reconciling these competing goals is a primary regulatory challenge for AI governance. AI systems are continuously evolving and can learn on their own, adding complexity to the task of defining and identifying a protected trade secret. It becomes more difficult to identify what confidential information was provided in the first place if an algorithm changes as a result of a learning process. Therefore, legal commentators believe that traditional static concepts of what constitutes a trade secret may need to change to deal with the evolving and iterative nature of AI technology[12] .In countries like India, where the law protects trade secrets through contracts and equitable remedies but does not have a statute, the technical issues associated with this type of technology create regulatory gaps. The absence of codified guidelines concerning the digital misappropriation of trade secrets, the algorithmic replication of trade secrets, and the improper use of data across borders indicates that the legal system in these countries may not be capable of protecting companies from these issues and enabling them to create value using new technologies.

5. TRADE SECRET MISAPPROPRIATION

When someone unlawfully obtains, discloses or uses confidential business data that can provide them with profitable advantages (commercially or otherwise) because the information is private (unknown to the general public – reasonably protected form) they have committed trade secret misappropriation. According to the Defend Trade Secrets Act, there are many methods through which a company could misappropriate a trade secret, including: obtaining via improper means

[12] Pamela Samuelson, "Trade Secrets and the Information Economy," 27 *Berkeley Technology Law Journal* 1025 (2012).

ISSN: 2582-6433

(e.g., theft, breach of trust, espionage, inducing a co-conspirator to breach their obligation under contract), using or disclosing without permission. There are similar laws found within other places throughout the world, such as the TRIPS Agreement, which establishes that all members of the World Trade Organization must protect undisclosed information from unfair commercial exploitation.

6. BURDEN OF PROOF AND EVIDENTIARY CHALLENGES IN AI MISAPPROPRIATION.

One of the more difficult issues to face in an artificial intelligence-related trade secret dispute is the burden of proof. In the traditional trade secret litigation setting, a plaintiff must demonstrate three main elements: there is a trade secret; the plaintiff used reasonable efforts to keep the information secret; and the defendant unlawfully acquired, used, or disclosed the information. While this sounds relatively straightforward, applying these elements is much more challenging in artificial intelligence cases. Most artificial intelligence models consist of multiple layers of neural architecture, multiple training parameters, and are being continually updated with new, incoming training data. Unlike tangible industrial processes and formulae/recipes, artificial intelligence exhibits dynamism, intangibility, and typically exists in multiple distributed and digital locations. To show that a particular trained model or algorithm is a "trade secret", you must provide evidence of not only that it is secret and has commercial value, but also that it has a specific confidential component located within the model. Courts can have difficulty determining what specific element is being misappropriated - for example, source code, model weights, training data, or how the model was optimally trained/adjusted.

There are other issues involved with proving misappropriation. In the old days, if there was direct access to another's work, and there was a lot of similarity between the competing items, one could assume copying. However, when it comes to an AI-generated output, there may still be similarities even if they are done independently using public/private tools and frameworks/apps that are available to anyone. That's a big evidentiary issue in how the similarity can be determined. Just because two programs do the same work with the same output, does not mean the work has been copied. A court may need to do a technical forensic analysis, utilize expert witness testimony to demonstrate the copying, and/or make some technical comparisons of the algorithms through which the code was generated—judicial competency and evidentiary standards may not have developed relative to these areas. Another problem is digital traceability. Most of the different types of AI are deployed via the "cloud"

ISSN: 2582-6433

and/or through remote servers and or by "collaborative" development. Unauthorized copying can occur in seconds but usually leaves no physical traces. The Computer Laws, such as the Information Technology Act, 2000, provide information rights as the remedy for unauthorized access to data13, but do not directly provide for evidence burdens in cases of trade secret misappropriation. The plaintiff may not be able to trace data exfiltration, identify internal actors who may have facilitated the exfiltration, establish proof that confidential information is now present in the competing system.

Concerns also exist with respect to procedural safeguards. In trade secret lawsuits it is often necessary to disclose sensitive technological data during discovery and at trial. If there are no adequate mechanisms to ensure confidentiality, the enforcement actions themselves will put proprietary algorithms at risk of being disclosed. In the United States, protective orders and sealed proceedings can be obtained under the Defend Trade Secrets Act to mitigate some of the risk associated with the public disclosure of such confidential material14. By comparison, there are limited formalized procedural protections in India, therefore, increasing the risk of litigation for AI businesses. Given these issues, there is increasing scholarly interest in creating new evidentiary standards concerning the establishment of trade secret claims involving AI-based technology. Possible reforms include developing structured forensic auditing processes, establishing burden-shifting mechanisms if prima facie access and similarity are established, mandatory utilization of technical experts, developing procedural safeguards that preserve confidentiality during the course of litigation regarding trade secrets, and ensuring the enforcement of trade secret rights against AI businesses will be as effective as they can be.

FINDINGS

This research indicates that AI is changing the parameters for identifying, protecting and stealing trade secrets by changing the type of assets on which trade secrets are based on traditional manufacturing methods (e.g., trade secrets) to new forms of assets based primarily upon data (such as algorithms, machine learning models, and proprietary data). International agreements such as the TRIPS Agreement provide a baseline of minimum protection for trade secrets (confidential business information), however actual implementation of the international rules into law, and then into practice, varies greatly from one country to another. The research

[13] The Information Technology Act, 2000 (India), §§ 43, 66, 72.
[14] Defend Trade Secrets Act, 18 U.S.C. § 1836(b)(2)– (3).

ISSN: 2582-6433

includes analysis by comparing two groups of laws with respect to protecting trade secrets from technological theft, specifically the Defend Trade Secrets Act in the U.S. and the European Union Trade Secret Directive, which provide statutory definitions for trade secrets, defined legal enforcement mechanisms for protecting trade secrets, and defined legal procedures which are particularly applicable to cases of theft of trade secrets by digital means. On the other hand, India utilises contractual and equitable principles (which are acknowledged by the Indian courts), however, they incur no statutory limits applicable to statutory remedies for obtaining relief from modern technological risks associated with commercial espionage, such as the misappropriation of algorithms through model extraction, data scraping, reverse engineering or cross-border commercial espionage. This research also includes a discussion regarding the challenges of providing sufficient evidence to substantiate a claim against a wrongful misappropriation of an algorithm, as well as reconciling the desire of the public for increased transparency with respect to algorithms and the desire of owners of algorithms for trade secret protections.

CONCLUSION

Trade secrets and trade secret law are two powerful areas of focus in today's world, especially when it comes to protecting confidential technological assets through the use of artificial intelligence (AI) systems. This intersection represents a vast area of growth for businesses and poses regulatory challenges that existing legal doctrines were never established to address. As AI continues to grow and become used more broadly for commercial innovation, protecting confidential technological assets requires both doctrinal adaptation and legislative reform. The current absence of an all-encompassing trade secret statute in India has resulted in a lack of clear rules to protect against potential cases of digital copying, the new evolution of machine learning, and the flow of information across borders. Therefore, to provide clear and stable rules for trade secret protection, a legislatively created and structured statutory framework (with strong procedural safeguards) will be required along with cross-disciplinary collaboration. Overall, improving trade secret protections during the era of AI will not only involve legal reform but is also essential to improving India's ability to compete in the global digital economy.

ISSN: 2582-6433

RECOMMENDATIONS AND FUTURE DIRECTIONS

i) Evolving Legal Landscape in India

India must amend its present legislation to address the evolving environment of trade secret protection as artificial intelligence (AI) continues to expand in a number of areas, including the financial, healthcare, industrial, and digital services sectors. A regulated framework that is both suitable for the current use of technology and structured in a way that can effectively cover the various areas of developing AI is desperately needed, as businesses become more reliant on proprietary algorithms, the data used to train those algorithms, and the automated systems used for decision-making..At the same time, there has been a focus on creating a new comprehensive statute entitled "the Protection of Trade Secrets Bill." This bill is designed to create a single, uniform, and statutory framework that will provide a clear definition of trade secrets, standardized rights of action and remedies, and procedural safeguards and enforcement procedures for the protection of trade secrets specifically related to the digital world and to the use of developments related to innovative AI technologies. Some of the issues that could be addressed with this type of legislation are the ability to replicate algorithms; the ability to extract data from proprietary sources; the ability to misappropriate trade secrets across international borders; and the need to maintain confidentiality during the course of litigation.

ii) Importance of codified trade secret legislation

In India, there is no specific statute governing trade secrets by itself which means that multiple different types of laws are used for protecting trade secrets like reliance upon judicial precedent and contracts. The courts have helped define what constitutes confidential business information, but the rapidly evolving nature of AI systems means the courts' limited ability to provide protection will only grow as these systems mature. If India were to create a statute, the statute would likewise define what constitutes a digital trade secret; what is permissible when it comes to reverse engineering; and would set forth how to prove that someone has wrongfully appropriated another's trade secrets through the use of algorithms. The statute would also provide direction on how to keep confidential information confidential during litigation as well as the manner in which confidential information should be handled while executing enforcement actions to prevent public disclosure of certain proprietary or sensitive data. When it comes to new technologies like generative AI and machine learning, the presence of clear

ISSN: 2582-6433

statutory guidance will help to eliminate uncertainty and build investor confidence in India's intellectual property ecosystem.

iii) Collaborative Framework Among Key Stakeholders

Legislation alone is insufficient to effectively prohibit the disclosure of trade secrets related to artificial intelligence; several parties must work together. Legal experts' opinions are crucial because they will evaluate the ever-changing legal landscape around artificial intelligence, help create enforceable contract protections, and promote fair legislative change. It is the responsibility of legal experts to participate in the development of enforcement tactics that combine the technological realities of contemporary technology with the legal principles of the law. Technologists and cybersecurity specialists play an equally significant role in creating robust technological protections, including as encryption techniques, suitable physical and logical access control systems, secure storage procedures, and audit trails. Complementing legal and technical precautions is crucial since it will reduce the possibility that data will be leaked or that it has been illegally reproduced. It is the responsibility of legislators and regulatory bodies to make sure that the rules designed to safeguard trade secrets remain adaptable to the current rapid pace of technological advancement. This includes making sure that regulations pertaining to data protection, competition legislation, and AI governance are in line with those safeguarding trade secrets. To guarantee that new and creative ways of conducting business are developed while maintaining fundamental values of accountability and openness, there must be constant contact between regulators and the business community.A collaborative and interdisciplinary approach will facilitate the establishment of a flexible and progressive legal regime in India that addresses innovation and offers confidence and security to all parties involved in commercial transactions. As the landscape of AI continues to develop, agile development of regulatory regimes and co-operation amongst stakeholders will be critical to maintaining an effective and balanced legal framework to protect trade secrets.