Page 1656 - 1670 **DOI:** *https//doij.org/10.10000/IJLMH.1110547*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 4

2025

Trade Secrets in the 21st Century: Legal Protections, Risks, and Policy Challenges in a Globalized Digital Economy

PREETI DESWAL[1] AND DIVYA GIRSA[2]

ABSTRACT

Trade secrets have become essential resources for preserving a competitive edge and promoting long-term company success in the contemporary innovation-driven economy. Trade secrets, as opposed to other types of intellectual property like patents or trademarks, are safeguarded by internal safeguards and confidentiality rather than registration. The legal, technological, and policy frameworks pertaining to trade secret protection in a globalized and digital setting are thoroughly examined in this essay.

The article starts out by going over the key traits that make up trade secrets and their strategic value to companies. The article then looks at the various legal systems in different countries, such as the Defend Trade Secrets Act (DTSA) in the US, the Trade Secrets Directive in the EU, and the common law system in India. It emphasizes the increasing global trend toward harmonization through treaties like TRIPS .

It also explores the growing risks that trade secrets confront, including as insider threats, cybercrime, and employee mobility. There includes a thorough discussion of the difficulties of litigation and enforcement, especially the costs of proof and jurisdictional discrepancies. The article also discusses restitution, monetary damages, and injunctive relief as remedies for misappropriation.

The paper highlights the growing difficulties brought about by cloud storage, artificial intelligence, and remote work in the context of digital transformation, all of which have changed the trade secret management environment. It also discusses important policy issues, such as the conflict between public interest and corporate secrecy, the length of time that trade secrets are protected, and employee rights.

This article's multifaceted viewpoint emphasizes the need for strong legal protections, corporate governance, and international collaboration to guarantee the efficient protection of trade secrets in a quickly changing technical and economic landscape.

I. INTRODUCTION

In today's fiercely competitive corporate world, where success or failure is often determined

[1] Author is an Assistant Professor at Innovative Institute of Law, India.
[2] Author is a PhD Scholar at Guru Gobind Singh Indraprastha University, India.

 [ISSN 2581-5369]

by innovation and strategic advantage, protecting vital data is crucial. While patents and copyrights are commonly used to protect inventions and artistic works, not all firm assets fall into these categories. Confidentiality is a better way to protect some of a business's most valuable assets than public registration, such as a unique recipe, a proprietary algorithm, a secret formula, or a customer database. They are known as trade secrets[3]. Although they are usually underestimated, trade secrets are crucial for fostering innovation and economic success. This article explores the meaning, characteristics, and significance of trade secrets as well as the reasons why maintaining confidentiality may sometimes be more valuable than disclosing information to the public.

In today's fiercely competitive and innovation-driven global market, trade secrets are crucial to maintaining a business's competitive advantage. Trade secrets are a wide variety of confidential information that gives a business an edge over its competitors. Manufacturing techniques, business plans, computations, designs, processes, client databases, financial information, and technological know-how may all be included. The reliance on confidentiality that sets a trade secret apart from other types of intellectual property. A trade secret is a type of exclusive business knowledge that includes formulas, designs, procedures, tools, or a collection of data that is not shared with the general public or rival companies. Unlike trademarks or patents, trade secrets are not formally registered with any government agency. Instead, they are protected by secrecy and the steps a company takes to keep themselves secret. Confidentiality is one of the main characteristics of a trade secret. Its relevance stems from the fact that the public is unaware of it. Whether intentionally or accidentally, the secret loses its protected status once it is revealed. Commercial value—the trade secret must give the company a competitive edge in the market—is an essential feature. A unique formula or unique production process can set a business apart from its competitors. Because there is no official registration process for trade secrets, they are favourable. Unlike patents, copyrights, or trademarks, they are not need to be published or acknowledged by the government in order to be protected.

A unique advantage of trade secrets is their ability to be protected indefinitely. Trade secret protection begins as soon as the knowledge is created and kept confidential. So long as the information remains private and has economic value, the protection will continue indefinitely. Other forms of intellectual property, on the other hand, have limited lifespans. However, trade secrets can be stolen or used for industrial espionage, among other forms of misuse. Compared to other forms of intellectual property, they may be more difficult to prove

[3] *Restatement (Third) of Unfair Competition § 39 (Am. L. Inst. 1995).*

 [ISSN 2581-5369]

ownership and theft in court because they are unregistered. Because of this, businesses usually rely on laws like the Defend Trade Secrets Act (in the United States)[4] and use internal policies and contracts to put protections in place.

II. LEGAL FRAMEWORK FOR TRADE SECRET PROTECTION

Each jurisdiction has a slightly different definition of what constitutes a trade secret. According to the United States' Defend Trade Secrets Act (DTSA) of 2016, trade secrets include any type of financial, business, scientific, technical, economic, or engineering information, including plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, regardless of their format or medium of storage. In order to standardise the protection of trade secrets among its member states and reduce the legal fragmentation that previously defined the domain, the European Union established a comparable definition through Directive (EU) 2016/943[5].

Trade secrets can be stolen through a variety of methods, such as bribery, theft, industrial espionage, contract violations, or cyberattacks. Modern business environments, which are marked by remote work, worker mobility, and increased reliance on digital infrastructure, have made trade secret exposure more dangerous. Misappropriation is the unjust or unlawful acquisition of a trade secret, even though some information gathering techniques, including independent discovery or reverse engineering, are permitted by law in many jurisdictions. A competitor may be committing trade secret theft if they hire a former employee to obtain confidential knowledge in violation of a non-disclosure agreement. One of the biggest threats to trade secret protection is employee mobility. Confidential company information is often accessible to employees, who may carry this knowledge with them to a new position. While industry knowledge and general skills are not protected, it can be difficult to distinguish between an employee's expertise and a former employer's trade secrets. Confidentiality clauses and non-compete agreements are common in employment contracts. Although there is a growing trend towards harmonization through international agreements, the legal framework for trade secret protection varies among jurisdictions, and the execution of these agreements varies greatly.

The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)[6], which is

[4] ***Defend Trade Secrets Act of 2016***, *18 U.S.C. § 1836 (2018)*

[5] ***Directive 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, 2016 O.J. (L 157) 1.*

[6] ***Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)***, *Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.*

 [ISSN 2581-5369]

governed by the World Trade Organization (WTO), is the main international instrument. Article 39 of the TRIPS Agreement requires member countries to protect secret information from unjust commercial exploitation. It stipulates that the information must be commercially valuable, confidential, and subject to adequate safeguards to protect its secrecy. By establishing a global standard, this requires member countries to enact laws or take other actions that guarantee the efficient protection of trade secrets. Legislation at the state and federal levels governs trade secret protection in the US. The most important federal statute is the Defend Trade Secrets Act (DTSA) of 2016, which allows owners of trade secrets to file federal court actions and provides remedies like damages and injunctions. The Uniform Trade Secrets Act (UTSA)[7], which has been passed by the majority of states, harmonises definitions and remedies among jurisdictions, albeit with minor modifications. Enacted to standardise laws among member states, the EU Trade Secrets Directive (Directive (EU) 2016/943) protects trade secrets in the EU. The directive outlines trade secrets, establishes guidelines for their lawful acquisition and use, and outlines sanctions for their unlawful use.

The regulation had to be incorporated into national laws in each EU member state in order to ensure uniform protection across the union while respecting national legal traditions. The Anti-Unfair Competition Law in China, which was revised in 2019[8], provides trade secret protection and strengthens enforcement. China has clear provisions against the abuse of trade secrets in both its Criminal Law and Civil Code. Partially in response to international pressure regarding the enforcement of intellectual property rights, China's system is now more closely aligned with international standards thanks to recent legal amendments. Although trade secrets in India are not specifically protected by law, they are recognised by common law principles of equity, contract, and tort. Legislative authorities have upheld confidentiality agreements and imposed penalties for betrayal or theft. Demand for comprehensive legislation to bring India's legal system into compliance with international norms is rising. Other countries with extensive frameworks include Canada, Australia, and Japan[9]. Although they differ in their definitions and methods of enforcement, the Unfair Competition Prevention Act of Japan, the common law principles and Criminal Code of Canada, and the equity-based protections and contractual laws of Australia all work together to protect confidential information.

[7] *Unif. Trade Secrets Act (Unif. L. Comm'n 1985, amended 1985).*
[8] *Anti-Unfair Competition Law of the People's Republic of China (2019 Amendment) (promulgated by the Standing Comm. Nat'l People's Cong., Apr. 23, 2019, effective Apr. 23, 2019) (China).*
[9] *See Unfair Competition Prevention Act, Act No. 47 of 1993 (Japan); Canadian Criminal Code, R.S.C. 1985, c. C-46; Contract Review Act 1980 (NSW) (Australia).*

 [ISSN 2581-5369]

Despite the widespread recognition of the concept of trade secret protection, different legal frameworks and enforcement levels exist. International programs, such as TRIPS and regional laws, aim to ensure that businesses operating internationally are at least partially protected, but still have to navigate various state legal systems. Trade secret protection requires a combination of legal laws, operational procedures, and technological safeguards. Confidentiality agreements (sometimes known as non-disclosure agreements or NDAs), invention assignment agreements, and restrictive covenants are examples of legal instruments. Non-disclosure agreements (NDAs), which apply to employees, contractors, vendors, partners, and investors alike, are among the most often used legal tools used to maintain confidentiality. The scope of sensitive information, the recipient's obligations, and the duration of the agreement must all be clearly stated in an NDA. Despite the fact that NDAs are normally enforceable in a number of jurisdictions, courts have the authority to reject enforcement if they are overly vague, broad, or have an irrational duration. Consequently, careful legal draughting and regular updates of such agreements are crucial.

In addition to formal contracts, businesses need to put in place organizational policies that demonstrate a proactive and unwavering commitment to maintaining secrecy. Internal training programs on the value of confidentiality, sensitivity-based document classification, and "need-to-know" regulations that limit access to critical information are all included in this. It is possible to reclaim all company-owned assets and reiterate confidentiality restrictions during exit talks with departing personnel. Monitoring and internal audits can help guarantee that employees are following trade secret policies. These organizational practices not only lessen the risk of inadvertent exposure but also strengthen a business's legal position by demonstrating that reasonable measures were taken to protect the information's confidentiality. In the digital age, technological safeguards are just as important as organisational and legal strategies. The increasing storage of trade secrets in electronic formats makes them susceptible to cyberattacks. Access control systems, data encryption, multi-factor authentication, secure storage options, and real-time monitoring of vital systems are all components of complete cybersecurity measures that organizations must implement. Organizations should restrict the use of personal devices for work-related activities, or at the very least, enforce strict bring-your-own-device (BYOD) policies. Employees should also be trained to avoid sharing sensitive information via unprotected channels without authorization.

Without putting such measures in place, businesses would find it difficult to convince a judge that they took "reasonable steps" to protect their trade secrets, which is a requirement for legal enforcement. Some jurisdictions allow for criminal remedies. Trade secret theft is illegal in

 [ISSN 2581-5369]

the United States under the Economic Espionage Act of 1996[10], especially when it benefits a foreign government or business. Penalties for breaking this rule include jail time and monetary fines, with corporate violators facing harsher sanctions. With the 2019 amendments to the Anti-Unfair Competition Law, which broadened the definition of trade secrets and lessened the burden of proof on plaintiffs, China, which was previously criticized for its lax enforcement, has made significant strides in recent years to improve its trade secret laws. A global shift towards improved trade secret protection is evident from similar actions that have taken place in other countries, including Brazil, South Korea, and Japan.

III. THREATS AND RISKS OF TRADE SECRETS

Trade secrets are strategic assets that often give businesses a significant competitive advantage. They are constantly vulnerable to various threats and vulnerabilities that could compromise their safety, though. These threats come from both internal problems, such staff negligence and organizational weaknesses, and external ones, like rivals and hackers. Understanding and reducing these risks is essential to maintaining trade secret integrity and ensuring long-term financial success. One of the biggest threats to trade secret preservation is cybersecurity and related issues. Businesses are more vulnerable to cyberattacks since they rely more on digital platforms and store critical data electronically.

Trade secrets can be stolen by cybercriminals, who can then sell them to competitor companies or foreign governments. Ransomware attacks are dangerous because they can disrupt operations and put valuable intellectual property at risk. These attacks occur when hackers encrypt important data and demand payment to decrypt it. Notwithstanding the deployment of advanced security measures, the dynamic nature of cyber threats demands a continuous endeavour to surpass malevolent actors. The danger posed by insider threats is substantial. Workers who have access to trade secrets, such as contractors or business partners, may purposefully or unintentionally divulge or take advantage of confidential knowledge. The risk increases when workers leave the company to work for competitors or start their own businesses. Because insiders are knowledgeable with the company's security procedures and operations, they pose a serious risk of corporate espionage, which is when they are forced or encouraged to reveal critical trade secrets. Even though leave interviews and non-disclosure agreements (NDAs) lessen this risk, they don't totally eliminate it, especially when workers might not fully comprehend the long-term repercussions of disclosing trade secrets. One of the biggest weaknesses in protecting trade secrets is still the

[10] *Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–39.*

 [ISSN 2581-5369]

human aspect. Even well-meaning staff members may make mistakes that cause information to leak, like mistakenly sharing information in casual conversations, misplacing devices that contain trade secrets, or delivering private documents to the wrong address. Social engineering techniques provide significant risks when attackers force victims to divulge personal information. Phishing emails or phone calls that look real but are designed to trick staff members into divulging important information can lead to security lapses.

Employees may also divulge trade secrets out of carelessness, ignorance, or both. Although a strong culture of secrecy, regular training, and clear company policies may mitigate these risks, human error will always be a risk. Threats to physical security increase trade secrets' susceptibility. Despite the rise in digital threats, physical breaches still happen, especially in industries that handle proprietary or sensitive data in physical form. Unauthorised individuals may install surveillance equipment, steal physical documents, or break into data centres or office buildings in order to obtain trade secrets. Employees may access personal information through public or unsecured networks, which creates extra risks with the growing use of mobile devices and remote work. As more and more businesses embrace flexible work schedules, it is critical to ensure secure communication channels and device control. The risks involved in protecting trade secrets are further increased by the complexity of legal protections. Laws governing trade secrets vary greatly from one jurisdiction to another, and it can be difficult to enforce legal protections, especially when there are international disputes. The transnational exchange of trade secrets is a consequence of globalisation of commerce, which increases the possibility of abuse. Trade secret protection standards vary by country, and intellectual property rules may not be as strict or enforceable in certain places as they are in others. Additionally, the public disclosure of trade secrets through patent applications, regulatory filings, or public debate may cause them to lose their protected status. Trade secret risks could increase as organisational control is weakened. Strict control of trade secret management may be challenging for businesses that are expanding quickly, merge, or outsource significant portions of their operations. The likelihood of information breaches increases with the number of workers, contractors, and outside partners involved. Unintentional disclosure or misuse may result from inadequate information-sharing systems or poor document management techniques.

All parties must understand the importance of protecting trade secrets and adhere to established procedures and regulations in order to reduce these risks. In conclusion, there are a number of threats that can affect trade secrets, both internal and external. Significant risks to the protection of personal data include insider threats, human error, physical security flaws,

 [ISSN 2581-5369]

legal issues, organisational barriers, and cybersecurity breaches. To protect the value and integrity of their trade secrets, businesses need to invest in employee training, implement strong security measures, and stay alert to emerging risks.

IV. DIFFICULTIES IN LITIGATION AND ENFORCEMENT

Protecting trade secrets is a complex and difficult task for businesses, legal systems, and governments around the world. In contrast to other forms of intellectual property like patents, copyrights, or trademarks, trade secrets are often harder to enforce, yet being crucial for fostering innovation and maintaining economic advantage. This problem stems from the inherent nature of trade secrets, which are unpublished, sensitive information that needs to remain hidden in order to maintain its legal protections. Unlike trademarks or patents, which are publicly recorded and formally registered, trade secrets rely heavily on legal contracts and internal procedures to be protected. Because of this, it may be much harder to prove ownership, prove misappropriation, and obtain legal recourse. The main obstacle to trade secret enforcement is the burden of proof in court cases. The plaintiff, usually the company, is responsible for proving that the information in question satisfies the requirements for a trade secret, that it was obtained or disclosed illegally, and that the business took reasonable steps to keep it confidential in cases of trade secret misappropriation. When dealing with intangible assets or concepts that have been explained to staff members, subcontractors, or business partners over time, this can be a very difficult task.

The international scope of trade secret theft and the uneven application of trade secret laws across different jurisdictions are major concerns. In addition, courts may reject trade secret claims if a corporation has failed to disclose its information protection measures or to establish strict confidentiality rules, regardless of the material's obvious value and private nature. Businesses commonly operate transnationally, share sensitive data with foreign partners, or assign tasks to foreign organisations in the modern global environment. The laws governing trade secrets range greatly between nations. There are some countries with strong trade secret laws, such as the Defend Trade Secrets Act (DTSA) in the United States[11], whereas other countries may have weak, badly executed, or nonexistent laws. It may be futile to pursue justice for trade secret theft in countries with weak or dishonest legal systems. The digital age has made enforcement more difficult. The difference in legal standards allows criminals to operate from jurisdictions with lax enforcement or use legal loopholes, making it more difficult for damaged businesses to obtain compensation or prevent further harm. Cyber

[11] *See 18 U.S.C. § 1836(b)(1) (allowing for a private right of action for misappropriation).*

 [ISSN 2581-5369]

attacks, data breaches, or the unauthorised transfer of digital content are common ways that trade secrets are stolen. Large amounts of proprietary data can be quickly expropriated by cybercriminals and instantly transferred across international borders, making recovery or tracing nearly impossible.

Anonymity technologies, proxy servers, and sophisticated hacking techniques make it difficult to link theft to a specific individual or organisation, and digital evidence is vulnerable to concealment, destruction, or modification. Enforcement may be impossible if cybercriminals operate outside the victim's legal jurisdiction, even if they are identified. Additionally, legal systems often fail to keep up with new technological threats, leaving businesses vulnerable to new forms of trade secret theft. One major barrier to effective trade secret enforcement is litigation problems. A lawsuit might be expensive, drawn out, and unexpected. In-depth technical evidence, expert testimony, and careful documentation are usually required in trade secret lawsuits, which raises legal costs and lengthens trial times. Additionally, the plaintiff's efforts to protect the trade secret may be jeopardised if it is eventually disclosed during the legal process. Courts may provide protective orders to prevent public exposure, but these measures are not always sufficient to reduce the risk. As a result, some businesses may choose not to file a lawsuit, fearing that it will expose their private information or that the costs of enforcement will outweigh the potential benefits. Making the distinction between trade secret theft and lawful competition is another problem.

A lot of experience and knowledge are brought with employees when they move across companies in the same industry. The law permits the use of general skills and knowledge gained during employment, but it prohibits the exploitation of trade secrets. Because it can be difficult to distinguish between legally acquired knowledge and protected trade secrets, enforcement is both morally and legally complex. Sometimes, courts reach contradictory results as they assess the information's confidentially and decide if its use constitutes misappropriation. The enforcement of trade secrets faces significant challenges due to the intangible and private nature of the knowledge, the difficulty of proving misappropriation, the disparities in international legal systems, the rise in cybercrime, and the practical difficulties of litigation. The difficulties are exacerbated by the need to balance the protection of business interests with individual liberties and the demands of a global economy. In order to improve trade secret enforcement, businesses need to invest in strong protection plans, legislative frameworks need to adapt to new threats, and international cooperation needs to be strengthened in order to effectively address cross-border problems.

 [ISSN 2581-5369]

V. REMEDIES FOR TRADE SECRET INFRINGEMENT

When a trade secret is stolen, the law provides a number of remedies to protect the owner's rights, pay damages, and discourage future infringement. Without robust and reliable enforcement processes, trade secrets are vulnerable, endangering economic competitiveness and innovation. These remedies are essential since trade secrets often contain the most valuable and private knowledge of a corporation, such as designs, methods, formulas, or business plans. Potential remedies often fall into four main categories: monetary damages, punitive damages, injunctive relief, and further equitable remedies like deleting or returning content that has been stolen. Although the scope and accessibility of these remedies may vary by jurisdiction, they always seek to address the wrongdoing of the offender as well as the harm suffered by the trade secret owner. One of the most effective remedies under trade secret law is the injunctive remedy. A judicial order that requires a person or organisation to carry out or refrain from a certain activity is known as an injunction. To prevent future disclosure, use, or dissemination of the stolen knowledge, an injunction may be used in the context of trade secrets. To stop misappropriation before the trial is over, courts may issue preliminary injunctions or temporary restraining orders (TROs) at the beginning of a lawsuit. Such protocols are necessary because the value of a trade secret depends on its privacy; if it is made public or widely used, it may no longer be safeguarded. If the plaintiff wins, the court may issue a permanent injunction that forbids the defendant from using or revealing the trade secret going forward. This remedy is especially important in industries where revealing a single formula or method could do irreversible harm to competition. In addition to the injunctive remedy, courts have the authority to award monetary damages to compensate the owner of the trade secret for losses resulting from misappropriation.

The goal of monetary damages is to return the victim to the position they would have held in the absence of the theft. Unjust enrichment, which refers to any monetary gain the defendant obtained from the illegal use of the trade secret, as well as actual losses, such as lost earnings or lost business opportunities, may be included in these damages. Courts in many jurisdictions use a fair royalty technique, especially in cases when it is difficult to calculate losses precisely. In cases of deliberate or bad faith misappropriation, courts may award punitive damages. This means that the offender pays the same amount as they would have paid to legitimately license the trade secret. These damages are more than just monetary compensation; they are intended to punish the offender for their heinous conduct and discourage similar behaviour in the future. In the United States, courts may award damages up

 [ISSN 2581-5369]

to twice the actual amount under the Defend Trade Secrets Act (DTSA)[12] if the misappropriation is shown to be deliberate and malicious. Restitution or obliteration of the stolen trade secrets is another important kind of remedy. Punitive damages serve as a powerful deterrent to people and businesses, sending a strong message that trade secret theft is unacceptable and can have serious financial consequences. This is particularly important when there is a continuous risk of future exploitation and the stolen content is still in digital or physical form. Courts can order the defendant to destroy digital information, return hard copies, or confirm that materials disclosing the trade secret have been destroyed. In some cases, the winning party may be awarded legal fees and litigation costs, especially if the defendant's actions were clearly malicious or deliberate. This lessens the trade secret owner's continued harm and restores the information's confidentiality as much as is practical. Promoting lawful enforcement and reducing the high costs of filing a trade secret lawsuit are the goals of this. The possibility of having to pay these costs also discourages dishonest defendants from prolonging the lawsuit or interfering with it. The legal system offers a number of remedies for trade secret misappropriation, each of which is intended to address a different aspect of the harm that results. Further harm is prevented by injunctive remedy, compensation and deterrence are provided by monetary and punitive damages, and confidentiality is restored by equitable remedies like information removal. Together, these remedies provide a comprehensive legal approach to the complex problems of protecting and enforcing trade secret rights in the modern, competitive, and digital marketplace.

VI. TRADE SECRETS IN THE DIGITAL ERA

When it comes to protecting and enforcing trade secrets, there are new challenges and complexities. Because businesses are relying more and more on digital technologies to store, transmit, and analyse sensitive data, the risks of trade secret theft have increased dramatically. Mobile devices, cloud storage, and digital platforms have made it easier to access, duplicate, and distribute private information with just a few clicks. Hacking, ransomware, and data breaches are examples of cybersecurity dangers that provide significant hazards since criminal organisations can quickly and often undetected expropriate large amounts of private information.

Digital theft is more difficult to detect than physical theft, and stolen data can be quickly shared across borders, making it more difficult for businesses to track down and recover the stolen trade secrets. Protecting trade secrets is further complicated by the rise in remote work

[12] *18 U.S.C. § 1836(b)(3)(C) (allowing exemplary damages).*

 [ISSN 2581-5369]

and the increasing use of collaboration tools like cloud-based apps and video conferencing. Secret information may be accessed by workers and contractors working from several locations using unsecured networks or personal devices, increasing the possibility of unintentional disclosure or deliberate cyberattacks. Sensitive information may become accidentally or purposely accessible to other parties due to the use of unencrypted communication channels or inadequate access controls. Since trade secrets can no longer be kept in physical locations, businesses need to protect their digital infrastructure from potential breaches and enforce strict rules for access to and sharing of private information. The rapid development of artificial intelligence (AI) and machine learning presents both opportunities and risks for trade secret protection. AI-powered systems have the ability to examine large databases, including private data, and extract knowledge that can be considered proprietary. However, improper distribution or access to AI models or training data could lead to the unauthorised use of private data. As nations around the world work to create and enforce consistent rules on trade secret protection in the face of rapidly developing technologies, the digital age poses legal challenges. International businesses must navigate complex and often contradictory legal frameworks to protect their intellectual property in foreign markets. To overcome these challenges, businesses must put stronger cybersecurity measures in place, such as encryption, multi-factor authentication, and data access controls, to protect trade secrets from unauthorised access. Additionally, companies should have comprehensive training programs that emphasise the importance of safeguarding digital trade secrets, together with strict internal policies on the use of digital technologies and the sharing of information. To counteract digital threats, legal frameworks have emerged, such as the Defend Trade Secrets Act (DTSA) in the US[13], which gives businesses the ability to file lawsuits against disgruntled employees or cybercriminals who steal or misuse confidential data. Despite this, the global nature of digital commerce means that businesses must consider international safeguards because enforcement in other countries might be uneven or problematic. The digital age has significantly changed the field of trade secret protection. Businesses now have more opportunities for efficiency and creativity because to technological improvements, but they also face new risks from unauthorised access and misuse of personal data. In order to protect the confidentiality of critical business information from evolving digital threats, protecting trade secrets in the modern environment requires a multifaceted approach that incorporates strict cybersecurity measures, employee education, and efficient legal frameworks.

[13] *Id.*

 [ISSN 2581-5369]

VII. CONSIDERATIONS AND DISCOURSES ON POLICY

The legislative concerns and disputes surrounding trade secrets are complex and varied, highlighting the tension between promoting innovation, protecting economic interests, and preserving fair competition. A significant topic in the policy discussion is striking a balance between strong trade secret protections and information accessibility for the general public. On the one hand, strict laws protecting trade secrets are crucial for encouraging innovation because they allow companies to spend in R&D and new technologies without worrying about others stealing their intellectual property. In industries like manufacturing, technology, and medicines, where exclusive methods or formulations are essential to success, these protections enable businesses to maintain a competitive edge in international markets.

Trade secret protections that are too broad, according to critics, may hinder innovation and prevent the exchange of information that could benefit the general public. The use of trade secrets to stifle competition or limit access to important technical or scientific advancements can stifle innovation and impair the advancement of the industry as a whole. One important topic of dispute is how long trade secrets are protected. As long as the information is kept hidden, trade secrets can last forever, unlike patents, which have a set period of protection. For businesses seeking long-term security, this might be advantageous, but others argue that ongoing secrecy could prevent the public from learning knowledge that could lead to future advancements or improvements. Similar to patents, some support a temporal restriction on trade secret protection to ensure that the information eventually enters the public domain after a predetermined amount of time, thereby encouraging further study and development. The issue of misappropriation and employee mobility is another contentious issue.

On the other hand, some contend that trade secrets should be protected as long as they are carefully maintained, since this incentivises businesses to continuously improve and expand their intellectual property. With the development of trade secret laws, concerns about how they may affect workers—particularly when they change jobs or start their own businesses—are growing. Trade secret protection often includes restrictions on departing employees that forbid them from using or sharing confidential knowledge they learnt while working for the company. While these safeguards are necessary for businesses, critics argue that highly restrictive non-compete agreements or non-disclosure agreements (NDAs) may unfairly limit an individual's ability to seek new opportunities or start their own businesses, potentially infringing on their rights to economic advancement and occupational freedom.

The growing importance of cybersecurity in protecting trade secrets also raises new policy

 [ISSN 2581-5369]

implications. This has sparked debates about how to fairly balance protecting company confidentiality with allowing people to use their knowledge and abilities for professional growth without undue restrictions. In a time when data breaches and cyberattacks are common, businesses are under increasing pressure to set up thorough cybersecurity procedures to safeguard their private data. However, many SMEs face challenges in obtaining the financial and technical resources required to adopt advanced cybersecurity practices. Legislators must determine how to give all businesses, regardless of size or resources, the same protection, and they must also consider ways to hold businesses responsible for failing to appropriately secure trade secrets from online theft or breaches. A current policy debate concerns the international enforcement of trade secret laws.

While some advocates favour mandatory cybersecurity standards that require companies to implement specific measures to protect trade secrets, others argue that overly stringent regulations may place an unwarranted financial burden on smaller businesses. Underutilisation of trade secrets has become a transnational issue as businesses operate more globally and share personal data globally. The legal framework is fractured as a result of the considerable differences in trade secret protections and enforcement strategies between jurisdictions. For example, whereas the US and EU have extensive systems in place to protect trade secrets, other areas—particularly developing countries—may not have effective legal safeguards against theft. Global corporations face challenges in protecting their intellectual property across multiple legal frameworks as a result of this mismatch. There is an ongoing discussion about the need for stronger international agreements and cooperation to establish international trade secret protections, ensuring that businesses can rely on consistent and fair legal remedies regardless of where their trade secrets are at risk. The need to balance the protection of business interests with broader social goals, such as fostering innovation, fostering fair competition, and protecting employee rights, informs trade secret discussions and policy considerations.

Trade secrets are essential to the modern economy, greatly fostering innovation, protecting competitive advantages, and advancing economic progress. As technological advancements and globalisation change the economic landscape, governments must address these complex issues, making sure that trade secret laws provide adequate protection while encouraging an environment that fosters innovation and competitiveness. As businesses rely more and more on proprietary knowledge to set themselves apart in cutthroat international marketplaces, robust trade secret protection is critical. Both new challenges and opportunities for the future of trade secrets are presented by the rapid advancement of technological advancements and

 [ISSN 2581-5369]

the rise of digital and cyber threats. As organisations strike a balance between the need to prevent the theft of valuable information and its dissemination, the proliferation of artificial intelligence, big data, and cloud computing will make intellectual property protection more complex. In the future, the global economy's trade secret domain is likely to prioritise cybersecurity and digital security measures as businesses work to protect their private data from sophisticated cyberattacks. Additionally, as global trade grows, the need for global trade secret harmonisation will increase, ensuring consistency across jurisdictions and facilitating the enforcement of protections in a transnational business setting. Policymakers need to strike a careful balance between encouraging innovation, preventing monopolistic behaviour, and preserving free and fair competition.

With ongoing debates about protecting individual freedoms and corporate interests in relation to trade secrets, employee mobility and fair labour practices will continue to be controversial topics. The future of trade secrets will ultimately depend on how well governments, businesses, and legal systems can adjust to the shifting dynamics of technology, globalisation, and intellectual property. As businesses depend more and more on data and connectivity, trade secrets will remain an essential resource for promoting innovation and ensuring that the financial benefits of confidential information are distributed fairly throughout industries and nations. To maintain a thriving, competitive global economy and protect the rights of both persons and businesses, it will be crucial to manage these complexities effectively.

*****

 [ISSN 2581-5369]