Page 186 - 198 **DOI:** *https://doij.org/10.10000/IJLMH.119687*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Protection of Trade Secret in Digital Era with special reference to India

NIKITA[1] AND DR. SANTOSH KUMAR TIWARI[2]

ABSTRACT

In the current digital era, the protection of trade secrets is becoming more challenging due to the rapid development technological advancement, connectivity and globalisation. This research paper examines the challenges in the protection of trade secrets in India amidst rising cyber threats, data breaches, and digital communication. It also analyses the legal framework, current practices, judicial pronouncement and suggests a framework combining legal technological and organizational strategies suited to India's unique environment.

Keywords: *Trade Secrets, Digital Era,Intellectual Property, Cybersecurity, Indian Law, Data Protection.*

I. INTRODUCTION

Intellectual property is important because it can be used for commercial purposes. The purpose of developing and protecting intellectual property is to allow the owner of the rights to use it for their own livelihood or to make money off of their original and creative ideas. The use of creative and innovative work for profit is the subject of intellectual property in all its forms. Intellectual property is safeguarded to provide financial compensation and a number of exclusive rights, which incentivize the creator or innovator to keep up their creative and innovative work. The protection and avoidance of commercialization and unauthorized use of the various rights is the general objective of intellectual rights.

Trade secret deals with the type of intellectual property that comprises of certain formulas, practices, processes, design, instrument, recipes or compilation of information that have inherent economic value that are generally not known or readily available to the people at large.[3]In general, to qualify as a trade secret, the information must be commercially valuable, to be known only to a limited group of persons,reasonable steps have been taken by the trade secret holder to keep it secret[4]. Trade secrets may take a variety of forms, such as a proprietary process, instrument, pattern, design, formula, recipe, method, or practice that is not evident to

[1] Author is a LL.M. Student at School of Law, Justice & Governance, Gautam Buddha University, Greater Noida, India.
[2] Author is the Head at School of Law, Justice & Governance, Gautam Buddha University, Greater Noida, India.
[3] **World Intellectual Property Organization. (n.d.).***Trade secrets*. https://www.wipo.int/tradesecrets/en/
[4] https;//www.wipo.int/en/web/trade-secrets

 [ISSN 2581-5369]

others and may be used as a means to create an enterprise that offers an advantage over competitors or provides value to customers.[5] Trade secrets are protected by the law from unauthorized use, acquisition or disclosure and if any effort is made to acquire the same through unfair and dishonest method, it will amount to a illegal activity or an offence punishable by law.[6] The validity of a trade secret remains till the secrecy of the of the information is maintained and kept away from the public, unlike patent, a trade secret does not have to be disclosed to fall under the scope of protection.[7] There are many examples of trade secrets that are tangible and intangible. For example, Google's search algorithm exists as intellectual property in code and is regularly updated to improve and protect its operations.[8]Well-known examples include the Coca-Cola formula and the recipe for Kentucky Fried Chicken.[9] In simple terms trade secrets is the confidential information that is protected through intellectual property laws and it may consists any confidential information that gives a company competitive advancement

Statement of Problem

In the contemporary digital era, trade secrets have emerged as one of the most vital components of intellectual property for businesses particularly within knowledge driven and technology intensive sectors. Trade secret encompass proprietary information such as business strategies, manufacturing processes and client data bases, which offer a competitive edge in the market however proliferation of digital tools, increased employee mobility, cloud based operation and rise in cyber threats have significantly escalated the risks associated with unauthorised disclosure data breaches and intellectual property theft.

Despite India’s growing role in the global digital economy and country lacks a dedicated statute that provides comprehensive protection for trade secrets.

This study seeks to analyze the challenges in the protection of trade secrets in the digital era and analyze the existing legal framework in India

II. MEANING AND CONCEPT OF TRADE SECRETS

A trade secret is any practice or process of a company that is generally not known outside of the company. Information considered a trade secret gives the company a competitive advantage over its competitors and is often a product of internal research and

[5] **Investopedia. (n.d.).** *Trade secret: Definition, examples, laws, vs. patent*.
[6] **World Intellectual Property Organization. (n.d.).** *Trade secrets*. https://www.wipo.int/en/web/trade-secrets
[7] **Merriam-Webster. (n.d.).** *Trade secret*. In *Merriam-Webster.com dictionary*. Retrieved April 18, 2025, from https://www.merriam-webster.com/dictionary/trade%20secret
[8] **Investopedia. (n.d.).** *Trade secret: Definition, examples, laws, vs. patent*.
[9] **Wikipedia contributors. (2025, March 18).** *Trade secret*. Wikipedia, The Free Encyclopedia.

development.[10]Trade secrets encompass both technical information, such as information concerning manufacturing processes, pharmaceutical test data, designs and drawings of computer programs, and commercial information, such as distribution methods, list of suppliers and clients, and advertising strategies.[11]

Extent of confidential information:

1. Manufacturing methods are covered by trade secrets

The entire process of creating something is frequently included in the term "trade secret." The trade secret frequently refers to special processes or strategies employed in the production of the goods. This kind of trade secret protects the production process rather than the final product

2. Methods of sales

Trade secret protection also extends to the methods and tactics used to market goods and services. Trade secret rules also safeguard the strategies used by any individual or organization to market their goods.

3. Recipe

The recipe of famous KFC or coca cola is the best example of recipes that are kept secret. The process by which some food or beverages are made by big restaurants and food chains also falls under the scope of trade secret. The recipes are protected by the laws if trade secret. The huge success of this fast food franchise or beverage franchise can be attributed to the confidential recipes that they use.

4. Formula, pattern or device

Any formula, pattern or device used by the company which is of economical value to the company and If information about such formula, pattern or device are published on the public domain or gets in the hand of their competition, will harm the company financially, it can be considered as trade secret. A trade secret also encompasses any formulas, patterns or devices that are used by the company to gain profit or advantage over other companies

5. Collectionof data

Even if the information is independently in the public domain, any data compilation created by

[10] Investopedia. (n.d.). What is a trade secret? Retrieved from https://www.investopedia.com/terms/t/trade-secret.asp

[11] World Intellectual Property Organization. (n.d.). Trade secrets. Retrieved from https://www.wipo.int/en/web/trade-secrets

 [ISSN 2581-5369]

a business that gives them an advantage over competitors may be regarded as a trade secret. The only thing that is regarded as a trade secret is the compilation of such work.

Trade secrets are not protected in India by any official laws, and attempts to obtain and disseminate such information in the public domain are not penalized. The common law doctrine governs trade secrets in India. India has worked to advance the trade secret industry in recent years. The national ipr policy was adopted in 2016 by Nirmala Sitharaman, the finance minister[12].This policy attempts to educate judges and those working in the legal field on how to handle trade secret infringement and the protection it can provide.

The dissemination, archiving, and utilization of trade secrets have been transformed by the digital age. Since the internet's creation and subsequent digitization, the world has entered a new era in which anything can be accessed with a single click and is available online. It is becoming increasingly difficult to protect trade secrets in the age of digital platforms and information exchange. Organizations and groups are having difficulty protecting trade secrets from unintentional disclosures, cyberattacks, and industrial espionage employing cutting-edge technologies[13]. The ease of access to the internet and the growing number of people using it to conduct criminal actions and conduct cyberattacks on digital platforms have affected and made it more difficult to safeguard and preserve trade secrets.

THE EMERGENCE OF DIGITAL OBJECTS AND ITS POTENTIAL FOR TRADE SECRET PROTECTION[14]

Today's corporate world relies heavily on digital objects. Organizations rely extensively on digital platforms since the introduction of cloud storage and computers, electronic communications, advanced data analytics, and massive language models such as GPT-4. The nature of digital things creates both opportunities and obstacles for trade secret protection. On the one side, digital formats enable efficient data storage, replication, calculation, and transmission. However, because digital material can be copied, shared, and distributed so easily, these qualities enhance the risk of illegal exposure, theft, or exploitation.

III. CHALLENGES IN THE PROTECTION OF TRADE SECRETS IN THE ERA OF DIGITALIZATION

The development of digitalization has changed the environment in the fields of intellectual

[12] **Narrative citation:** Press Information Bureau (2024) states that the Intellectual Property Rights Policy Management framework covers eight types of intellectual property rights.
[13] How Can We Safeguard Trade Secrets in the Digital Era?, PA Legal
[14] Wipo, at WIPO Guide to Trade Secrets and Innovation - Part VII: Trade secrets and digital objects

property and trade secrets particularly. In today's world, information can be found in a matter of seconds via digital channels. In the modern world, digitization has brought about a number of difficulties, such as the acquisition of private information by electronic means and the sharing of that information for profit. Due to digitalization, criminals now have a unique opportunity to obtain confidential information that large corporations keep hidden, which they can use to extort money from them or sell to rival companies. The consequences of misusing a trade secret can be disastrous; businesses whose trade secret has been compromised not only lose money but also their competitive advantage and marketpower.These effects of a compromised trade secret are long-lasting. The competitive edge that a firm has over other businesses is derived from its trade secrets, which are comparable to the hidden elements that make any business successful. Due to its delicate nature, trade secrets require a higher level of security and preservation than other types of information. It is the responsibility of businesses to protect trade secrets, and various laws should work to do so.

Trade secrets are more likely to be stolen online. Companies are increasingly using digital platforms to keep and preserve trade secrets. It is an efficient technique that simplifies a complex system of record keeping and allows for quick access. This has proven advantageous to businesses because it is cost-effective and saves time when accessing data and information via a common database. Data storage on a digital platform might give numerous benefits, but it also has many disadvantages. Digital storage is subject to being hacked, and any individual with adequate knowledge of computers can defeat the encryption to acquire the information held in these digital storage[15]. They can gain a company's trade secret by taking advantage of its network vulnerabilities, and they can compromise not just the trade secrets but also all of the data and information available on the digital platform.

Employees have the ability to share trade secrets as well. They can readily gain access to the database by granting permission, or they can grant permission to others to do the same. According to records, employees of those organizations[16] are responsible for 60% of all IT breaches. In addition, it has been observed that employees of the company violate the majority of trade secrets. These individuals have the ability and chance to steal confidential data without informing the appropriate authorities.

Digitalization has made it possible for information to be shared more methodically, and as a result, trade secret confidentiality is compromised when information is stolen via various

[15] Olmstead, L. (2022, December 2). *11 critical digital transformation challenges to overcome*. Whatfix.
[16] AMLEGALS. (n.d.). *Safeguarding trade secrets in the era of digitization*. Retrieved April 18, 2025, from https://amlegals.com/safeguarding-trade-secrets-in-the-era-of-digitization

electronic methods and sold or made public via digital platforms. The majority of the time, businesses steals trade secrets in order to compete with the company that owns them. The stealers utilize the information to obtain a competitive advantage. In order to stop the business that owns the confidential information from employing it in the marketplace, trade secrets are occasionally violated or made public. The advent of digital platforms has played a significant role in trade secrets. It has enormous obstacles for which no clear solution has been found.

1. Vulnerability to theft, cyber-attacks and data breaches[17]

Protecting digital trade secrets is difficult and risky in the digital age, especially when it comes to data breaches, cyberattacks, and theft. The security and integrity of important private information are seriously jeopardized by these dangers, which could have detrimental effects on a company's finances and reputation. Since digital trade secrets are so easily copied, shared, and distributed, one of the biggest obstacles to their protection is their increased susceptibility to theft. The preservation of digital trade secrets may also be seriously threatened by cyberattacks by skilled hackers and cybercriminals. The entire value of the trade secrets might also be lost due to data breaches, which are the disclosure of private information by hackers or unauthorized people who have access to a company's digital infrastructure.

Strong security measures, such as frequent updates and incident response plans, can be put in place to reduce the risks; however, security measures should also be reasonable, just like any other trade secret protection measures; the organization's features and the trade secret's value versus the cost of trade secret protection may also need to be considered.

2. Exposure during audits[18]

Internal and external audits are essential for evaluating financial performance, finding operational efficiencies, and guaranteeing compliance. Even when they are subject to non-disclosure agreements, auditors must have access to private company data in order to assess financial statements, internal controls, and regulatory compliance. This information exchange increases the possibility of trade secret theft or unintentional exposure to third parties.Businesses should create strong confidentiality agreements with auditors that clearly define the depth of crucial information they are permitted to access and their responsibilities with regard to trade secret protection in order to reduce the risk of digital trade secret exposure

[17] World Intellectual Property Organization. (n.d.). *Trade secrets and digital objects*. WIPO. Retrieved April 18, 2025, from https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

[18] World Intellectual Property Organization. (n.d.). *Guide to trade secrets and innovation – Part VII: Trade secrets and digital objects*. Retrieved April 18, 2025, from https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

during audits. Provisions for the return or destruction of any trade secret material gathered during the audit process should also be included in this agreement. Digital trade secrets can also be further protected during audits by putting in place technological measures including data encryption, access limits, and data trails.

3. Retrieving and regaining control of digital trade secret data[19]

Due to their digital accessibility, recovering and regaining control of digital trade secrets can be extremely difficult after they have been stolen or utilized without permission. To address this problem and try to minimize the possible harm, organizations might take specific actions. Businesses may think about using technology and digital forensics to trace and recover digital trade secrets in addition to the "traditional" method of recovering them through legal action. To track the unlawful use of trade secrets, locate the systems or places involved, and try to recover possession of the data, this may need collaborating with forensic specialists or specialized cybersecurity companies.

The level of skill of the unauthorized user, the scope of their actions, and the accessibility of digital proof all play a significant role in how successful these attempts are. A complete recovery may not always be ensured by legal and technological procedures to recover and reclaim control over the trade secret information. Thus, it may be emphasized once more how important it is to protect digital trade secrets from exposure and unauthorized use by implementing strong security and contractual measures, employee training, etc.

IV. METHODS TO SAFEGUARD TRADE SECRETS IN THE DIGITAL AGE

Businesses arefinding it more and more difficult to safeguard their trade secrets from infringement by competitors, and especially internet, this type of infringement has increased in frequency and severity. Digitalization has a number of implications on trade secrets, the most significant of which is that it can spread information in public, making the protections granted to trade secrets invalid or inaccessible. In the long run, the difficulties are so severe that they weaken the competitive edge that the business with the trade secret possesses. Governments around the world are working to preserve trade secrets and trademarks by expanding the protections already provided by the law. In addition to reducing the monopoly that trade secret holders have over the market, digital platforms aid in the public disclosure of trade secrets. The process of digitization has granted the ability to hack and obtain the trade secrets kept in the digital storage.

[19] WIPO,Trade Secret And Digital Object., Available at https://www.wipo.int/web-publications/wipo-guide-to-trade-secrets-and-innovation/en/part-vii-trade-secrets-and-digital-objects.html

Due to the growing difficulties businesses encounter in protecting trade secrets in the digital age, both the government and businesses must implement steps to safeguard and maintain trade secrets. The following are the measures:

Limiting access[20]

Limiting the amount of individuals who have access to sensitive information and making sure that the information provided to them is limited to what they require are the first and most important steps in ensuring trade secret protection. It will be simple to track down the source of secret information that has been made public if it is only shared with a small number of people. Restricting access to information also guarantees that only reliable individuals are exposed to it.

Contracts and non-disclosure agreements[21]

Second, it is crucial that businesses that possess trade secrets implement agreements and nondisclosure agreements (NDAs) that have the capacity to safeguard and maintain trade secrets. In the event that the trade secret being dealt with is stolen, the contract and NDAs will alert the other parties to the possibility of legal action and compensation. By employing the many techniques outlined by the legislation, the contracts and NDAs aim to protect the trade secret. Generally speaking, corporate entities advise using NDAs before to conducting business with any other parties, organizations, or institutions**.**

Measure regarding cybersecurity[22]

Businesses should invest in cybersecurity development if they want to keep their databases and networks safe. The majority of the time, the information and data held in digital storage are sensitive and require confidentiality. Digital storage systems are susceptible to hacking and tampering, which could reveal the data and information stored within its network. Sensitive information may include trade secrets or simply daily statistics and information. Functioning of the business. Improved cybersecurity and other safeguards like access control, authorization, review, and so forth are required for this data storage. to prevent the world from learning about trade secrets.

[20] World Intellectual Property Organization. (n.d.). *How to protect trade secrets?* Retrieved April 18, 2025, from https://www.wipo.int/tradesecrets/en/protection.html
[21] Provide. (n.d.). *Non-disclosure agreements (NDAs) in Singapore: 7 must-knows*. Retrieved April 18, 2025, from https://www.providecover.com/non-disclosure-agreements-ndas-in-singapore-7-must-knows
[22] AMLEGALS. (n.d.). *Safeguarding trade secrets in the era of digitization*. Retrieved April 18, 2025, from https://amlegals.com/safeguarding-trade-secrets-in-the-era-of-digitization

 [ISSN 2581-5369]

Regular review and revision[23]

Trade secret security and preservation can also be aided by measures like firewalls, access restrictions, and the use of specialized electronic devices to access sensitive data. Firewalls prevent hackers from accessing digital storage and give the business time to take action if they do. Restricting access to data guarantees that only a small number of individuals may access the database, and it will be simpler to identify any confidentiality violations. By enabling quick action in the event that one of the measures is not functioning as intended, a system of review and revision will guarantee that all the measures implemented for trade secret protection are effective and have not been compromised.

The digitization of intellectual property rights has forced businesses to apply a variety of strategies to safeguard trade secrets and reduce the harm that sensitive information may do to their businesses and the market. In order to safeguard trade secrets, the government and a number of businesses are interested in implementing new protection strategies.

V. LEGAL FRAMEWORK IN INDIA

The current trade secret protection framework in India is based on inter partes contractual obligations, common law remedies for breach of confidence, and equity considerations. The provisions of the Indian Contract Act, 1872 (henceforth referred to as the Contracts Act) and the Specific Relief Act, 1963, are crucial for contractual situations, especially those involving employer-employee conflicts. Under the Indian Penal Code, 1960 (and the Bharatiya Nyaya Sanhita, 2023, after it takes effect on July 1, 2024), there may be criminal liability for theft of trade secrets, criminal breach of trust, or cheating. The Information Technology Act of 2000 may also apply in cases involving computer-related offenses involving the theft or destruction of electronic records.[24]

1. Common Law (Contractual Obligations): In India, trade secrets are generally protected by contract law. Confidentiality and non-disclosure agreements (NDAs) are important instruments for protecting sensitive information because they place legal duties on workers, contractors, and third parties to retain confidentiality. Breaching these agreements may result in litigation lawsuits for damages or injunctions

[23] Brook, C. (2022, July 19). *What are the most important tips for preventing trade secret theft?* Digital Guardian. https://www.digitalguardian.com/blog/what-are-most-important-tips-preventing-trade-secret-theft

[24] The 22nd Law Commission Report on Trade Secrets: Call for a Balancing Act? Retrieved from https://corporate.cyrilamarchandblogs.com/2024/05/the-22nd-law-commission-report-on-trade-secrets-call-for-a-balancing-act/#:~:text=In%20India%2C%20the%20extant%20system,on%20July%201%2C%202024)

2. The Indian Penal Code (currently known as the Bharatiya Nyaya Sanhita) Unauthorized theft or misappropriation of property, including trade secrets, can result in criminal penalties. However, these clauses are primarily used in cases of theft rather than larger breaches of company secrets.
3. Indian Contract Act, 1872: The Indian Contract Act establishes a framework for enforcing non-disclosure agreements and confidentiality clauses, enabling businesses to protect trade secrets by imposing contractual restrictions on employees and stakeholders regarding the disclosure of sensitive information
4. The Information Technology Act of 2000: While the IT Act primarily addresses cybercrime and electronic transactions, it also includes safeguards to protect trade secrets, notably in circumstances of digital data misappropriation or unlawful disclosure. Section 66E penalizes violations of information privacy, including trade secrets that are digitally stored or communicated.
5. The Competition Act of 2002: The Competition Commission of India (CCI) oversees anti-competitive practices, and while it does not explicitly address trade secrets, it may be applicable in circumstances where improper use of confidential business information results in an unfair market advantage.

VI. CASE STUDY

The judiciary plays a vital role in protecting and developing the concept of trade secret where there is no codified law relating to it.

Diljit Titus, Advocate v. Mr. Alfred Adebare[25]

Ms. Seema Ahluwalia Jhingan, and others The plaintiff was the proprietor of Diljit Titus and Co., a legal business. Some of his employees left the company to form other businesses. Diljit said that the former workers stole client lists, legal advice, and views that the company had offered to clients. Mr. Adevare is said to have stolen over 3,000 business cards from Diljit's office. The argument was that any discussions between the client and the attorney in the attorney's office were confidential, privileged, and should not be disclosed at any time, whether employed or not. Plaintiffs must keep confidential information regarding their clients.The case of Diljeet Titus v. Alfred A. Adebare, decided by the Delhi High Court on May 8, 2006, established a landmark precedent in the field of legal professional relationships and the

[25] Delhi High Court upholds employer's exclusive rights over confidential legal databases. Retrieved from https://www.casemine.com/commentary/in/delhi-high-court-upholds-employer's-exclusive-rights-over-confidential-legal databases/view.

preservation of confidential information within law firms. This issue developed from a severance of contacts between the plaintiff, Mr. Diljeet Titus, and his former collaborators, which resulted in countersuits over the ownership and use of proprietary legal data and client databases.

Hi-Tech Systems v. Suprabhat Ray (2015 AIR Cal. 261)[26]

According to the Calcutta High Court, the workers were software developers who had a duty to keep all information and documents given to them private for the duration of their employment and for three years following the date of termination. actions taken against them. They quit, founded their own business, and used private information from alleged workers to start stealing the plaintiff's clients.The court decided that a restricted contract might be signed for a specific amount of time after leaving the company, even after employment. This is due to two factors: first, the settlement was time-limited and so satisfied the reasonableness standard established in Niranjan Golikari's case; second, it was intended to prevent the exploitation of the plaintiff's company's confidential information.

Waymo LLC v. Uber Technologies, Inc. (2018)[27]

Uber Technologies, Inc. (Uber) and Anthony Levandowski (defendants) were sued by Waymo LLC (plaintiff) in federal district court on the grounds that they had stolen Waymo trade secrets related to Waymo's development of so-called LiDAR, a crucial component of the experimental self-driving cars that both businesses were vying to create. Strong but not conclusive preliminary evidence presented by Waymo demonstrated that (1) a former key Waymo employee named Levandowski stole encrypted Waymo data related to LiDAR and then left Waymo under suspicious circumstances; (2) Uber invested a significant amount of money to entice Levandowski to leave Waymo, knowing that Levandowski had the stolen data and suspecting that some of the data contained LiDAR information that Uber could not easily determine on its own[28]

The Waymo LLC v. Uber Technologies, Inc. case clarified significant issues regarding digital trade secret theft in the technology sector, particularly with regard to the unlawful acquisition and use of confidential data pertaining to autonomous vehicle technology. In a market that is becoming more digital and linked, this ruling highlighted the necessity of robust legal protection

[26] Hi-Tech Systems & Services Ltd. v. Suprabhat Ray & Ors. (n.d.). High Court of Calcutta, India. Retrieved from https://vlex.in/vid/hi-tech-systems-services-654399605

[27] Waymo LLC v. Uber Technologies, 2017 WL 2123560 (2017). Retrieved from https://www.quimbee.com/cases/waymo-llc-v-uber-technologies

against trade secret theft.

VII. NECESSITY OF TRADE SECRETS STATUTE

The High Court of Delhi's Honourable Ms. Justice Pratibha M. Singh made a comment regarding the importance of trade secrets and data in light of the rise of artificial intelligence, technology, and the startup ecosystem. Companies spend a lot of money on data security and research. Businesses could suffer significant financial consequences if such private information were to leak. Given the serious repercussions of such theft, Justice Singh suggested that a trade secret statute be established.

The Law Commission report outlines the basic structure of the proposed legislation, including provisions on exceptions, limitations, remedies, and so on, and a draft bill named 'The Protection of Trade Secrets Bill, 2024' has been included to the LCR.[29] This bill proposes to formalize the acquisition, use, and disclosure of trade secrets, as well as the legal actions surrounding them. The question of whether trade secret law should be codified in order to balance the interests of industry, innovators, and the general public remains open. However, given the importance of trade secrets and sensitive information in Industry 4.0, the Commission's endeavour to establish comprehensive legislation on trade secret holder rights, legitimate acquisition/use, compulsory licensing, redress, secrecy, and so on may prove formative.

VIII. CONCLUSION

The protection of trade secrets in the digital era presents novel legal challenges that demand a dynamic and adaptive response. As proprietary information increasingly exists in digital formats, traditional concepts of trade secret protection—rooted in physical security and contractual obligations—must evolve to address threats such as cyber intrusion, unauthorized access, and global data transmission.

This research underscores the insufficiency of relying solely on conventional legal frameworks. While statutes like the Trade Secrets Act and international instruments such as the TRIPS Agreement and the EU Directive provide foundational protection, they must be interpreted and applied in light of digital realities. Courts, legislators, and legal practitioners must work in tandem to refine doctrines around reasonable security measures, misappropriation, and the extraterritorial reach of enforcement mechanisms.

Moreover, the burden on legal counsel has expanded. Legal professionals must now advise

[29] **Law Commission of India.** (2024). *22nd report* Government of India

 [ISSN 2581-5369]

clients not only on drafting robust confidentiality agreements and employment clauses but also on implementing data protection protocols, cybersecurity policies, and incident response strategies that satisfy the legal threshold for trade secret protection.

In an interconnected digital environment, harmonization of legal standards across jurisdictions is imperative. Disparities in national laws pose significant barriers to effective cross-border enforcement and create uncertainty for multinational entities.

In conclusion, safeguarding trade secrets in the digital age requires a legal approach that is both forward-looking and technologically informed. Only by integrating legal doctrine with technological understanding can trade secret law remain an effective tool for preserving competitive advantage and encouraging innovation in the modern economy.

*****

 [ISSN 2581-5369]