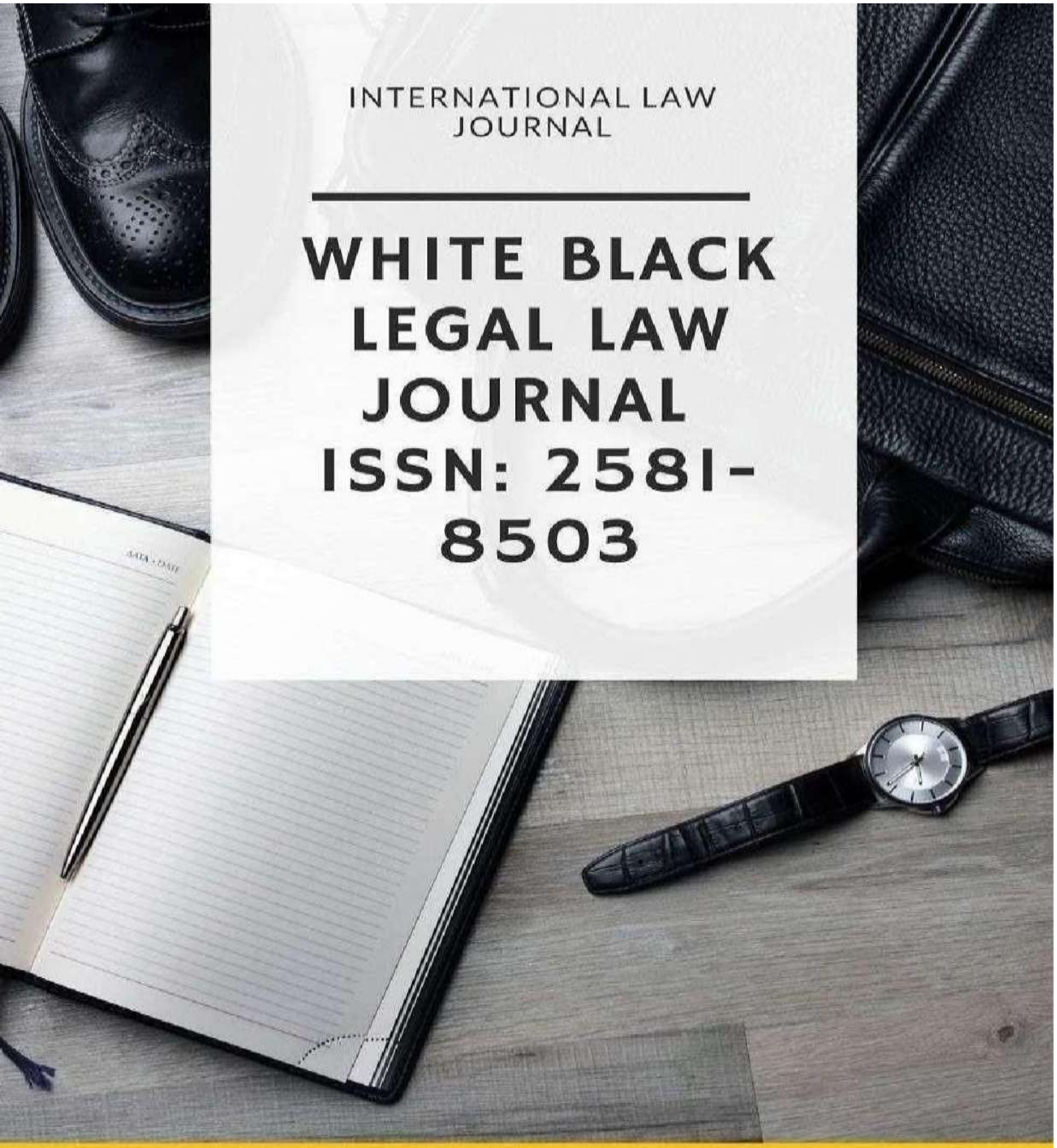

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

TRADE SECRET PROTECTION IN INDIA: LEGAL CHALLENGES IN THE DIGITAL AGE

AUTHORED BY - SHIVAM GAUR[1]

I. Introduction

In a world in which intangible property is becoming central to national economy and in which trade secrets have become the invisible plumbing of competitive advantage the sufficiency of the legal regime of a particular country to protect them has ceased to be a household legal matter but now a matter of world economic impact.

It is most acutely exemplified nowhere than in India the third largest knowledge economy in the world a fast digitising economy and a country that is positioning itself as the next global hub in pharmaceuticals semiconductors artificial intelligence and defence manufacturing and ironically the only major knowledge economy in the world that still operates without having a specific statutory regime in place to protect trade secrets.

The world has experienced a radical change in the economy shifting to the knowledge-driven innovative and intangible-based economy. Trade secrets have become possibly the most important element of intellectual property that a corporation possesses in this new environment. In the midst of India's growth and ambition, the law protecting the intellectual resources behind it remains weak. Protection now rests on a fragmented mix of contract law, breach of confidence, the IT Act, BNS provisions, and scattered judicial decisions. This is an analogous pre-digital legal architecture being tasked to do a fully modern job of guarding encrypted data bases cloud data repositories AI model weights and strategic data sets against AI-mediated extraction software insider cloud-based exfiltration and state-sponsored cyber espionage.

The cyber-economic espionage is a paradigm shift in the trade secrets compromising. In contrast to the older forms of industrial espionage where physical theft or employee subversion took place new forms of cyber-espionage exploit the interconnectedness of the global digital infrastructure to hack corporate networks all around the world with the use of Advanced Persistent Threats APTs Remote Access Trojans RATs and complex phishing attacks.[2]

Trade secrets are no longer paperwork that can be locked in a safe vault they are coded

[1] Final Year B.A.LL.B (Hons) Student at Amity Law School, Noida (AUUP)

[2] E Rowe, "RATs, TRAPs, and Trade Secrets" (2015) Boston College Law Review; Iryna Kornilova, "Cyber-Industrial Espionage: Its Nature and Consequences" (2024) Economic Scope.

databases secret algorithms the formula of a drug the layout of a semiconductor chip and the weights of an AI model uploaded to cloud servers and accessed remotely by remotely distributed workforces. Such assets can be stolen in a single cyber intrusion which can be performed immediately and without any physical evidence which makes the traditional legal framework essentially ill-equipped to combat.

This threat is also increased by the fact that it is transnational and supported by the state. Cyber-industrial espionage is also becoming a practice not only as a form of corporate malpractice but also as a tool of national economic policy with state-sponsored cyber-attackers gradually going after foreign businesses to steal proprietary information in favor of their local industries.

In the case of India where much of the global IT services infrastructure is based and where national capabilities in the areas of defence production space technology and semiconductor fabrication are rapidly emerging the overlap of trade secret vulnerability with national security has become a matter of concern that cannot be overlooked. The insider threat aspect further complicates the matter and is something that the current framework of India is especially unprepared to handle.

A large percentage of misappropriation of trade secrets is carried out by an employee or former employee who uses their legitimate access to do so maliciously with the assistance of outside cyber-attackers who offer technical assistance in data exfiltration. In India the judiciary hostility to apply post-employment non-compete agreements pursuant to sub-clause 27 of the Indian Contract Act 1872 provides a structural weakness through which valuable proprietary information is free to move in incumbent employees to rivals and upon which no civil or criminal remedy can be pursued by the harmed enterprise.[3]

II. Knowledge Economy Imperative

India's participation in the global knowledge economy is growing fast. By December 2024, it had become the world's third largest startup ecosystem, with over 1,57,000 DPIIT registered startups, more than 17.28 lakh direct jobs, and strong FDI inflows in 2024 to 25, especially in software, hardware, and other knowledge driven sectors such as pharmaceuticals, semiconductors, AI, and defence manufacturing.[4]

Trade secrets have become possibly the most important element of intellectual property that a corporation possesses in this new environment. Trade secrets have an advantage over patents

[3] Indian Contract Act 1872, s 27

[4] Press Information Bureau, Government of India, "Nine Years of Startup India" (PIB, January 2025) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2093125> accessed 20 March 2026.

because they are not required to be publicly disclosed in exchange of a limited monopoly and offer perpetual protection so long as the information stays secret and offers a competitive advantage. But it is within this context of ambitions and growth that the legal system that addresses the safeguarding of what are the intellectual resources that support this ecosystem is conspicuously weak.

The fragmented constellation of the Indian Contract Act 1872 the equitable doctrine of breach of confidence the provisions of the Information Technology Act 2000 criminal breach of trust under the Bharatiya Nyaya Sanhita 2023 and a case-by-case body of judicial precedents all contribute to protection. This is an analogous pre-digital legal architecture being tasked to do a fully modern job of guarding encrypted data bases cloud data repositories AI model weights and strategic data sets against AI-mediated extraction software insider cloud-based exfiltration and state-sponsored cyber espionage.

India is the only leading BRIC country that does not have a specific statute that regulates trade secret protection. Brazil protects trade secrets in the Industrial Property Law that offers civil and criminal protection. China has continued to reinforce its structure by making amendments to its Anti-Unfair Competition Law and Russia acknowledges commercial secrets under its Civil Code. On the contrary India still carries on with a patchwork of contractual duties equitable principles and common law doctrines which were created in the pre-digital era.[5]

III.Cyber Espionage Threats

Cyber espionage has become one of the most dangerous methods of trade secret theft in the present economy. It does not come with noise or open force. It works quietly through hidden access, copied files, and long periods where the victim does not even know that the system has already been entered.

The risk is especially serious because of Advanced Persistent Threats. These attacks are not random or momentary, they are planned and sustained intrusions that stay inside a network for long duration, observe the movement of data, and slowly remove what is valuable. By the time the organisation detects the breach, the secret may already be gone, and sometimes the damage is only visible much later.

The insider threat makes the situation more difficult. An employee or a former employee may already have legitimate access to confidential material, so the wrongful act can begin from

[5] Christopher A Buscaglia and Miriam F Weismann, "How 'Cybersafe' Are the BRICs?" (2012) 19 Richmond Journal of Global Law and Business 1.

inside the organisation itself. In such cases the breach often looks ordinary at first, and that is exactly why it is hard to control and hard to prove.

The pharmaceutical sector is one of the clearest examples of this danger. Trade secrets there include drug formulas, research notes, clinical trial data, production methods, and biosimilar techniques. If this information is stolen, the loss is not only financial, it can also destroy years of research and reduce the very basis on which market advantage is built.

AI related assets are under the same pressure, and in some cases even more. Model weights, training data, algorithm structure, and cloud based code libraries have now become core business assets. They can be copied very quickly once access is gained, but their real value is produced over long development cycles, so even a small leak can weaken the entire commercial position of the owner.[6]

Semiconductors and defence production raise the stakes further. These sectors depend on process knowledge, design information, and technical methods that are not easy to replace once exposed. If such material is taken by foreign linked actors, the loss goes beyond commerce and enters the field of national security, strategic autonomy and industrial self reliance.

The wider Indian digital economy is also exposed. Global Capability Centres, software development units, and data driven service platforms all hold sensitive proprietary information that is highly attractive to cyber attackers. As India becomes more central to innovation and technology services, the incentive to target such systems grows in the same measure.

The present law is not built for this reality. Cyber espionage is difficult because the stolen material is often not noticed at once, and its later use may appear only in another product, another market, or another business cycle. That creates serious proof problems, since the victim may know that a breach happened but still not be able to show exactly what was copied or how it was later used.

So cyber espionage should not be seen only as a technical problem. It is a direct attack on business value, innovation, and in some cases national strength itself. The real harm is not only in taking the information, but in breaking control over knowledge that gives a firm, or a sector, its competitive life.

[6] Iryna Kornilova, CYBER-INDUSTRIAL ESPIONAGE: ITS NATURE AND CONSEQUENCES, 2024 Econ. scope, https://doi.org/10.32782/2224-6282/190-45.

IV. Current Legal Framework

The Indian position on trade secret protection is still not settled in a proper and complete way. It is built on a mix of contract law, breach of confidence, the IT Act, the BNS, and separate judicial decisions, but there is no single statute giving one clear rule. In a fast digitising economy, that kind of arrangement is too loose and too uncertain.

NDAs are the primary ways that the Indian Contract Act of 1872 provides the fundamental contractual support. These agreements can be used between the parties that signed them, but they do not bind third parties, foreign hackers, or competing businesses that did not accept the terms of the agreement. Thus, only a portion of the actual issue is protected by the law.

Section 27 of ICA is the biggest legal obstacle. Indian courts have usually treated post employment restraints very strictly, and this means an employer cannot easily stop a former employee from joining a competitor even where sensitive information was handled during service. The result is a sharp gap between the need for secrecy and the law on labour mobility. This creates an odd situation. The employee may leave with knowledge, memory, and access to important material, while the employer is left to argue that some of that knowledge was really a protected secret. The line is often thin, and courts do not always draw it in the same way. That makes the law unpredictable for both sides.[7]

English law based breach of confidence doctrine helps, but only up to a point. Courts use it to stop misuse of confidential information, yet the test is still judge made and not fully stable.

One court may look at the secrecy, the manner of disclosure, and the misuse in one manner, while another may apply the same facts with different emphasis. This creates inconsistency in relief.[8]

Cyber theft makes the issue more acute. The owner might not notice the loss for months, and information can be duplicated without leaving any obvious marks. It could be challenging to prove precisely which files were stolen or how they later got into a competing system, even if the breach is suspected. The burden of proof becomes extremely heavy and occasionally nearly unattainable in these situations.[9]

The springboard principle is useful, but it is also unevenly applied. It is meant to stop a person from using stolen confidence as a head start, yet the exact reach of this rule changes from case to case. That is a serious weakness in technology related disputes, where former employees

[7] Indian Contract Act 1872, s 27

[8] J.P. Associates. The role of doctrine of confidentiality in intellectual property rights. *Trademark - India*. https://www.mondaq.com/india/trademark/1503186/the-role-of-doctrine-of-confidentiality-in-intellectual-property-rights. Published August 8, 2024.

[9] Iryna Kornilova, "Cyber-Industrial Espionage: Its Nature and Consequences" (2024) Economic Scope

may carry both lawful skill and confidential knowledge into new employment.[10]

IT Act 2000 also does not fully solve the issue. It deals with unauthorised access, copying, extraction, and some forms of electronic disclosure, but it does not treat trade secret theft as a separate economic wrong. A stolen pharma formula or AI model is not just hacked data, it is valuable business intelligence, and the law does not clearly reflect that.[11]

Same problem remains under the BNS. Its general offences on theft, cheating, and breach of trust are not designed for intangible digital assets. They can sometimes be used by analogy, but that is not enough for a modern trade secret regime. The law needs clearer language, stronger remedies, and a proper fit with the commercial nature of the harm.[12]

Present framework remains fragmented and weak. Contract law is narrow, Section 27 is rigid, breach of confidence is uncertain, and the IT Act and BNS do not speak directly to the real nature of cyber misappropriation. For India's knowledge based sectors, this is a serious legal gap.

V. Global Best Practices

The useful point for India is not copying any one system, but taking the parts that can actually fit its own legal and institutional setting. The real value of comparative models is in transferability, because India needs a framework that is stronger, faster, and more predictable, but still consistent with its constitutional structure and market realities.

One transferable element is a clear statutory definition of trade secrets. The foreign models show that protection becomes more workable when the law says what kind of information is covered, what counts as reasonable secrecy efforts, and how misappropriation is understood in a digital setting. For India, this matters because business certainty is weak when firms must depend on scattered contract law and vague common law ideas.

Another transferable element is evidence relief. Where trade secret theft is hidden and technical, the plaintiff often knows that something has been stolen but cannot easily prove the exact details at the start. A burden shifting rule, used in some systems, is useful for India because it reduces the unfairness of forcing the victim to prove what the thief has already concealed.

A third transferable element is quick and practical emergency relief. Trade secret cases are

[10] Juriah Abd. Jalil, "Addressing the Threats of Online Theft of Trade Secret and Cyber Espionage in Malaysia: The Legal Landscape" (2018) 6th International Conference on Cyber and IT Service Management (CITSM)
[11] Information Technology Act 2000, ss 43, 43A, 66, 72, 72A.
[12] Bharatiya Nyaya Sanhita 2023, ss 303, 316.

often lost by delay, because once data is copied, sent, or uploaded, later court success may come too late to matter. India can use the lesson that interim preservation, seizure like relief, and fast injunction type response are more valuable than slow and formal remedies that arrive after the secret is already spread.

The administrative side is also important for India. A system that allows some form of specialized enforcement, without forcing every case into expensive and lengthy ordinary litigation, would help smaller firms and also reduce pressure on courts. The main lesson here is that enforcement must be usable, not only correct on paper.

Criminal deterrence is another transferable idea, but it needs Indian calibration. The point is not to create harshness for its own sake, but to make deliberate theft, especially of strategic commercial information, a real legal risk for the offender. For India, this is most useful where the penalty reflects the gravity of the stolen information and the harm to competition, innovation, and security.

The comparative analysis also suggests that protection should be balanced with mobility and fair competition. India cannot afford a law that blocks employees from using honest skills or creates fear around legitimate reverse engineering. The better lesson is that a good system protects secrecy without freezing the movement of knowledge that healthy innovation depends on.

Institutional predictability is another key lesson. Trade secret protection becomes credible when courts or specialised forums apply the rules consistently, handle confidentiality carefully, and give commercially meaningful relief. India can take this lesson without imitation, by building more specialisation, more technical understanding, and more reliable case handling inside its own framework.

In the Indian context, the central transferability question is therefore simple. Which foreign tools can close India's evidentiary gap, its delay problem, its deterrence weakness, and its uncertainty in enforcement, without overreaching into overprotection? The answer lies in a selective model that improves definition, proof, urgent relief, deterrence, and institutional speed while still preserving employee freedom and competitive balance.

The larger conclusion is that global best practice is useful only when it is translated into Indian conditions. India does not need a borrowed model in full, but it does need transferable elements that make trade secret law more real, more usable, and more aligned with the demands of a modern knowledge economy.

VI.Economic and Security Stakes

The weakness of Indian trade secret protection is not only a legal gap, it is a direct economic loss and a security risk too. In a knowledge economy like India, the cost of one serious theft can move from one company balance sheet to whole sectors, and sometimes to national interest also.

The economic side is measurable. The trade secret injury is not limited to lost data, but it includes lost research years, lost market edge, lost investor confidence, and delay in future growth. The links between stronger protection is reciprocal to higher FDI, more technology transfer, and better innovation output, so the absence of a proper statute becomes a real competitive disadvantage and not a theoretical one.

This is why the deterrence need is so important. If the law only gives weak civil remedies, or slow process, then a well resourced offender can treat trade secret theft as a low risk activity. The text notes that the current framework does not provide enough emergency relief, and that digital evidence can disappear in hours, which makes ordinary remedies too late in many cases.

The losses are sharper in sectors where secrets are the main asset. Pharmaceuticals depend on formulas, manufacturing methods, clinical data, and process know how. IT services and GCC work depend on source code, algorithms, customer structures, and AI related assets.

Semiconductors and defence depend on design architecture, process technology, and highly sensitive technical information, so one leak can damage future contracts and also weaken strategic capability.[13]

The security overlap is now unavoidable. The article language shows that India is facing rising cyber incidents, state sponsored attacks, and targeted espionage against defence, telecommunications, manufacturing, and strategic infrastructure. When trade secret theft is done for a foreign government or foreign entity, it is not just commercial cheating, it starts looking like economic warfare with national security effect.

That is why a stronger criminal response is needed, not only a private law response. The current structure does not clearly punish economic espionage as a separate wrong, and that leaves a gap where foreign linked actors can exploit commercial weakness without facing enough legal fear. In such situations, deterrence is not about punishment for its own sake, it is about making sure the cost of theft becomes higher than the benefit of stealing.

There is also a broader policy loss if the law stays weak for long. Multinational companies,

[13] Foreign Direct Investment (FDI). India Brand Equity Foundation. https://www.ibef.org/economy/foreign-direct-investment

research centres, and high value manufacturers look at the legal climate before putting their most sensitive operations in a country. If the system cannot protect trade secrets properly, India risks losing the very kind of investment that brings technology transfer, advanced jobs, and deeper industrial capacity.

The security point is even more serious because trade secret theft can target defence supply chains, semiconductor design, pharma research, and critical digital systems without touching classified government files directly. That means the harm can sit in the private sector but still hurt the state, the economy, and public resilience. So the need is not only for protection of business confidence, but for a stronger national security posture that recognizes cyber enabled commercial espionage as a strategic threat.

The basic message is simple. India cannot treat trade secret theft as a small commercial dispute anymore, because the losses are economic, the deterrence gap is real, and the national security overlap is already visible in current cyber threat patterns.

VII. Reforms and Conclusion

The needed reform is not a grand overcomplication, but a cleaner statutory structure that gives trade secrets a clear legal home. India should move from scattered protection to one coherent framework that can deal with digital theft, insider misuse, and foreign linked misappropriation in a more direct way.

The first suggestion is simple definition. The law should clearly say what a trade secret is, including digital information, AI related material, datasets, source code, process know how, and other confidential business information that gets real commercial value from secrecy. The present uncertainty only helps the wrong side, because businesses then do not know exactly what is protected and courts also have to improvise too much.

The second suggestion is stronger and faster enforcement. A trade secret owner should not be forced to wait until the damage is already complete, because in the digital world leakage can happen in minutes and not in months. The legal system must therefore give quick interim relief, easier preservation of evidence, and special procedures that can stop destruction, copying, or overseas transmission before the secret is gone for good.

The third suggestion is criminal deterrence. Civil remedies alone do not properly answer serious economic espionage, especially when the theft is planned, organised, or done for foreign advantage. The law should create a clearer offence for deliberate trade secret theft, with seriousness linked to the value of the stolen information and the harm caused to the business

and to national interest.

The fourth suggestion is cross border reach. Trade secret theft today rarely stays inside one border, because the stolen material can move through servers, cloud systems, shell entities, and foreign hands very fast. Indian law should therefore give better tools for jurisdiction, cooperation, and evidence gathering when the wrongdoer or the receiving benefit is outside India, otherwise the law remains local while the crime is global.

The fifth suggestion is institutional capacity. Trade secret disputes are not ordinary commercial disputes only, because they often need technical understanding, secrecy control, and speed of hearing. Specialised benches, trained judges, and forensic support would make enforcement more practical and less dependent on slow general procedure.

At the same time, reform must stay balanced. Protection should not become a weapon against employee mobility, fair competition, or legitimate reverse engineering. The aim is not to lock down all knowledge, but to protect genuinely secret and valuable information while still allowing skills, experience, and lawful learning to move in the economy.

That balance is important because India's strength is its innovation ecosystem, its skilled labour, and its growing role as a global technology base. A good trade secret regime will not hurt that strength, it will support it by giving investors and innovators confidence that their most sensitive work will not be stolen without consequence.

In conclusion, the larger point is that India can no longer rely on a weak and fragmented arrangement for something that now touches competitiveness, innovation, and security together. A proper statutory regime, if drafted with clarity and restraint, would not only protect private business interests but also strengthen the country's place in the global knowledge economy.