Himachal Pradesh National Law University, Shimla (India)
HPNLU JOURNAL OF LAW, BUSINESS AND ECONOMICS (HPNLU JLBE)

JOURNAL ARTICLES *ISSN: 2584-0436* **HPNLU JLBE**

Volume III (2024)

PROTECTION OF TRADE SECRETS IN INDIA: AN ANALYSIS

Santosh Kumar Sharma & Girjesh Shukla

CONTENTS

Essay & Comments

PROTECTION OF TRADE SECRETS IN INDIA: AN ANALYSIS

Santosh Kumar Sharma & Girjesh Shukla***

Abstract

This paper analyses the inadequacy of India's existing legal framework in protecting trade secrets and confidential business information, especially from a criminal law perspective. In the absence of a specific statutory provision, businesses rely on tortious liability, contractual obligations, and principles of equity to secure such sensitive data. The newly introduced the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code, 1860, fall short in prescribing remedies for violation of trade secrets.

Drawing a comparative analysis from jurisdictions of the United States, the United Kingdom, and the People's Republic of China, each having a mix of civil and penal protection for trade secrets, the paper makes a case for India to enact statutory provisions, particularly penal sanctions, to safeguard trade secrets. It further provides a critique of the proposed Protection of Trade Secrets Bill, 2024. The paper concludes with policy recommendations to harmonise India's approach with global best practices.

Keywords: Trade Secrets, BNS, 2023, Intellectual Property Rights, IPR, Penal Law, TRIPS, Business Law, etc.

I

Introduction

Trade secrets form an essential pillar of intellectual property in the modern globalised economy. Unlike patents or trademarks, which rely on public disclosure in exchange for exclusivity, trade secrets derive their commercial value by remaining undisclosed. Trade secrets cover a wide array of proprietary business information, such as algorithms, manufacturing processes, client lists, pricing strategies, research data, chemical formulas, etc., often making the difference between competitive leadership and market irrelevance.[1] In a world increasingly

* Associate Professor of Law, Himachal Pradesh National Law University, Shimla.
** Professor of Law, Himachal Pradesh National Law University, Shimla.

driven by innovation, data, and rapid technological advancement, trade secrets have emerged as the currency of knowledge economies. With the expansion of digital infrastructure, the boundaries between physical and intangible property have blurred, exposing confidential information to cyber risks, insider threats, and cross-border theft. In such an environment, the absence of a clear and enforceable legal regime to protect trade secrets leaves businesses, particularly startups, research institutions, and high-tech firms, extremely vulnerable.[2]

India, despite being a major hub for IT services, pharmaceuticals, and R&D-intensive sectors, does not have a specific standalone statute governing trade secrets. The existing legal protection revolves around the judicial decisions, the law of contract law, and the law of torts, viz., breach of confidence.[3] The Indian courts have granted injunctions and awarded damages in certain cases of proven breach of trade secrets, yet the instances are limited and without much deterrent value. Without having provisions for penal sanctions, there is a serious gap in the law, especially in terms of misuse of confidential information, theft of trade secrets, or hackers committing cyber theft.

In view of the growing economy with over 1 lakh startups, incubation centres, and a phenomenal development in the biotechnology sector, fintech, and artificial intelligence, protecting trade secrets is imperative, and a key to providing economic strength and national competitiveness.[4] Further, India is a signatory to the TRIPS Agreement, which *inter alia* mandates the member states to protect '*undisclosed information*' from being wrongly used, stolen, or shared.[5]

The Law Commission of India, in its 289th Report (2024), has suggested a new law called the *Protection of Trade Secrets Bill*. This proposed law includes both civil and criminal provisions against the violator, along with protection for the whistleblowers. It further provides conditions and circumstances under which the trade secrets can be used in the public interest, such as through compulsory licensing. The new bill has probably been an attempt due to the inefficacy of the present framework. Even the judicial precedents, such as *Niranjan Shankar Golikari v. Century Spinning*[6] and *John Richard Brady v. Chemical Process Equipments Pvt. Ltd*,[7]

---

[1] World Intellectual Property Organization (WIPO), "What is a Trade Secret?", *available at:* www.wipo.int.
(Last visited April 12,2025)
[2] Peter K. Yu, *Trade Secret Hacking and the Civil–Criminal Divide*, Colum. J. Transnat'l L., 2016.
[3] The Indian Contract Act, 1872. S. 27.
[4] The Ministry of Commerce and Industry, STARTUP INDIA ANNUAL REPORT, 2023.
[5] WORLD TRADE ORGANIZATION, TRIPS Agreement, Art. 39.
[6] AIR 1967 SC 1098.
[7] AIR 1987 Delhi 372.

etc., locate their legal force through non-disclosure agreements. Recently, in *HT Process Controls Pvt. Ltd. v. Ankur Gupta*,[8] the Delhi High Court gave temporary relief when private business data was transferred without permission. The problem with this approach is that the availability of civil remedies doesn't go far enough to punish wrongdoers or stop others from doing the same.

This paper begins with the assumption that civil law remedies are not enough to protect trade secrets. We need criminal laws, similar to those of other developed economies like the U.S. Economic Espionage Act, 1996, and China's Anti-Unfair Competition Law, to stop the violations of trade secrets and show investors that their ideas and information will be protected.

II

Comparative Legal Approaches to Trade Secret Protection

The law relating to trade secrets is very dynamic and keeps developing differently in different countries. Some countries, like the United States, mostly use criminal laws to deal with trade secret theft, whereas others, like the United Kingdom, depend more on civil laws and fairness-based principles, often called equitable doctrines. There is a third approach, also, like China, which uses a mix of both civil and criminal to deal with trade secrets.

The United States: A Dual Enforcement Model

The United States offers a dual-layered system for trade secret protection — consisting of civil and criminal remedies. The civil law in the United States for the protection of trade secrets relies on the Uniform Trade Secrets Act, 1979 (UTSA), a model law published by the Uniform Law Commission in 1979, and the Defend Trade Secrets Act, 2016 (DTSA). Most of the states of the USA have adopted the UTSA, which provides a civil framework for owners of trade secrets to seek relief in the form of injunctions, damages- actual or exemplary, and recovery of litigation costs.[9] The Defend Trade Secrets Act of 2016 was enacted at the federal level, which offers a civil cause of action in federal court, allowing trade secret owners to obtain *ex parte* seizure orders, injunctive relief, and damages. Bringing a national uniformity to civil trade secret protection, this law enables companies to file claims across states, especially in cross-border data misappropriation cases.[10]

[8] 2024 SCC OnLine Del 1192.

[9] Uniform Trade Secrets Act, National Conference of Commissioners, USA.

[10] Defend Trade Secrets Act, Pub. L. 114–153 (2016).

The criminal law remedies in the USA revolve around the Economic Espionage Act, 1996. This law criminalises theft of trade secrets intended to benefit a foreign entity or theft for commercial advantage. Penalties include up to 15 years of imprisonment and fines up to $5 million for corporations.[11] One key aspect of U.S. enforcement is the active role of federal agencies, including the Department of Justice, in prosecuting trade secret crimes.

United Kingdom: The Doctrine of Breach of Confidence and The EU Influence

Unlike the USA, the United Kingdom does not have a specific standalone statute on trade secrets. Instead, it relies on the common law doctrine of breach of confidence, supplemented by statutory tools like the Trade Secrets (Enforcement, etc.) Regulations, 2018, and thereby brings the European Union Trade Secrets Directives into domestic law.[12] Post-Brexit, the UK continues to enforce the Trade Secrets (Enforcement, etc.) Regulations, 2018, and thereby UK courts often order injunctions, damages, destruction or delivery-up of infringing material, and protection of confidential information during litigation through non-disclosure orders and private hearings.[13]

Under the common law doctrines, such as 'breach of confidence', a claimant is required to prove three elements to prove their case. *Firstly*, the information must have the necessary quality of confidence; *secondly*, it must have been communicated in circumstances importing an obligation of confidence; and *thirdly*, there must be an unauthorised use of that information causing detriment to the owner.[14] This doctrine has been affirmed in cases such as *Coco* v. *A.N. Clark (Engineers) Ltd.*[15] and *Attorney General* v. *Guardian Newspapers Ltd. (No 2)*,[16] commonly known as the *Spycatcher* case.[17] However, criminal liability under UK law is limited. Theft or fraud statutes may be applied in egregious cases, but there is no general offence of trade secret misappropriation unless tied to economic espionage or state security concerns.

China: A Mixed Model

[11] 18 U.S. Code §§ 1831–1839, Economic Espionage Act.
[12] Trade Secrets (Enforcement, etc.) Regulations 2018, SI 2018 No. 597.
[13] UKIPO, "Trade Secrets and the Law Post-Brexit," 2022.
[14] Coco v. A.N. Clark (Engineers) Ltd., [1969] RPC 41.
[15] *Id.*
[16] Attorney General v. Guardian Newspapers Ltd. (No 2), [1990] 1 AC 109.
[17] [1990] 1 AC 109; [1988] 3 All ER 545; [1987] 1 WLR 1248.

In the People's Republic of China, the protection of trade secrets is primarily regulated by the Anti-Unfair Competition Law, 2019 (AUCL), supplemented by the Criminal Law and judicial interpretations. The AUCL, 2019, especially Article 9, defines trade secrets and includes unauthorised acquisition, disclosure, and use through means such as theft, bribery, coercion, or cyber intrusion.[18] The amendments in AUCL, 2019, further instituted burden-shifting provisions, thereby granting courts the authority to presume misappropriation upon the presentation of *prima facie* evidence. China has also enacted punitive damages for instances of egregious misappropriation and has augmented the maximum penalties imposed on infringers. It further creates employer liability, exceptions for reverse engineering, and the involvement of intermediaries in violations of trade secrets. Further, Article 219 of the Criminal Law of the People's Republic of China criminalises the theft of trade secrets in situations where the resultant losses surpass a specified financial threshold. Penalties include up to 7 years imprisonment, and in state-related offences, charges may escalate to espionage under national security statutes.[19]

With judicial guidelines on admissibility of evidence, information secrecy during court cases, and burden of proof, the Chinese legal system made the legal process stronger for both civil and criminal matters.[20] One reason for these changes was the US–China Phase One Trade Agreement signed in 2020, where the United States asked China to improve how it protects trade secrets.

The U.S. model shows that criminal enforcement and civil protection must go hand-in-hand for effective deterrence, whereas the Chinese hybrid model suggests that a rapid legislative reform, supported by judicial and administrative mechanisms, can deliver credible protection to trade secrets. The above developments can be a lesson for other countries, such as India.

III

India's Legal Framework: Doctrinal Origins & Statutory Gaps

India's legal architecture for the protection of trade secrets suffers from being underdeveloped, lacking any statutory definition, innovative procedural tools, and adequate penal consequences. The system remains heavily reliant on contractual

[18] Anti-Unfair Competition Law of the People's Republic of China, 2019, Article 9.
[19] The Criminal Law of the People's Republic of China, Article 219 (Amended 2020).
[20] "Top court grows confidence in protection of seed breeding" available at Criminal Law

obligations, equitable remedies, and judicial interpretation rather than codified norms.

Reliance on Civil Remedies & Equitable Doctrines

In India, trade secrets are usually protected through service contracts, i.e. by adding confidentiality clauses in service agreements, signing non-disclosure agreements, and inserting terms in licensing or partnership agreements.[21] While these laws do not allow agreements that stop someone from doing business (such as restraint of trade), it does allow reasonable conditions if they are needed to protect essential business information. In *Niranjan Shankar Golikari* v. *Century Spinning & Mfg. Co.*,[22] the Supreme Court ruled that restrictions placed on employees can be valid, even after their leaving the employment, if they are meant to protect confidential information and trade secrets. In *John Richard Brady v. Chemical Process Equipment Pvt. Ltd.*,[23] the Delhi High Court agreed that breaking someone's trust by sharing confidential information is a good reason to stop a former employee from using business secrets learned during the job.

While these decisions provide legal support for businesses seeking to enforce trade secret rights, they suffer from key limitations, *viz.*, no statutory definition of what constitutes a trade secret; remedies are *ex post* and largely limited to injunctions or damages; heavy burden of proof on the plaintiff, resulting in protracted litigation; and the courts vary significantly in interpreting what level of 'confidentiality' is sufficient to qualify for protection.

Indian courts have relied on equitable doctrines such as *breach of confidence* to protect trade secrets. These are rooted in common law and require proof, *firstly*, that information disclosed had the necessary quality of confidence, *secondly*, the information was communicated under circumstances importing an obligation of confidentiality; and *thirdly*, there was an unauthorised use or disclosure causing harm to the owner.[24]

This doctrine has been applied in India with mixed results. For example, in *Mr. Anil Gupta* v. *Mr. Kunal Dasgupta*,[25] the Delhi High Court recognised breach of confidence in the context of a business idea, awarding interim relief despite the absence of a

[21] The Indian Contract Act, 1872. S. 27.
[22] AIR 1967 SC 1098.
[23] AIR 1987 Delhi 372.
[24] *Saltman Engineering v. Campbell Engineering*, [1948] 65 RPC 203.
[25] 2002 SCC OnLine Del 518.

formal contract. Further, equitable relief is discretionary and does not always provide for punitive consequences.

Information Technology Act, 2000

The Information Technology Act, 2000, *vide* Section 72, penalises breach of confidentiality and privacy by persons who have access to data through lawful means. This section applies primarily to intermediaries, data custodians and has been applied in some trade secret violation cases. There is no comprehensive provision in the IT Act that criminalises misappropriation of business secrets *per se*. Moreover, enforcement under the Act is riddled with procedural and evidentiary issues, making it a weak substitute for a dedicated penal framework.[26]

Inconsistent Interpretations

The Indian courts have struggled with many questions while examining criminal liability in breach of trade secrets. For example, can a business process or algorithm be protected without a patent? What distinguishes general skill and knowledge from proprietary information? How do courts handle trade secrets embedded in digital formats like source code or AI models?

In *Tata Motors Ltd.* v. *State of Bengal*,[27] the Calcutta High Court expressed scepticism over claims of proprietary business data, suggesting that unless there is "clear secrecy" and "economic value," no claim of misappropriation arises. In contrast, other High Courts have granted broad relief even on tentative evidence of misuse. Such inconsistency underscores the need for legislative clarity. Without a definition of trade secrets or guidelines for evaluating "reasonable efforts to maintain secrecy", as seen in U.S. or Chinese models, courts are left to rely on a patchwork of precedents and general principles.

Even where relief is granted, enforcement faces practical hurdles in terms of delays in interim relief, lack of confidentiality protection in litigation and related risks of further disclosure, etc. Also, India does not have a provision for punitive damages, as seen in U.S. or Chinese law. India's Commercial Courts Act, 2015, mandates faster resolution of commercial disputes, but procedural reform alone cannot cure doctrinal weaknesses.

The failure to provide robust trade secret protection has broader economic consequences. *Firstly*, Indian startups may hesitate to collaborate with foreign firms

[26] *Tata Motors Ltd. v. State of Bengal*, 2011 SCC OnLine Cal 1064.
[27] Section 2(c)(xvii), The Commercial Courts Act, 2015.

due to fear of idea theft. *Secondly,* Multinational corporations often restrict R&D or knowledge transfer into India. *Lastly, d*omestic innovators resort to patenting even when secrecy would be a better option — increasing costs and diluting competitive advantage. Worse, in sectors like pharmaceuticals, Agri-tech, and AI, the absence of trade secret protection exposes Indian firms to reverse engineering and unfair competition.

IV

The Bharatiya Nyaya Sanhita, 2023: Emerging Criminal Law and Protection of Trade Secrets

The most glaring deficiency in the Indian legal regime is the absence of criminal liability for trade secret misappropriation. Victims must attempt to fit their claims into general penal provisions under the hitherto existing Indian Penal Code, 1860 or its successor, the Bharatiya Nyaya Sanhita, 2023. Commonly invoked provisions are dishonest misappropriation of property,[28] criminal breach of trust,[29] and criminal breach of trust by clerk or servant, etc.[30] However, these provisions are not tailored to the unique character of trade secrets. They often require proof of physical misappropriation, ownership of "property" in a tangible sense, or a fiduciary relationship — none of which precisely aligns with the nature of digital or intangible proprietary data.[31] In *Emergent Genetics India (P) Ltd.* v. *Shailendra Shivam & Ors.*[32] , the Delhi High Court refused to classify genetic information as a "property" under IPC, demonstrating the limitations of applying archaic provisions to modern trade secret issues.

India's criminal law system has undergone a major transition with the enactment of the Bharatiya Nyaya Sanhita, 2023. This enactment offered a unique opportunity to align India's criminal jurisprudence with the demands of the modern digital and innovation economy — including the long-neglected domain of trade secret protection. However, a close reading of BNS reveals that while certain interpretive openings exist, the law still fails to provide a specific, direct, and coherent penal framework for trade secret misappropriation.

The BNS introduces several forward-looking concepts, such as expanding the definition of "property" to include intangible assets, recognising cybercrimes and

---

[28] Indian Penal Code, 1860, Sections 403 / The Bhartiya Nyaya Sanhita, 2023, S. 314.
[29] Indian Penal Code, 1860, Sections 406 / The Bhartiya Nyaya Sanhita, 2023, S. 316.
[30] Indian Penal Code, 1860, Sections 408 / The Bhartiya Nyaya Sanhita, 2023, S. 316(4).
[31] *Emergent Genetics India (P) Ltd. v. Shailendra Shivam*, (2005) 11 SCC 245.
[32] The Information Technology Act, 2000, Section 72.

digital offences, enhancing criminal penalties for corporate fraud and speedier trial processes and digital evidence admissibility.

A few sections of BNS could be interpreted to address certain aspects of trade secret misappropriation, but these applications are neither direct nor doctrinally precise.

The offence of theft of intangible property,[33] is a novel inclusion, and it would expand the concept of theft, covering certain forms of intangible property.[34] The earlier definition under IPC, 1860, offence of theft involves movable property, but now it will cover digital assets, data files, or digitally stored confidential material. If 'trade secrets' are stored in digital form, the same would be attracting this law now, even though trade secrets are explicitly not mentioned.

Dishonest Receipt of Stolen Property,[35] **is** penalizes the receipt or concealment of stolen property, which may theoretically extend to trade secrets, particularly if stolen in digital form. However, "property" in the penal sense has traditionally referred to tangible or movable goods. Courts have hesitated to extend this concept to data, especially where the "original" remains with the owner and no physical transfer occurs.[36] Section 316 (1) is a re-codification of Section 405 of the IPC, 1860, penalising any person who dishonestly misappropriates or converts to their own use any property entrusted to them, or who violates any legal contract—express or implied—regarding such trust.[37]. In cases where employees misuse trade secrets for personal gain or pass them to rivals, this provision becomes particularly relevant. Courts have previously applied criminal breach of trust doctrines to IP and commercial misappropriation cases under the IPC.[38]

The offence of criminal breach of trust,[39] criminalizes dishonest use or disposal of property entrusted to someone to whom the property was entrusted. It may apply in employment-related trade secret theft, particularly when an employee misuses confidential information. This section requires a fiduciary relationship, and thus, provides a limited applicability in cases of trade secrets, as may not exist in all trade secret violations — especially those involving cyber-espionage or third-party actors. For instance, if a company executive shares proprietary pricing models or technical blueprints with a competitor, it may fall within the scope of '*unauthorised disclosure*'

---

[33] Bhartiya Nayay Sanhita, 2023, S. 303 (1) read with Explanation.
[34] Bhartiya Nayay Sanhita, 2023, S. 303.
[35] Bhartiya Nayay Sanhita, 2023, S. 316(1).
[36] *Emergent Genetics India (P) Ltd.* v. *Shailendra Shivam*, (2005) 11 SCC 245.
[37] Bhartiya Nayay Sanhita, 2023, S. 316(1).
[38] *R. K. Dalmia v. Delhi Administration*, AIR 1962 SC 1821.
[39] Bharatiya Nyaya Sanhita, 2023, S. 316(5).

under this section. This creates a statutory bridge between fiduciary misconduct and criminal liability, especially in employer-employee contexts

The BNSS also introduces procedural reforms that support trade secret enforcement. Now the electronic evidence is granted expanded admissibility,[40] witness protection measures are streamlined, and forensic digital analysis becomes central to investigations.[41] This strengthens the ability of victims of trade secret theft to collect, preserve, and present digital evidence, which is often a challenge under the older IPC framework.

No Statutory Recognition of Trade Secrets

The BNS, 2023, does not define "trade secrets" as a distinct legal category. Without a statutory definition, enforcement agencies and courts remain bound by case-specific arguments and creative pleading, weakening deterrence and increasing the litigation burden on victims.[42]

The rationale for criminalising trade secret misappropriation lies in economic harm, breach of trust, and societal deterrence. The Trade secret theft often results in economic harm, i.e. irreversible loss of market share, reputational damage, and compromised innovation. It also results in breach of trust. To address these concerns, the BNS, 2023 should be amended to include a new chapter or section specifically addressing trade secret offences, along with a definition of 'trade secret' in line with Article 39 of the TRIPS Agreement.[43]

It may be pointed out that in the absence of a clear definition and provision for punishment, law enforcement authorities may not be able to pursue trade secret theft under general penal laws. Courts are wary of criminalising commercial disputes, cross-jurisdictional digital evidence complicates trials, and a lack of technical expertise amongst the enforcement agencies weakens evidence collection. Embedding trade secret protection in new criminal laws would eliminate these ambiguities.

---

[40] Bhartiya Sakshya Adhiniyam, 2023, S.479-482.
[41] Bhartiya Sakshya Adhiniyam, 2023, S.61–65, S.73 and S.74 are relevant for digital evidence protocols.
[42] *Emergent Genetics India (P) Ltd*. v. *Shailendra Shivam*, (2005) 11 SCC 245.
[43] TRIPS Agreement, Article 39, WTO.

V

The Protection of Trade Secrets Bill, 2024

Based on the Law Commission recommendation *vide* 289th Report, 2024, the Protection of Trade Secrets Bill, 2024 became the recent response towards having a legal framework for protecting confidential business information. It provides comprehensive remedies, drawing on some of the global best practices, tailored to India's domestic needs.

The 289th Law Commission Report[44], titled *"Trade Secrets and Economic Espionage"*, identified the absence of specific legislation as a key factor in India's poor trade secret enforcement record. The Commission highlighted that the existing contract and tort remedies were insufficient for deterrence, and the digital misappropriation was often left unaddressed. It further pointed out that without having a legal structure, India was lagging in TRIPS compliance under **Article 39,** which mandates 'protection of undisclosed information.'

Definitional Clarity and Scope

Section 2(f) of the draft Bill for the protection of Trade Secrets defines "trade secret" as:

> *"trade secret" means any information*
> *(i) that is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;*
> *(ii) that derives commercial value on account of being secret;*
> *(iii) that has been subject to reasonable steps under the circumstances, by the holder of such information, to keep it secret; and*
> *(iv) the disclosure of which is likely to cause damage to the holder of such information.*
> *Explanation.-For the purposes of sub-clause (f), (II) experiences and skills acquired by an employee in the course of normal professional*

[44] LAW COMMISSION OF INDIA, *Trade Secrets and Economic Espionage*, Report No.289, March,2024, *available at:* https://lawcommissionofindia.nic.in/report_twentysecond/ (last visited 4th December 2024).

> *practice; or (II) any information disclosing a violation of any law shall not amount to a trade secret."*[45]

This definition aligns with the Uniform Trade Secrets Act, 1979 (UTSA), of the United States, and also Article 39 of the TRIPS Agreement. It covers both tangible and intangible information, whether technical or commercial. The Bill does not require formal registration, thereby maintaining the flexible nature of trade secret protection.

The Bill allows trade secret holders to approach civil courts for injunctions, destruction or return of misappropriated material, compensatory and punitive damages, along with costs of litigation in certain cases. To improve procedural efficiency, it mandates designated IP benches within High Courts, modelled on India's Commercial Courts regime.[46]

Compulsory Licensing, Third-Party and Corporate Liability

In an unusual but noteworthy provision, the Bill permits compulsory licensing of trade secrets in situations involving public health emergencies, national security, and essential service disruptions.[47] This clause draws inspiration from the Doha Declaration on TRIPS and Public Health,[48] and offers India a strategic tool in sectors like vaccines, food tech, or disaster response.

The Bill also contemplates secondary liability. Entities that knowingly benefit from trade secret violations, including joint ventures, licensees, or vendors, may be prosecuted or sued alongside the primary violator. This doctrine of "constructive knowledge" is vital to prevent the outsourcing of misappropriation, deter shell-company schemes and bring multinationals under Indian enforcement scope. Further, directors and officers may be held personally liable in case of wilful avoidance or failure to implement safeguards.

Despite its strengths, the Bill raises several concerns, including a lack of a dedicated appellate mechanism or tribunal. The Protection of Trade Secrets Bill, 2024, marks a transformative step in India's journey toward modernising its IP infrastructure. However, successful implementation will depend on institutional readiness, judicial

---

[45] The Protection of Trade Secrets Bill, 2024 under Law Commission of India, 289th Report, S. 2(f).

[46] *Id*., Chapter 4.

[47] *Id*., Section 6.

[48] WORLD TRADE ORGANIZATION, Declaration on the TRIPS agreement and public health, *available at:* https://www.wto.org/english/thewto_e/minist_e/min01_e/mindecl_trips_e.htm (last visited 5th December 2024).

clarity, and harmonisation with existing frameworks such as BNS, 2023. The Bill must not remain a paper tiger; it must be embedded in a broader strategy of legal, administrative, and economic reform.

VI

Judicial Trends

Over the last two decades, Indian courts have played a crucial — albeit inconsistent — role in shaping the protection of trade secrets. In the absence of a specific statutory framework, courts have relied on contractual interpretation, equitable doctrines like breach of confidence, and fiduciary obligations to adjudicate such disputes. While there is recognition of the economic value of confidential information, enforcement has been marred by procedural delays, inconsistent precedent, and an over-reliance on discretionary equitable relief.

One of the earliest and most cited decisions is *Niranjan Shankar Golikari* v. *The Century Spinning & Manufacturing Co. Ltd.*[49] The Supreme Court upheld the enforceability of confidentiality clauses in employment agreements, ruling that restraints protecting proprietary business interests such as know-how and customer lists were valid even post-employment, provided they were reasonable. In *John Richard Brady* v. *Chemical Process Equipments Pvt. Ltd.*,[50] the Delhi High Court granted injunctive relief to prevent the misuse of proprietary information by a former employee. The Court reiterated that technical know-how and processes disclosed in confidence were protectable even in the absence of express patents.

These cases established, *firstly* that trade secrets could be protected under equity and contract law. *Secondly*, that a post-employment obligation to protect confidentiality was not per se in restraint of trade and *lastly*, that Indian courts were willing to act in the absence of specific statutes if proprietary information was at risk.

In *Emergent Genetics India (P) Ltd***. v.** *Shailendra Shivam & Ors.* (2005)[51], the Delhi High Court refused to classify confidential genetic data as "property" under the Indian Penal Code, 1860, holding that mere possession of such data, without unauthorised commercial exploitation, did not amount to criminal misappropriation. This case highlighted the judicial hesitance to extend criminal law to trade secret theft. In a

[49] AIR 1967 SC 1098.
[50] AIR 1987 Delhi 372.
[51] 2005 (7) SCC 228.

recent development, under the *HT Process Controls Case*, [52] the Delhi High Court granted an interim injunction restraining a former employee from using client databases and proprietary software taken during employment. The Court observed:

> *"In the absence of statutory legislation, this Court must rely on equitable principles to protect valuable commercial information. Trade secret theft cannot be allowed to go unpunished merely because it lacks penal teeth under Indian law."*[53]

This case is important for multiple reasons like, it reaffirmed courts' proactive role in protecting digital trade secrets. It also upheld injunctive relief even before the start of full trial proceedings. *Lastly*, it noted the absence of a legislative definition and recommended parliamentary action. However, the court could not award punitive damages or recommend criminal prosecution, once again exposing the limitations of India's current legal regime.

In *Tata Motors Ltd. Case* (2011)[54], the Calcutta High Court dealt with a trade secret claim involving project data and business strategy documents. The Court, however, rejected the plea, stating that the documents lacked sufficient confidentiality and economic distinctiveness to qualify as protectable secrets. This ruling highlighted the subjectivity involved in judicial determination of 'confidentiality'. In contrast, in *American Express Bank Case*[55] (2006), the Delhi High Court granted partial relief to a company whose ex-employee allegedly misused client data. While the Court upheld the general principles of confidentiality, it balanced this against the employee's right to practice her profession, refusing an absolute restraint.

In recent years, Indian courts, especially the Delhi and Bombay High Courts, have adopted procedural innovations from foreign jurisdictions by allowing in camera hearings in sensitive IP disputes. These steps, though promising, remain *ad hoc* and not codified, depending entirely on judicial discretion.

The judiciary has sent strong signals to the legislature, particularly in the 2024 HT Process Controls Case,[56] urging legislative codification. Until that occurs, trade secret holders must navigate fragmented remedies, inconsistent precedents, and slow enforcement, undermining India's aspirations as a global innovation hub.

---

[52] *HT Process Controls Pvt. Ltd. v. Ankur Gupta*, 2024 SCC OnLine Del 1192.
[53] *Ibid.*, Para 34
[54] *Tata Motors Ltd. v. State of Bengal*, 2011 SCC OnLine Cal 1064.
[55] *American Express Bank Ltd. v. Priya Puri*, 2006 (110) DLT 510.
[56] *HT Process Controls Pvt. Ltd. v. Ankur Gupta*, 2024 SCC OnLine Del 1192.

VII

Summary & Conclusion

India stands at a pivotal moment in reshaping its criminal justice system through the Bhartiya Nyaya Sanhita, 2023 (BNS). However, as established in previous sections, the failure to criminalise trade secret misappropriation represents a significant legislative void. Addressing this gap requires multi-layered reforms, legislative, institutional, and procedural, that reflect the needs of a knowledge-based economy while preserving due process and civil liberties.

The most urgent reform is the incorporation of a specific provision in the BNS, 2023, to address trade secret violations, which should include a definition of "trade secret" in harmony with Article 39 of the TRIPS Agreement, focusing on the secrecy, commercial value, and reasonable steps taken to protect the information.[57] It should provide penal sanctions against unauthorised acquisition, disclosure, or use of trade secrets, particularly when committed with dishonest intent, economic motive, or corporate espionage objectives. The law must consider providing corporate criminal liability, especially in organised trade secret theft or collusion by senior executives.

Such a chapter will bring India in line with countries like the United States[58], China[59], and Germany[60], where criminal law has long recognised the gravity of trade secret violations.

Capacity Building for Enforcement Agencies

The government should establish specialised IPR cells within cybercrime or economic offences wings at the state and national levels; train police, prosecutors, and judicial officers in digital forensics, metadata analysis, and non-compete litigation; and foster collaboration between public enforcement bodies and industry associations (e.g., NASSCOM, CII) for technical understanding and real-time cooperation. In this regard, create anonymous whistleblower portals to report internal breaches safely, good of some assistance.

[57] TRIPS Agreement, Article 39, WTO.
[58] Economic Espionage Act, 1996 (U.S.).
[59] Criminal Law of PRC, A. 219.
[60] Unfair Competition Act, Germany, S 17.

These reforms would reduce prosecutorial inertia and improve case-building capacity — both key shortcomings identified in previous Indian case law.[61]

Institutional Reform

India should think about creating a *National Trade Secrets Board (NTSB),* a special expert body set up under the Ministry of Law & Justice or DPIIT. This board can assist in framing contemporary policies, keep records of trade secret misuse cases to study patterns and trends, and help in resolving such matters through arbitration or mediation, and support international cooperation in cases involving trade secret theft across borders.

Conclusion

The protection of trade secrets lies at the intersection of intellectual property, criminal law, digital forensics, and economic policy. In an era where innovation is not just an asset but a national resource, the unauthorised disclosure or theft of confidential business information represents a threat not only to enterprises but also to India's global competitiveness. The *Bharatiya Nyaya Sanhita, 2023,* was a good chance to update India's criminal laws to match the needs of today's digital and modern economy. While BNS includes some modern features like rules for using digital evidence, cybercrime definitions, and faster court procedures, it still does not clearly treat trade secrets as a special kind of property that needs protection. It does not give any direct definition, specific criminal section, or even mention other laws that deal with information protection. Thus, the protection for trade secrets remains weak, unclear, and often not properly enforced.

The United States and the People's Republic of China offer explicit recognition of the fact that they have penal sanctions against trade secrets, with adequate penalties that can bring a better protection system, in tune with economic development. The speed at which information is transmitted, the irreversible loss of exclusivity, and the difficulty of evidence collection demand a deterrence-based response, which only criminal law can adequately provide. As India aspires to lead in artificial intelligence, biotechnology, semiconductor design, and other high-tech domains, it must treat intangible assets with the same gravity as physical assets. Legal systems must evolve in parallel with markets — and the BNS must evolve to criminalise and deter trade secret violations.

[61] *Emergent Genetics India (P) Ltd. v. Shailendra Shivam*, (2005) 11 SCC 245.