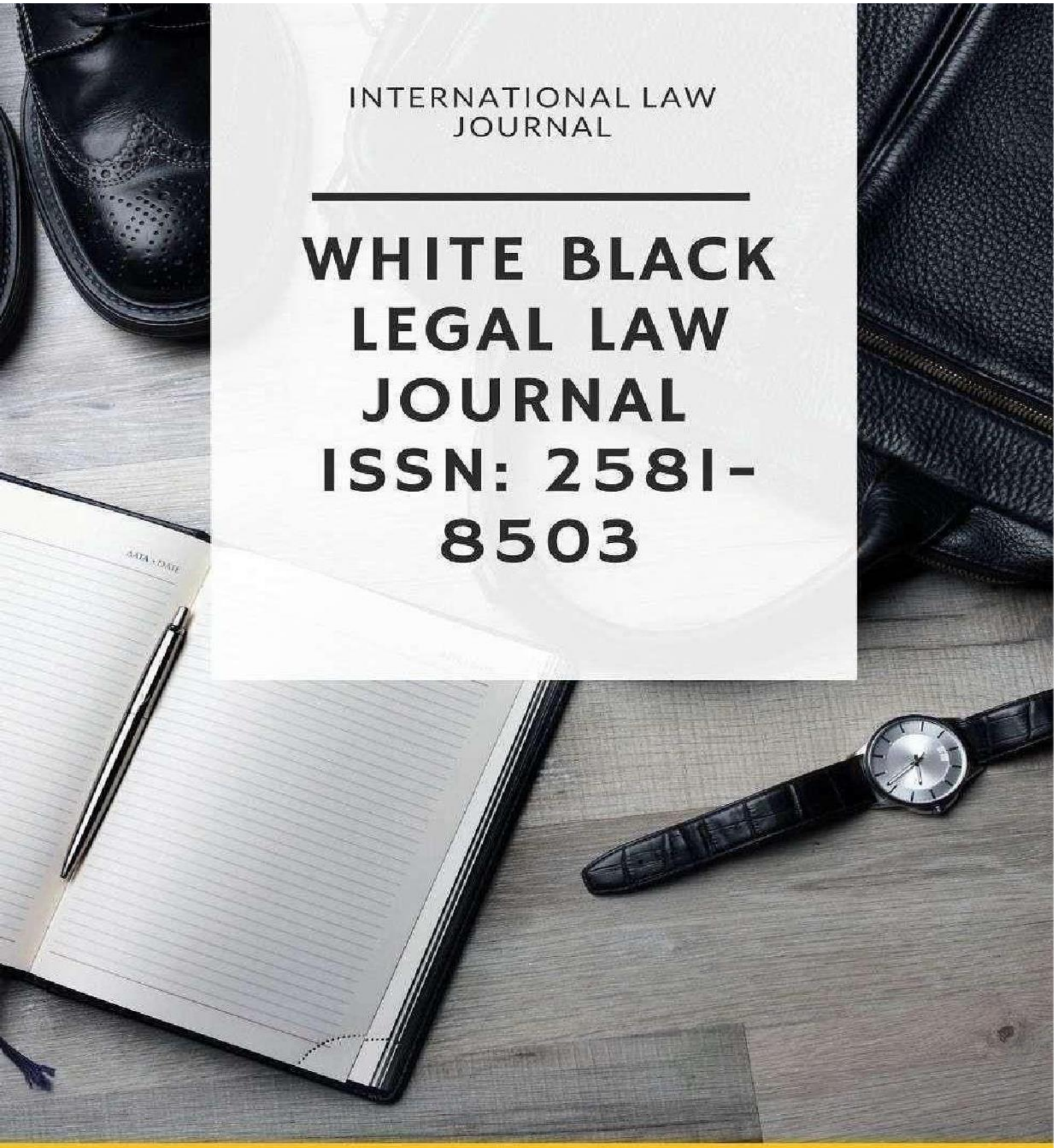


INTERNATIONAL LAW JOURNAL

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

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

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.

WHITE BLACK LEGAL

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.

www.whiteblacklegal.co.in
Volume 4 Issue 2 | Oct 2026 ISSN: 2581-8503

LEGAL PROTECTION OF TRADE SECRETS AGAINST EMPLOYEE MISAPPROPRIATION: A COMPARATIVE STUDY OF CIVIL AND CRIMINAL LIABILITY IN INDIA, THE UNITED STATES AND THE EUROPEAN UNION

AUTHORED BY - AARYA SHARAN
AMITY LAW SCHOOL, AMITY UNIVERSITY PATNA

ABSTRACT

Trade secrets represent a crucial type of commercially valuable information, specially in employment contexts where employees might access sensitive business strategies, technical methods, client databases, and proprietary knowledge. The unauthorized acquisition, utilization, or revelation of such information brings up issues regarding the range of legal protection, the degree of employee responsibilities, and the situations where misappropriation could incur civil or criminal liabilities. This article explores the legal system regulating employee theft of trade secrets by comparing the law operating in India, the United States, and the European Union. Utilizing a doctrinal and comparative approach, it examines pertinent laws, court rulings, international agreements, and legal doctrines regulating the safeguarding of confidential business information. The research examines India's dependence on contractual commitments and legal doctrines, the statutory structure of the United States under the Defend Trade Secrets Act of 2016, and the European Union's unified civil-protection system established by Directive (EU) 2016/943. It also analyses the difference between civil and criminal responsibility and the connection between trade-secret safeguarding and employee movement. The comparative analysis shows that, even though the jurisdictions vary in their legislative frameworks and available remedies, liability relies on the type of information, the context of its acquisition or use, and the legal stipulations pertinent to the specific jurisdiction. The document emphasizes the necessity of differentiating between the improper use of legally safeguarded confidential information and the legitimate utilization of general professional expertise and abilities gained while employed.

Keywords: Confidential Information; Employee Theft; Criminal Responsibility; Breach of Trust; Comparative Jurisprudence; Workforce Mobility.

Introduction

Trade Secrets, in today's knowledge-based economy, represent a significant type of commercially valuable information. They can encompass production methods, technical expertise, research information, programming code, client data, pricing tactics, and strategic plans that offer businesses a competitive edge. In contrast to patents and copyrights, trade secrets gain their commercial value primarily from the secrecy of the information instead of official registration. Therefore, their safeguarding relies on maintaining confidentiality and the legal repercussions linked to the unauthorized obtaining, use, or sharing of such information. Employees play a crucial role in safeguarding trade secrets as their job duties often necessitate access to sensitive business information. The employment relationship therefore includes a significant interaction between an employer's desire to safeguard trade secrets and an employee's capability to apply their professional knowledge, skills, and experience. The legal handling of employee misappropriation should thus be viewed in relation to both trade-secret safeguarding and the rights and duties stemming from employment.

The topic also includes an aspect of criminal law. Depending on the nature of the actions and the relevant legal regulations, the unauthorized acquisition, use, or disclosure of confidential information could lead to consequences that go beyond contractual or civil responsibility. Analysing the connection between these types of liability is crucial for grasping the legal structure regulating employee theft of trade secrets.

The protection of trade secrets has evolved through various legal frameworks in different jurisdictions. These mechanisms consist of contractual confidentiality requirements, civil remedies, legal principles related to confidential information, and legislative measures targeting specific types of illegal activities.

In India, there is no unified, independent statute for the protection of trade secrets. Rather, the applicable legal framework consists of contractual principles, recognized obligations of confidentiality by the judiciary, and other statutory provisions when their conditions are met. The 289th Report of the Law Commission of India, titled Trade Secrets and Economic Espionage (2024), explored the topic and envisioned a specific legislative framework.[1] The United States and the European Union offer valuable comparative perspectives as they tackle trade-secret protection using different legal frameworks. US federal legislation offers civil remedies and criminal offenses for certain types of trade-secret misappropriation, whereas EU Directive 2016/943 lays out a structure for safeguarding trade secrets from illegal

[1] Law Comm'n of India, Trade Secrets and Economic Espionage, Report No. 289 (2024).

acquisition, usage, and disclosure, including rules regarding employee mobility and other safeguarded interests.[2][3]

These various methods offer a framework for analysing how legal frameworks identify safeguarded data, govern worker behaviour, create remedies, and establish the conditions under which criminal responsibility may occur.

The research examines the legal handling of employees misusing trade secrets, emphasizing the link between confidentiality duties, civil remedies, and criminal responsibility. It analyses the pertinent Indian legal system and contrasts it with the methods utilized in the United States and the European Union. The comparative study examines the legal bases for trade-secret protection, the consequences of unauthorized acquisition or sharing, and the consideration of employee interests within each system. It also differentiates trade secrets from general professional knowledge, skills, and experience, acknowledging that the legal safeguarding of confidential information should be viewed within the wider framework of employment and business activities.

The research seeks to:

- Describe the legal notion and key features of trade secrets.
- Analyse the legal principles and remedies related to employee theft of trade secrets according to Indian law.
- Examine the situations where employee misappropriation could lead to criminal responsibility under relevant Indian laws.
- Examine the legal structures regulating trade-secret safeguarding in the United States and the European Union.
- Examine the methods employed by the three jurisdictions regarding confidentiality duties, accessible remedies, criminal accountability, and employee interests.

The research is directed by these inquiries:

1. What are the key traits of a trade secret, and how does it differ from other types of intellectual property?
2. Which legal principles and remedies regulate employee theft of trade secrets in India?
3. In which situations can employee misappropriation lead to criminal liability according to Indian law?

[2] Directive 2016/943, of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

[3] 18 U.S.C. §§ 1831–1839 (2018 & Supp. V 2023); Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended at 18 U.S.C. §§ 1836–1839).

4. In what ways do the United States and the European Union oversee misappropriation of trade secrets and deal with issues concerning employees?
5. What commonalities and distinctions arise from a comparative analysis of the frameworks in India, the US, and the EU?

The study adopts a doctrinal and comparative legal methodology. It examines relevant legislation, judicial decisions, official reports, and legal scholarship concerning trade-secret protection and employee misappropriation in India, the United States, and the European Union. The doctrinal analysis identifies the applicable legal principles and remedies, while the comparative analysis examines the similarities and differences between the selected jurisdictions. The study draws its conclusions from the legal materials examined and does not presuppose the inadequacy of any particular framework.

The research unifies the concepts of trade-secret safeguarding, confidentiality in employment, and criminal responsibility within a comparative legal context. Through the analysis of pertinent laws[4] and their implementation across three jurisdictions, it aims to offer a systematic comprehension of the legal frameworks regulating employee theft of trade secrets. The comparative method also clarifies how various legal systems structure trade-secret safeguards and differentiate between civil remedies and criminal enforcement. The research aims to enhance the scholarly comprehension of the overlap between intellectual property law, employment relations, and criminal law.

Conceptual Framework: Trade Secrets and Employee Misappropriation

Trade secrets represent a type of information that has commercial value, and its economic importance is entirely or partly reliant on its secrecy. This information can encompass production methods, technical designs, formulations, research results, source code, customer databases, pricing strategies, marketing plans, and various business details that grant a company a competitive edge. In contrast to patents, trademarks, and other types of intellectual property that often need registration to secure specific legal rights, trade secrets are usually safeguarded by maintaining confidentiality and the legal implications tied to their unauthorized acquisition, use, or revelation.

Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) offers a globally accepted framework for recognizing trade secrets. Under this provision, information must meet three criteria to be eligible for protection: it must be

[4] Indian Contract Act, No. 9 of 1872, § 27, INDIA CODE (1872)

confidential, have commercial worth due to its confidentiality, and have been subject to reasonable measures to preserve its secrecy by the lawful holder.[5] These criteria help differentiate protectable trade secrets from information that is publicly accessible and information that does not gain commercial value from being confidential. The necessity for confidentiality does not inherently imply that information has to be known solely by one individual or organization. Data can be disclosed to employees, advisors, contractors, or business partners without forfeiting its confidential nature, as long as the conditions and protective measures maintain its confidentiality. In the same way, the need for reasonable actions acknowledges the significance of efforts aimed at avoiding unauthorized access or disclosure. This could consist of confidentiality contracts, limited access to sensitive documents, internal data management protocols, secure storage solutions, and suitable technological protections. The legal nature of a trade secret relies not just on the economic value of the information, but also on its confidentiality, the worth derived from that confidentiality, and the actions implemented to protect it. These characteristics form the conceptual basis for examining the protection of confidential business information across different legal systems.

Employee misappropriation generally relates to the unauthorized or illegal acquisition, utilization, or sharing of qualifying trade-secret information by a person who has access to it through an employment connection. The exact legal interpretation and implications of misappropriation vary based on the relevant law and the context in which the actions take place. Misappropriation can occur while employed or after employment has ended. While employed, an employee may send confidential research information to an unauthorized person, replicate restricted company documents for a wrongful intent, or reveal a protected production method to a rival. After termination, a former employee may keep confidential documents or use safeguarded information acquired from a previous employer for unauthorized business purposes.

Digital technologies have introduced additional aspects to these circumstances. Sensitive data may be stored in digital formats, transmitted over networks, duplicated onto external devices, or accessed from a distance. Consequently, the investigation of purported misappropriation might include access logs, electronic communications, file-transfer records, confidentiality contracts, and other relevant documents or digital evidence. The evidential importance of such

[5] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.

material relies on its genuineness, relevance, and acceptability within the relevant legal context. However, the exchange of information among employees and organizations does not inherently create misappropriation. An employee can reasonably apply general professional expertise, depend on publicly accessible data, or create a comparable method or process on their own. The legal evaluation thus necessitates an examination of whether the information meets the criteria for a trade secret, the conditions under which it was acquired, the character of its later use or sharing, and the presence of any applicable legal duty. It is therefore crucial to differentiate the actual account of employee behaviour from its legal designation. Behaviour that seems detrimental to business may lead to inquiries regarding contractual obligations, civil remedies, statutory breaches, or criminal responsibility, but the relevant legal standards need to be assessed before reaching any conclusions.

The misappropriation by employees can lead to various legal consequences based on the type of behaviour and the relevant legislation. Civil liability typically pertains to the upholding of legal rights and offering remedies to a party whose legally safeguarded interests have been violated. Contingent on the situation and applicable legal standards, these remedies could involve injunctions, compensation, or other suitable relief. Criminal responsibility fulfills a unique legal role. It occurs only when actions align with a relevant criminal offense and the necessary components of that offense are demonstrated. The presence of a confidentiality agreement, the economic importance of the information, or the occurrence of a loss to an employer does not, by itself, prove that a criminal act has taken place. The difference is particularly significant when an employment conflict involves the extent of a confidentiality duty, the categorization of information, or the employee's permission to access or utilize specific materials. The legal ramifications of this behaviour must be assessed by examining the relevant statutory laws, the pertinent facts, and the criteria that apply to the type of liability under consideration.

WHITE BLACK LEGAL

Trade Secret Protection and Employee Misappropriation under Indian Law

In India, trade-secret protection functions through a mix of contractual commitments, legal doctrines related to confidential information, and statutory regulations relevant to specific types of behaviour. In contrast to specific jurisdictions that have implemented specialized trade-secret laws, India lacks a complete, independent statute solely addressing trade secrets. The relevant legal principles should be comprehended by analysing the relationships among current legal sources. A significant global reference is Article 39(2) of the Agreement on Trade-Related

Aspects of Intellectual Property Rights (TRIPS). Members must safeguard undisclosed information that is confidential, has commercial worth due to its secrecy, and has undergone reasonable measures to maintain its confidentiality.[6]

These standards establish a global foundation for recognizing the traits of safeguardable private business information. The 289th Report from the Law Commission of India, titled Trade Secrets and Economic Espionage (2024), analyses the current legal stance in India and explores the need for a specific legislative structure for trade-secret safeguards.[7] This report is part of the wider legal discourse on the management of confidential business information in India. The main sources related to employee misappropriation consist of contractual confidentiality duties, court rulings on breach of confidence, the Indian Contract Act of 1872, and legal statutes that might apply if the actions meet their criteria. The Copyright Act of 1957 and the Information Technology Act of 2000 may also apply in specific situations, depending on the type of information and the actions engaged. These sources fulfill various legal functions. Consequently, their application relies on the specifics of the individual dispute, the nature of the information, the responsibilities regulating its use, and the legal standards of the remedy or offense referenced.

Contractual duties serve as a crucial means of safeguarding confidential information in employment relationships. Employment contracts, confidentiality provisions, and non-disclosure contracts might outline the types of information that employees need to safeguard, the reasons for which the information can be utilized, and the situations where sharing is allowed. These obligations are specially important when employees have access to information about research and development, manufacturing methods, business strategies, pricing agreements, customer relations, or internal commercial activities. The agreement's terms can help clarify the obligations of the parties and whether specific actions exceed the allowed limits of access or usage.

The Indian Contract Act of 1872 establishes the basic structure regulating contractual duties and their implications. Section 73 pertains to compensation for losses or damages resulting from a contract breach, adhering to its legal stipulations.[8] If an employee violates a binding confidentiality obligation, the employer may pursue suitable contractual remedies based on the agreement's terms and the specifics of the breach. However, contractual confidentiality must

[6] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299.
[7] Law Comm'n of India, Trade Secrets and Economic Espionage, Report No. 289 (2024).
[8] Indian Contract Act, No. 9 of 1872, § 73, INDIA CODE (1872).
Id. § 27.

be differentiated from a general limitation on future employment. A confidentiality provision aims to manage the treatment of sensitive information, while a non-compete provision aims to limit designated competitive actions. The two fulfill distinct functions and should be analysed independently. Section 27 of the Indian Contract Act states that an agreement preventing an individual from pursuing a lawful profession, trade, or business is invalid to the extent set by the provision, with consideration of its statutory exception. [4] This is pertinent when contractual terms related to confidentiality include limitations on an employee's future professional endeavours. The legal effect of a contractual clause consequently depends on its substance rather than merely the label attached to it. A provision protecting qualifying confidential information raises different considerations from a provision that prevents an employee from joining a competing enterprise or pursuing a lawful occupation.

Indian courts have addressed conflicts regarding sensitive business information, client databases, company records, and data held or utilized by ex-employees. These rulings offer direction on the situations where confidential information can obtain legal protection and the differentiation between that information and general professional expertise.

In *Beyond Dreams Entertainment versus Zee Entertainment Entreprises (2016)*, [9]the court laid down three conditions for protection: the information must be confidential in nature, it must have been disclosed in circumstances giving rise to an obligation of confidentiality, and the person confidant must have attempted to use or disclose it.

In the case of *John Richard Brady v. Chemical Process Equipments Pvt. Ltd.*,[10] the Delhi High Court examined a conflict regarding sensitive technical data and the utilization of information shared within a business relationship. [5] This ruling is often cited concerning the safeguarding of confidential information by means of confidence principles. The scenario demonstrates the importance of the context in which information is exchanged and the responsibilities linked to its reception. The legal handling of confidential information might therefore go beyond merely determining if the parties have obtained an intellectual property right, based on the relevant principles and circumstances.

In *American Express Bank Ltd. v. Priya Puri*,[11] the Delhi High Court examined a conflict related to customer data, banking connections, and confidentiality duties stemming from employment.[7] This case highlights the difference between information asserted to be confidential and insights or relationships gained through an employee's professional

[9] Beyond Dreams Entm't Pvt. Ltd v. Zee Entm't Ltd.,2015 SCC OnLine Bom 4223 (India)
[10] John Richard Brady v. Chemical Process Equipments Pvt. Ltd., 1987 SCC OnLine Del 248
[11] American Express Bank Ltd. v. Priya Puri, 2006 SCC OnLine Del 638

endeavours.

The ruling highlights the necessity of scrutinizing the particular facts in contention instead of assuming that every client detail or business connection is inherently confidential. The legal examination should consider the nature of the information, its availability, and the grounds on which confidentiality is claimed.

In *Burlington Home Shopping versus Rajnish Chibber (1995),*[12] the Delhi High Court determined that a trade secret refers to information whose release to a rival would result in genuine or considerable damage to its proprietor. This was similarly affirmed in Linde v Kerr [1991] 1 All ER 418. Protection therefore goes beyond confidential production formulas to, in relevant situations, the identities of clients and the products they purchase.

In *Ambiance India versus Naveen Jain (2005),*[13] The court determined that routine workplace issues familiar to many and generally recognized by others do not qualify as trade secrets. It acknowledged that workers in a company face numerous issues while performing their responsibilities, yet not all are private or detrimental to the employer if revealed. Knowledge of business practices or methods of customer engagement acquired on the job also do not qualify as a trade secret.

In *Navigators Logistics versus Kashif Qureshi (2018),*[14] the Delhi High Court determined that information an employee acquires during their employment without extraordinary effort cannot be classified as a trade secret or confidential information. Simply being aware of such information cannot be classified as a trade secret.

Collectively, these rulings indicate that conflicts regarding employee theft can raise issues related to confidentiality, the type of information, contractual agreements, intellectual property rights, and procedural obligations. The legal importance relies on the particular issues addressed and the factual circumstances of each case.

Civil remedies provide a means of addressing alleged misuse of confidential information and protecting legally recognised commercial interests. The remedies available in a particular case depend on the legal basis of the claim, the applicable statutory provisions, and the evidence presented.

Injunctions

A request for an injunction can be made to stop the unauthorized use or release of confidential information. Depending on the situation, a claimant might request temporary relief during the

[12] Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, 1995 SCC OnLine Del (India)
[13] Ambiance India Pvt. Ltd. V. Naveen Jain, 2005 SCC OnLine Del 367 (India)
[14] Navigators Logistics Ltd. V. Kashif Qureshi, 2018 SCC OnLine Del 11321 (India)

process or a definitive injunction after the decision. The provision of injunctive relief is regulated by the relevant procedural and substantive rules. The claimant needs to demonstrate the applicable legal grounds for relief, and the court evaluates the case's specifics when determining if an injunction is suitable.

Damages and Compensation

If a violation of a binding contractual duty is proven, compensation might be obtainable under Section 73 of the Indian Contract Act, 1872, depending on its criteria related to loss or damage arising from the breach.[15] The evaluation of compensation relies on the type of claim and the evidence backing the reported loss. In conflicts concerning confidential business data, pertinent factors might encompass the business repercussions of the unauthorized use or revelation and the damages legally linked to the behavior.

Restoration of Data and Other Suitable Remedies

Based on the situation and the relief allowed by law, a claimant might ask for the return of documents, the provision of materials, or orders preventing the ongoing use or release of confidential information. Conflicts concerning electronic records might also necessitate the investigation of devices, access logs, and additional pertinent evidence as per applicable procedural law. The shape and extent of relief are determined by the type of information, the legal grounds of the claim, and the authority of the court. Consequently, these remedies ought to be evaluated concerning the specific cause of action instead of being presumed to be applicable in the same manner across all trade-secret conflicts.

The legal consequences of employee misappropriation are not confined to civil and contractual remedies. Certain conduct may also fall within the scope of an existing criminal offence where the relevant statutory requirements are satisfied. India does not, however, treat every breach of confidentiality as a standalone criminal offence merely because commercially valuable information is involved.

The applicable provisions must be examined according to the nature of the conduct, the character of the information or property involved, the required mental element, and any other statutory conditions.

Criminal Breach of Trust under section 316 of Bhartiya Nyaya Sanhita 2023

Section 316 of the Bharatiya Nyaya Sanhita, 2023 (BNS), deals with criminal breach of trust. It pertains to situations where an individual given responsibility for property, or having control over it, deceitfully misuses or converts it for personal gain, or improperly utilizes or disposes

[15] Indian Contract Act, No. 9 of 1872, § 73, INDIA CODE (1872).

of it contrary to the relevant legal guidelines or contract that regulates the trust.[16] In a workplace setting, this clause might be applicable when the circumstances meet the criteria for entrustment or control over property and deceitful misappropriation or utilization. Its use in a specific conflict concerning confidential information necessitates thorough examination of the legal definition of property and the additional components of the offense. The presence of a confidentiality agreement or the unauthorized release of information does not, on its own, constitute a criminal breach of trust. The legal obligations must be fulfilled based on the circumstances of the case.

Theft and other- property related Offences under Bhartiya Nyaya Sanhita 2023

Section 303 of the BNS characterizes theft as the dishonest removal of movable property from someone else's possession without permission.[17] The applicability of this provision to specific actions involving electronic information hinges on the characteristics of the material and the statutory criteria. The reproduction or transfer of digital data should not be automatically considered as stealing. The legal categorization relies on the actions and the components of the offense in question. Additional offenses may also be pertinent if their specific criteria are fulfilled, but their enforcement must be demonstrated independently instead of being assumed solely from a claim of trade-secret theft.

Cheating under Bhartiya Nyaya Sanhita 2023

Section 318 of the BNS pertains to cheating, encompassing actions that involve deception and the subsequent inducement outlined in the provision.[18] In an employment dispute, its applicability would rely on whether the circumstances demonstrate the necessary deception, inducement, and other legal components. In the same way, additional criminal regulations might be relevant if the behaviour separately fits within their range. The suitable analysis thus starts with the claimed actions and then assesses if the components of a specific crime are fulfilled.

Electronic information is crucial in contemporary trade-secret conflicts. Workers might obtain confidential details via workplace computers, databases, email accounts, cloud services, or other digital systems. Accusations might involve unauthorized access, duplication, downloading, transmission, modification, or revelation of digital records. The Information Technology Act, 2000, includes clauses that might pertain to specific types of online misconduct. Section 43 deals with particular actions related to computer systems or

[16] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 316, INDIA CODE (2023).
[17] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 303, INDIA CODE (2023).Id. § 303.
[18] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 318, INDIA CODE (2023).Id. § 303.Id. § 318.

networks, such as unauthorized access, data downloading, copying, or extraction, provided that the legal conditions are met.[19] Section 66 outlines criminal penalties if an action mentioned in Section 43 is performed dishonestly or fraudulently, as outlined in the Act.[20]

These regulations may be applicable when reported employee behaviour pertains to unauthorized actions involving computer systems or data. The use of their application relies on the particular legal components and the conditions of access and utilization. Access granted for employment purposes raises different factual issues compared to access or copying that surpasses the applicable authority. Section 72A of the Information Technology Act pertains to the revelation of information that violates a lawful contract by an individual, including intermediaries, who gains access to personal information while rendering services under the terms outlined in the provision.[21] Its enforcement is contingent on the legal parameters of the information and the context of the disclosure. It must not be regarded as a broad criminal rule that applies to all disclosures of commercial trade secrets. Electronic evidence can also be significant in legal or criminal cases. Relevant documents might consist of access logs, emails, file transfer logs, forensic reports, and various electronic records. The applicable law of evidence and procedure dictates the evidentiary handling of such material.

Confidential information might, in some situations, coincide with content safeguarded by different intellectual property regulations. For instance, original content found in software, technical documents, or other works might be eligible for copyright protection if the relevant legal criteria are met.

The Copyright Act of 1957 safeguards eligible original creations under its provisions.[22]Nonetheless, the presence of confidential information does not by itself confirm copyright violation. The claimant needs to specify the pertinent protected work and demonstrate the criteria for the relevant copyright claim. This difference is demonstrated through conflicts related to customer databases and business documentation. Depending on the type of compilation and the evidence, a database may pose issues related to confidentiality and copyright that necessitate independent legal evaluation. A request for safeguarding confidential information should thus be differentiated from a request based on the violation of copyright or any other legal intellectual property right.

The legal system in India that regulates employee theft of trade secrets relies on contractual

[19] Information Technology Act, No. 21 of 2000, § 43, INDIA CODE (2000).
[20] Information Technology Act, No. 21 of 2000, § 66, INDIA CODE (2000).
[21] Information Technology Act, No. 21 of 2000, § 72A, INDIA CODE (2000).
[22] Copyright Act, No. 14 of 1957, §§ 13, 14, INDIA CODE (1957).

duties, judicial standards related to confidential data, civil remedies, and legal rules pertinent to specific behaviours.

Contract law establishes a framework for analysing confidentiality duties and compensation for eligible violations. Court rulings provide insight into handling confidential data, client databases, employee expertise, and limitations after employment. The BNS and the Information Technology Act could be pertinent if the claimed behaviour meets the criteria of a relevant offense. Additional intellectual property laws may be relevant if the subject matter qualifies for protection on its own.

Consequently, the legal categorization of employee behaviour relies on the information at stake, the context of its collection or utilization, the governing obligations, and the stipulations of the specific remedy or offense applied. This structure lays the groundwork for the comparative analysis of the United States and the European Union in the upcoming sections.

Comparative Study of trade Secret Protection: United States, European Union and India

The United States of America

The United States safeguards trade secrets via federal laws, state statutes, and contractual agreements. The main federal law is the Defend Trade Secrets Act of 2016 (DTSA), found in Chapter 90 of Title 18 of the United States Code. It offers civil remedies and particular criminal offenses regarding the misappropriation of trade secrets.[23]

According to 18 U.S.C. § 1839(3), information is deemed a trade secret when its owner implements reasonable steps to maintain its confidentiality, and this information gains independent economic value from not being widely known or easily obtainable through lawful means. Section 1839(5) defines misappropriation to encompass certain unauthorized acquisition, usage, or disclosure under situations involving improper methods or obligations of confidentiality.[24]

Section 1836(b) allows for civil litigation and gives courts the authority, under specific legal conditions, to issue:

- Orders to prevent real or anticipated misappropriation.
- Compensation for real losses and eligible unjust enrichment.

[23] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2, 130 Stat. 376, 376–77 (codified as amended at 18 U.S.C. § 1839(3) (2024)).
[24] 18 U.S.C. § 1836(b) (2024).

- Fair royalties in suitable situations.
- Punitive damages for intentional and harmful appropriation
- Legal fees in designated situations.
- Civil confiscation in exceptional situations, dependent on procedural protections.

The DTSA restricts injunctions that impact employment. An employee cannot be barred from starting a new job solely because they possess certain information; limitations must comply with legal standards and relevant state regulations. The United States explicitly makes certain types of trade-secret theft illegal through two main provisions:

Section 1831—Economic espionage: Relates to particular actions concerning trade secrets where the defendant acts with the intent or knowledge that the crime will advantage a foreign nation, foreign entity, or foreign representative.

Section 1832—Theft of trade secrets: Pertains to particular actions relating to trade secrets, necessitating the intent to gain economic advantage for a party other than the owner and the necessary intent or awareness regarding harm to the owner, adhering to the mandated commerce statute.[25]

The offenses possess unique components. A violation of a confidentiality agreement by an employee alone does not create criminal liability.

In *PepsiCo, Inc. v. Redmond*, the Seventh Circuit upheld an injunction in a dispute involving a former employee who had access to confidential marketing and strategic plans and accepted employment with a competitor. The decision is associated with the doctrine of inevitable disclosure, under which threatened misuse may be inferred from the circumstances. Its application is not uniform across the United States, and it does not create a general prohibition on employees joining competitors.[26]

European Union

The main EU tool is Directive (EU) 2016/943, which standardises key elements of civil protection against the illegal obtaining, usage, and sharing of trade secrets. It does not create a consistent criminal offense across the EU for trade-secret misappropriation.[27]

Article 2(1) outlines a trade secret based on three criteria: the information must remain confidential, possess commercial worth due to its confidentiality, and be protected by adequate

[25] 18 U.S.C. §§ 1831–1832 (2024).
[26] PepsiCo, Inc. v. Redmond, 54 F.3d 1262, 1268–72 (7th Cir. 1995).
[27] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) Against Their Unlawful Acquisition, Use and Disclosure, 2016 O.J. (L 157) 1.

measures to maintain its secrecy.[28]

Article 3 acknowledges valid acquisition via independent discovery or creation, specific methods of observation or reverse engineering, and other activities that align with fair commercial practices. Article 4 outlines the illegal acquisition, utilization, and disclosure of information, which includes unauthorized duplication of documents or electronic files, as well as violations of confidentiality or contractual obligations that restrict usage. These regulations apply when an employee duplicates, shares, or reveals protected information without permission. The legitimate obtainment of general professional knowledge and skills differs from the theft of a trade secret.[29]

Articles 10–15 stipulate provisional measures, injunctions, corrective actions, damages, and protections related to confidentiality in the course of proceedings. The existence and execution of these remedies rely on the Directive and the relevant national legislation. Article 1(3) clearly maintains employee mobility. The Directive does not limit employees' use of information that is not classified as a trade secret or of abilities and knowledge legitimately gained during their regular job duties. Article 5 outlines particular protected situations, such as specific disclosures aimed at exposing misconduct for the public good. Directive 2016/943 mainly aligns civil protection measures. [30]

The applicability of criminal liability for trade-secret misappropriation is contingent upon the criminal law of the pertinent EU Member State. Consequently, it is crucial not to consider the Directive as establishing a uniform criminal offence applicable across the EU.

India, the United States, and the European Union acknowledge the significance of safeguarding commercially valuable confidential data, yet they implement varying legal methods for trade-secret protection. In India, protection mainly stems from contractual confidentiality duties, judicial rules related to breach of confidence, and legal regulations relevant to specific types of behaviour. India lacks a thorough independent trade-secret law. Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) serves as a key international guideline for recognizing protectable confidential information, whereas the 289th Report of the Law Commission of India, titled Trade Secrets and Economic Espionage (2024), explores the

[28] Directive (EU) 2016/943, art. 2(1)
[29] Directive (EU) 2016/943, art. 3., Directive (EU) 2016/943, art. 4
[30] Directive (EU) 2016/943, arts. 10–15, Directive (EU) 2016/943, arts. 1(1), 10–15. The Directive harmonises civil-law measures; criminal liability is principally addressed under the laws of individual Member States., Directive (EU) 2016/943, art. 1(3). Directive (EU) 2016/943, art. 5.

legal stance in India.[31]

The United States possesses a clear federal legal structure established by the Defend Trade Secrets Act of 2016 (DTSA), supported by state trade-secret regulations and contractual requirements. The DTSA outlines what constitutes trade secrets and misappropriation, offering civil remedies such as injunctions, damages, and reasonable royalties when suitable. It further delineates particular criminal offenses under 18 U.S.C. §§ 1831 and 1832, concerning economic espionage and the misappropriation of trade secrets, respectively. Criminal responsibility still relies on demonstrating the specific statutory elements of the offense; simply violating a confidentiality agreement is not enough.[32]

The European Union adopts an alternative legislative strategy via Directive (EU) 2016/943, which standardises key elements of civil protection against the illegal acquisition, use, and sharing of trade secrets. The Directive outlines provisional measures, injunctive relief, corrective actions, and compensations, while primarily assigning criminal liability to the legislation of individual Member States. Article 1(3) clearly maintains employee mobility and specifies that the Directive does not limit employees' ability to utilize information that isn't a trade secret or to apply experience and skills genuinely gained during regular employment.

The jurisdictions vary in how they handle employee mobility and the connection between confidentiality and future jobs. In India, obligations of confidentiality need to be differentiated from lawful employment restrictions, which includes the significance of Section 27 of the Indian Contract Act of 1872.[33] In the United States, the DTSA restricts employment injunctions solely based on a person's knowledge and mandates adherence to relevant state laws. In the European Union, the mobility of employees is explicitly acknowledged in Article 1(3) of Directive 2016/943. In all three jurisdictions, the difference between protected confidential information and an employee's overall professional knowledge and expertise is still significant.

The main comparative difference relates to the legal methods by which protection and liability are determined. India depends on a mix of contract law, judicial principles, and relevant statutory provisions; the United States has a clear federal framework for civil remedies and particular criminal offenses; and the European Union standardizes civil protections while allowing Member States to mainly handle criminal liability. Therefore, employee

[31] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2), Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299; Law Comm'n of India, Trade Secrets and Economic Espionage, Report No. 289 (2024).

[32] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified as amended at 18 U.S.C. §§ 1831–1839 (2024)); 18 U.S.C. § 1836(b) (2024).

[33] Indian Contract Act, 1872, § 27; 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2024); Directive (EU) 2016/943, art. 1(3).

misappropriation should be evaluated by considering the type of information, the context of its acquisition or usage, the employee's obligations, and the stipulations of the specific civil remedy or criminal offense cited.[34]

The comparative analysis shows that the protection of trade secrets is mainly influenced by the characteristics of the information, its economic worth, the context of its acquisition or utilization, and the actions taken to maintain its confidentiality. Article 39(2) of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) establishes a crucial international benchmark by mandating that information remain confidential, have commercial value due to its secrecy, and be protected by reasonable measures to uphold its confidentiality. These standards are evident in the legal structure of the United States and the Trade Secrets Directive of the European Union. In India, protection is primarily established through contractual agreements, the law on breach of trust, and relevant legal regulations. The research also suggests that not all types of business information are considered trade secrets. Data that is accessible to the public, widely recognized in the pertinent sector, or simply a component of a worker's usual professional background does not inherently qualify for trade-secret safeguards. Customer databases, technical schematics, business plans, and production methods may be eligible if the relevant legal criteria are met. Their safeguarding relies on the specifics of each situation instead of merely the employer designating them as confidential.

Findings and Discussion

The safeguarding of trade secrets relies on the confidentiality, market value, and appropriate security measures for the information. These standards are represented in TRIPS Article 39(2), US legislation, and the EU Trade Secrets Directive. In India, safety mainly originates from contractual duties, legal doctrines, and relevant statutory laws. Data like customer records, technical methods, and business plans can be eligible for protection, but common professional expertise and information accessible to the public do not inherently qualify as trade secrets. Civil liability can emerge from the unauthorized obtaining, utilizing, or revealing of confidential information and may lead to injunctions or compensation. Criminal responsibility, however, necessitates evidence of the components of a particular crime. The Defend Trade Secrets Act clearly establishes civil remedies and designated criminal offenses within the United States. The EU Directive mainly standardizes civil protection, whereas criminal liability

[34] Agreement on Trade-Related Aspects of Intellectual Property Rights art. 39(2); Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1831–1839 (2024); Directive (EU) 2016/943, arts. 2–5, 10–15.

is mainly regulated by the laws of Member States. In India, relevant criminal laws can be applied only when their legal criteria are met. A violation of confidentiality by itself does not inherently create criminal responsibility. Trade-secret protection should be differentiated from limitations on an employee's overall knowledge, competencies, and professional abilities. In India, obligations of confidentiality need to be evaluated in conjunction with Section 27 of the Indian Contract Act, 1872. Federal law in the United States limits job restrictions that rely solely on the knowledge an employee possesses, whereas Article 1(3) of the EU Trade Secrets Directive acknowledges employee movement. Consequently, the legal evaluation relies on the type of information, the actions of the employee, and the relevant legal criteria.

The three jurisdictions vary in their legal structures. India depends mainly on contractual agreements, legal principles, and relevant laws. The United States offers a clear federal structure for civil remedies and designated criminal offenses, in addition to state legislation. The European Union aligns key elements of civil protection via Directive 2016/943. Regardless of these differences, all three systems acknowledge the significance of safeguarding commercially valuable confidential information while differentiating between protected information and legitimate professional knowledge. Employee misappropriation can entail the unauthorized duplication, sharing, or relocation of sensitive information. Nonetheless, this behaviour does not inherently qualify as a criminal act. In India, laws related to theft, breach of trust, fraud, or computer-related offenses can be enforced if their legal components are proven. In the United States, liability for a crime under 18 U.S.C. §§ 1831–1832 is contingent upon demonstrating the pertinent offense. The relevant national criminal law in the European Union needs to be analysed. Consequently, criminal liability relies on the actions, the necessary mental state, and the evidence, instead of simply on the presence of a confidentiality agreement.

Conclusion

Trade secrets play a crucial role in safeguarding commercially valuable information, especially in employment scenarios where employees could access technical expertise, business plans, customer records, and other confidential data. This study analyzed the legal structures regulating employee theft of trade secrets in India, the United States, and the European Union, focusing specifically on the difference between civil liability and criminal liability. The comparative study reveals that the three jurisdictions safeguard confidential commercial information via distinct legal methods. India mainly depends on contractual confidentiality requirements, legal principles related to breach of confidence, and relevant statutory laws. The

United States offers a more clearly defined federal structure via the Defend Trade Secrets Act of 2016, which outlines civil remedies and distinct criminal offenses associated with trade-secret theft. The European Union, via Directive (EU) 2016/943, standardizes key elements of civil protection while primarily assigning criminal responsibility to the legislation of each Member State. Regardless of these differences, the level of protection in each jurisdiction relies on the type of information, the context of its acquisition or usage, and the relevant legal stipulations.

The research also indicates that violating a confidentiality duty and committing a criminal offense are separate legal issues. While unauthorized obtaining, sharing, or utilizing of sensitive information can lead to civil lawsuits, establishing criminal responsibility necessitates demonstrating the essential elements of a relevant crime. In India, for example, laws regarding criminal breach of trust, theft, fraud, or particular computer-related activities may be relevant if their legal criteria are met. Likewise, the federal criminal laws of the United States necessitate evidence of the actions and mental aspects defined by statute.

The framework of the European Union should be viewed in conjunction with the applicable national criminal laws. Consequently, employee misappropriation should not be regarded as a uniform type of behaviour that results in the same legal outcomes in different jurisdictions. Another important discovery relates to the connection between trade-secret safeguarding and workforce movement. An employer's concern for safeguarding confidential information should be differentiated from the effort to manage an employee's overall knowledge, expertise, and professional abilities. This difference is evident in court rulings in India, limitations on employment injunctions according to United States federal law, and the explicit acknowledgment of employee mobility under Article 1(3) of Directive (EU) 2016/943. The legal evaluation thus necessitates consideration of the confidential nature of the information as well as the type of behaviour exhibited by the employee. To sum up, the comparative analysis shows that the legal ramifications of employee misappropriation hinge on the interplay between confidentiality duties, the legal classification of the information, accessible civil remedies, and the stipulations of criminal law. Although India, the United States, and the European Union have different legislative frameworks and methods, each mandate that the pertinent facts be evaluated according to its own legal system. Grasping these differences offers a more precise explanation of how trade-secret safeguards function within employment relationships and how civil and criminal liability are established under the respective legal systems.