confidential information and trade secrets; however, if a trade secret or any confidential information is disclosed breaching the non-disclosure agreements/contracts or confidentiality agreements, primarily, civil remedies for the breach of contract will be available for the aggrieved party.[199] Other notable civil remedies may include injunction, damages and accounts of profits.

### *L. South Korea*

4.78. In South Korea, trade secrets are governed by the Unfair Competition Prevention and Trade Secret Protection Act[200], which is a comprehensive piece of legislation dealing with all the necessary aspects of trade secrets. Additionally, if a trade secret is in the form of an 'industrial technology' under the Act on Prevention of Divulgence and Protection of Industrial Technology[201], then it is also protected by this legislation.

4.79. The Unfair Competition Prevention and Trade Secret Protection Act defines a 'trade secret' as technical or managerial information useful in business activities, such as production or marketing methods, which is not publicly known, which holds and economic value, and is actively kept as a secret.[202] It is pertinent to note that through an amendment to the Act in the year 2019, the requirement for reasonable efforts to maintain secrecy was removed. Hence, the current Act stipulates that as long as the secrecy is maintained, the requirement of being a trade secret is considered fulfilled

---

[199] *Ibid.*
[200] Unfair Competition Prevention and Trade Secret Protection Act of Korea, *available at*: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62546&lang=ENG.
[201] South Korean Act on Prevention of Divulgence and Protection of Industrial Technology, *available at*: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=24351&lang=ENG.
[202] Unfair Competition Prevention and Trade Secret Protection Act, art. 2(2).

regardless of the effort put into maintaining it. The only essentials are the information being secret and having an economic value.

4.80. The said Act provides the remedies for the infringement of trade secrets and prohibits acts of acquisition and use or disclosure of trade secrets. Article 2(3) of the Act[203] defines 'infringement of trade secrets' and stipulates different acts and practices which may constitute infringement. It covers the following aspects:

> *"(a) An act of acquiring trade secrets by theft, deception, coercion, or other improper means, or subsequently using or disclosing the trade secrets improperly acquired (including informing any specific person of the trade secret while under a duty to maintain secrecy;*
> *(b) An act of acquiring trade secrets or using or disclosing the trade secrets improperly acquired, with knowledge of the fact that an act of improper acquisition of the trade secrets has occurred or without such knowledge due to gross negligence;*
> *(c) An act of using or disclosing trade secrets after acquiring them, with knowledge of the fact that an act of improper acquisition of the trade secrets has occurred or without such knowledge due to gross negligence;*
> *(d) An act of using or disclosing trade secrets to obtain improper benefits or to cause damage to the owner of the trade secrets while under a contractual or other duty to maintain secrecy of the trade secrets;*
> *(e) An act of acquiring trade secrets, or using or disclosing them with the knowledge of the fact that they have been disclosed in the manner prescribed in item (d) or that such disclosure has been involved, or without such knowledge, due to gross negligence;*
> *(f) An act of using or disclosing trade secrets after acquiring them, with the knowledge of the fact that they have been disclosed in a manner prescribed in item (d) or that such disclosure has been involved, or without such knowledge due to gross negligence."*

[203] *Id.*, art. 2(3).

4.81. Hence, a trade secret owner in South Korea will have to prove that the alleged trade secret infringement falls under one of the above stated categories to establish the case.

4.82. In South Korea, a trade secret owner can avail both civil and criminal remedies against the infringement of trade secret. The Unfair Competition Prevention and Trade Secret Protection Act provides for various civil remedies in terms of prohibition of trade secret, liability of damages for infringement of trade secret and restoration of reputation etc.[204] However, this Act focuses more on criminal penalty for trade secret misappropriation. Misappropriating a trade secret is a violation of the Act and can result in a penalty of up to 10 years of imprisonment or a fine of up to KRW 500 million. Provided, if the pecuniary gain from such an action exceeds 10 times KRW 500 million, the fine will be at least 2-10 times the amount gained. Moreover, if the trade secret is used abroad or disclosed to a third party with the knowledge that it will be used abroad, the penalty is more severe, resulting in a maximum penalty of 15 years of imprisonment or a fine of up to KRW 1.5 billion.[205] Apart from the Unfair Competition Prevention and Trade Secret Protection Act, stringent criminal punishments are provided for misappropriation of industrial technology under the amended Industrial Technology Act.

4.83. Thus, the Unfair Competition Prevention and Trade Secret Protection Act is the basic comprehensive law dealing with trade secrets and its infringement. Under the Act, joint ownership of the information is possible and the owner can grant a license to use its trade secret. The only embargo

[204] *Id.* arts. 10, 11, 12, 13, 14.
[205] *Id.* art. 18.

upon the licensee is to keep the trade secret as confidential under the confidentiality agreement and maintain its secrecy.

### *M. Spain*

4.84. In Spain, protection of trade secrets is dealt primarily under the Spanish Trade Secrets Act[206], which gave effect to the Trade Secrets Directive[207] passed by the European Union. The Spanish Criminal Code[208] also includes criminal penalties in case of unlawful acquisition or disclosure of trade secrets.

4.85. The Spanish Trade Secrets Act defines a trade secret[209] as:

> *"An information or knowledge (including technological, scientific, industrial, commercial, organizational or financial information or knowledge), which meets the following conditions:*
> *a. it is secret in the sense that it is not, as a body or in the configuration and precise composition, generally known to persons within the circles in which this type of information or knowledge is normally dealt with, or is accessible;*
> *b. it has commercial value, real or potential, because it is secret; and*
> *c. it has been subject to reasonable steps, by the holder of the trade secret, to keep it secret."*

4.86. The Spanish Trade Secrets Act includes the regulation of trade secrets as a property right. It makes trade secrets transferable and licensable.[210] If an individual sell or licenses a trade secret for a fee and it is later determined that they lacked proper ownership or rights to do so, they will be held

---

[206] The Spanish Trade Secrets Act, 2019 (Act 1 of 2019).
[207] EU Directive 2016/943.
[208] The Criminal Code of Spain, 1995 (Act 10 of 1995).
[209] *Id.*, art. 1(1).
[210] *Id.*, art. 4.

responsible for any resulting damages, unless the agreement specifies otherwise. If the seller or licensor acted with dishonest intentions, they will be held accountable for the damages regardless.[211]

4.87. Under this Act, a trade secret can have multiple owners, and in such instances, the arrangement will be governed by the agreement made by the involved parties.[212] If there is no such agreement, the arrangement will be governed by the provisions of the Spanish Trade Secrets Act. According to these provisions, any co-owner has the right to:

a. Commercially exploit the trade secret (with prior notification to the other co-owners).

b. Take necessary measures to maintain the secrecy of the trade secret.

c. Pursue civil and criminal actions to defend the trade secret, though notifying the other co-owners is necessary so they can participate in the action.[213]

4.88. As per the Spanish Trade Secrets Act, trade secrets can be violated by their unauthorized acquisition, use, or disclosure.[214]

4.89. 'Unlawful acquisition' of a trade secret, without the consent of the trade secret holder, can occur through:

a. Unauthorized access to, appropriation of, or copying of any documents, objects, materials, substances, electronic files, or other mediums containing the trade secret or from which the trade secret can be inferred.

---

[211] *Id.*, art. 7.
[212] *Id.*, art. 5(1).
[213] *Id.*, art. 5(2).
[214] *Id.*, art. 1(2).

b. Any other behavior that, given the circumstances, is deemed to be against fair commercial practices.[215]

4.90. Similarly, the use or disclosure of a trade secret will be deemed unlawful whenever it is done without the consent of the trade secret holder by a person who unlawfully obtained the trade secret, or violates a confidentiality agreement or any other obligation to keep the trade secret undisclosed, or breaches a contractual or other obligation to restrict the use of the trade secret.[216] Furthermore, the acquisition, use or disclosure of a trade secret will also be deemed unlawful if, at the time of such actions, a person knew or should have known, given the circumstances, that the trade secret had been acquired directly or indirectly from another individual who was unlawfully using or disclosing the trade secret.[217]

4.91. Actions for violation of trade secrets under the Spanish law include the declaration of the trade secret infringement, cessation or prohibition of acts infringing trade secrets, prohibition of manufacture, commercialization, sale or use of infringing goods, or the import, export or storage of infringing goods for those purposes, or withdrawal, which consists of delivery of the documents, objects, materials, substances, electronic files and any other medium containing the trade secret and, when appropriate, their total or partial destruction. Remedies also include claim for compensation for damages in case of willful intent or negligence by the person infringing trade secrets.[218]

---

[215] *Id.*, art. 3(1).
[216] *Id.*, art. 3(2).
[217] *Id.*, art. 3(3).
[218] *Id.*, art. 9.

4.92. When determining compensation for damages, all relevant factors will be taken into account, such as economic damages, including loss of profits, suffered by the owner of the trade secret, unjust enrichment obtained by the infringer and, where appropriate, others elements that are not of an economic nature, such as the moral damage caused to the owner of the business secret due to its illegal obtaining, use or disclosure.[219]

4.93. This Act also allows competent judicial authorities to take specific measures, either on their own initiative or upon an application by a third party, to safeguard the confidentiality of trade secrets. These measures include the following (though any suitable and proportionate measure may be requested):

a. Limiting access to any document, object, material, substance, electronic file, or other medium containing trade secrets or alleged trade secrets to a restricted number of individuals.

b. Restricting access to hearings where trade secrets or alleged trade secrets may be revealed, and limiting the distribution of the corresponding record or transcript of those hearings to a restricted number of individuals.

c. Providing a non-confidential version of any judicial decision to any person other than those included in the limited number of individuals mentioned above, with the sections containing trade secrets removed or redacted.[220]

4.94. With regard to protection of whistleblowers, Spain has also given effect to the European Union's Directive on whistleblower protection[221] by enacting

[219] *Id.*, art. 10.
[220] *Id.*, art. 15.
[221] EU Directive 2019/1937.

the Whistleblower Protection Act[222] which aims to protect persons who report regulatory breaches and combat corruption.

### *N. Sweden*

4.95. Being the global leader in design and innovation, trade secrets serve as a cornerstone for Sweden's innovative and competitive economy. Legal protection to trade secrets and intellectual property fosters transparency and collaboration of businesses. Legislations on other Intellectual property rights in Sweden are based on European Union directives and regulations; however, trade secrets in Sweden are protected by a dedicated law.

4.96. In Sweden, trade secrets are primarily governed by the Act on Trade Secrets (2018:558)[223], which replaced the old Act of 1990[224] after the European Union Directive.[225] The new Act on trade secrets is a result of the initiative by European Union to strengthen the protection of trade secrets which implies disclosure of trade secrets is unlawful and anyone who infringes the trade secret would be liable to pay damages. It also included negligence as a constitutive element for acquiring trade secrets and the unlawful use of the same.

4.97. As per new Swedish law on trade secrets, any information of business or its operating conditions, whose disclosure cause damages to the owner of business in terms of market competition, is called a trade secret.[226] The

---

[222] The Whistleblower Protection Act of Spain, 2023 (Act 2 of 2023).
[223] Swedish Act on Trade Secrets (2018:558).
[224] Swedish Act on the Protection of Trade Secrets (1990:409).
[225] 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.
[226] Swedish Act on Trade Secrets (2018:558).

owner of trade secrets is required to take reasonable measures to maintain the confidentiality of information through confidentiality agreements or non-disclosure agreements.[227] However, if an employee acquires any skill or experience during the course of one employment, then he shall not be restricted to practice the same in another employment.

4.98. The new Act of 2018 consists of 28 sections. This Act is applicable where the trade secret is misappropriated, wherein a person takes the access of trade secret, appropriate it for some use and disclose the same but this Act is not applicable to whistleblowing for illegal activity. As per Section 27 of the Trade Secrets Act, unlawful dealing of trade secret is also punishable with an imprisonment of up to four years.

4.99. In case of infringement of trade secret, owner can seek remedies such as injunctions and damages. As per Section 5 of Chapter 10 of the Swedish Criminal Code, criminal penalties for breach of trust can be imposed for misappropriation of trade secrets.[228] The new Act also provides punishment of imprisonment for two years or fine for the crime of economic/corporate espionage, whereby someone intentionally and unlawfully obtains access to a trade secret and if such a crime is of severe nature, then the Act provides an imprisonment of minimum six months and maximum upto six years.[229] Moreover, the Act also stipulates punishment for unlawful dealing in a trade secret, whereby a person intentionally acquires a trade secret despite knowing that the provider of such information has obtained the access through corporate espionage. Thus, the Swedish law on trade secrets provides sufficient remedies for infringement of trade secrets.

---

[227] *Ibid.*
[228] Swedish Criminal Code (*brottsbalken*, SFS 1962:700), Ch. 10, s. 5.
[229] Swedish Act on Trade Secrets (2018:558), s. 26.

### *O. Taiwan*

4.100. The Trade Secrets Act of Taiwan, promulgated on 17th January 1996[230], acts as the basic legal framework to protect trade secrets in Taiwan. Initially the Act provided civil liability to the trade secret owners for misappropriation of their trade secret and remedy in the form of damages. However, as the instances of international economic/corporate espionage and theft of corporate trade secrets grew manifold, Taiwan amended the Trade Secrets Act in the year 2013 and criminalized the theft of trade secrets by introducing criminal liability and fines for the offenders. Thus, the existing Trade Secrets Act of Taiwan contains both civil and criminal liability for better protection of the trade secrets in their country.

4.101. As per the Trade Secrets Act, a 'trade secret'[231] means any method, technique, process, formula, program, design or other information used in the course of production, sales, or operations and that meets all of the following requirements:

i. It is not generally known to persons in the relevant industry.
ii. It has economic value, actual or potential, due to its secretive nature.
iii. Its owner has taken reasonable measures to maintain its secrecy.

Therefore, the Act provides a comprehensive definition of 'trade secret' and focuses on the aspects of secrecy, economic value and reasonable steps taken by the owner to protect the undisclosed information.

---

[230] Laws & Regulations Database of the Republic of China (Taiwan), *available at:* https://law.moj.gov.tw/ENG/LawClass/LawHistory.aspx?pcode=J0080028 .

[231] Trade Secrets Act of Taiwan, art. 2, *available at:* https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=J0080028.

4.102. Under the Act, the trade secret can be protected for an indefinite time period provided that the information remains confidential and all the essential requirements are met. Article 3, 4 and 5 of the Act provides for the ownership right and lays down different instances where the secret information may belong to different people. The Act also provides for a provision of joint ownership and rights and liabilities associated with such ownership.[232] A trade secret may be assigned in whole or in part, or it may be jointly owned. Any use or disposition of a jointly-owned trade secret shall be unanimously approved by all co-owners in the absence of a contractual provision. Apart from assigning, the owner of a trade secret can also grant a license to another person for the use of the trade secret, whose terms are governed by the contract.[233] Given that licensing arrangements may potentially expose trade secrets to disclosure or misuse, trade secret proprietors can implement the following safeguards when issuing licenses:

i. Incorporate confidentiality provisions within the licensing agreement, obligating the licensee to safeguard the trade secret.

ii. Limit the license to individuals who have a demonstrable need-to-know, restricting access solely to those requiring the information for authorized purposes.

iii. Require the licensee to uphold adequate security measures.

iv. Retain the authority for the trade secret proprietor to monitor the licensee's utilization of the trade secret and conduct periodic audits to verify adherence to the terms of the agreement.[234]

---

[232] *Id.*, arts. 3, 4, 5.

[233] *Id.*, arts. 6, 7, 8.

[234] Chambers and Partners, "Trade Secrets for Taiwan" (2023) *available at:* https://practiceguides.chambers.com/practice-guides/trade-secrets-2023/taiwan#:~:text=The%20Trade%20Secrets%20Act%20(TSA,secrets%20for%20their%20own%20gain. (last visited on February 26, 2024).

4.103. The Act specifically defines misappropriation of trade secrets and what acts constitute misappropriation. Acts such as acquiring a trade secret by improper means; acquiring, using, or disclosing a trade secret knowingly or unknowingly due to gross negligence; using or disclosing an acquired trade secret knowing, or not knowing due to gross negligence; using or disclosing by improper means a legally acquired trade secret; or using or disclosing without due cause a trade secret to which the law imposes a duty to maintain secrecy, falls under the category of misappropriation of trade secret.[235]

4.104. Taiwan has both civil and criminal remedies for misappropriation of trade secret and all the remedies are specifically stipulated under the Trade Secrets Act of Taiwan. For civil remedy, a trade secret owner can request for removal of misappropriation and destruction of products generated from the misappropriation or any instrument used for such misappropriation.[236] Similarly, the owner can claim for damages, can recover the cost as well as profits and also request for injunction under the law.[237] Apart from civil remedies, the Act also stipulates specific criminal remedies, whereby if any person obtains any illicit gain or inflict any loss to the actual owner of the trade secret, then such a person can be sentenced to a maximum of 5 years imprisonment or any short-term imprisonment, and a fine between NT$1 million and NT$10 million can be imposed.[238] Thus, the Trade Secrets Act of Taiwan in itself is efficacious in providing protection to trade secret owners.

---

[235] Trade Secrets Act of Taiwan, art. 10.
[236] *Id*, art. 11.
[237] *Id*, arts. 12, 13.
[238] *Id*, art. 13-1.

### *P. United Arab Emirates (UAE)*

4.105. For enhancing transparency and harmonious business environment, protection of trade secrets become imperative for a country like UAE which is expanding its business network. Intellectual property rights are governed majorly by Copyright Law[239], Regulation & Protection of Industrial Property Rights[240], Trademark Law[241], whereas commercial contracts are governed by Commercial Transactions Law[242], Commercial Companies Law[243], Civil Code[244]. Commercial Contracts which are concluded electronically will be subjected to Cyber Crime Law[245], Electronic Transactions Law[246]. Some exclusive distribution agreements and agency agreements are governed by the Agency Law[247].

4.106. UAE does not have a separate dedicated legal framework for the protection of trade secrets. Instead, protection comes from a patchwork of different regulations across various federal laws. Trade secrets are given protection under the Penal Code[248] as well as the Civil Code[249] and Labour Law[250] of UAE.

4.107. Article 905(5) of the Civil Code imposes a duty on the employees to not to reveal the trade secret of the employer even after the expiry of employment

---

[239] Federal Decree-Law No. 38 of 2021.
[240] Federal Law No. 11 of 2021.
[241] Federal Decree-Law No. 36 of 2021.
[242] Federal Decree-Law No. 50 of 2022.
[243] Federal Decree-Law No. 32 of 2021.
[244] Federal Law No. 5 of 1985.
[245] Federal Decree-Law No. 34 of 2021 and Federal Decree-Law No. 45 of 2021.
[246] Federal Decree-Law No. 46 of 2021.
[247] Federal Law No. 3 of 2022.
[248] Federal Law No. 3 of 1987.
[249] Federal Law No. 5 of 1985.
[250] Federal Decree-Law No. 33 of 2021.

period. Those who breach the duty is liable to pay compensation to the party/parties whose information has been disclosed against the contract.[251]

4.108. As per Article 354 of Commercial Companies Law, anyone who discloses a company's secrets is punishable by imprisonment or fine.[252] It also provides grounds for the dissolution of company that engage in unfair competition using trade secrets.

4.109. Penal provisions of UAE also criminalize industrial espionage and unauthorized access to trade secrets. It penalizes the use and disclosure of trade secrets for personal gain and makes a person liable to pay penalty not less than AED 20,000 and imprisonment for not less than one year.[253]

4.110. Labour Law also provides for the dismissal of an employee from the company in which they are working, in case of any disclosure of any secrets of the company.[254] Article 127 of the Labour Law also provides a restrictive covenant along with liquidated damages for the benefit of employer to protect confidential information wherein an employee can be restricted to work for the company in direct competition with former employer company within a specified location, having similar nature of business for a specific period of time.[255] It is pertinent to note that there is no time limit mentioned as to the existence of confidentiality of any information, which means any information can remain trade secret till the time it is open for public access.

---

[251] Federal Law No. 5 of 1985, art. 905(5).
[252] Federal Decree-Law No. 32 of 2021, art. 354.
[253] Federal Law No. 3 of 1987, art. 379.
[254] Federal Decree-Law No. 33 of 2021, art. 120.
[255] *Id*, art. 127.

### *Q. United Kingdom*

4.111. In the United Kingdom, the classification of trade secrets as 'property', remains uncertain and it is widely believed that trade secrets do not fall under the category of property. Nevertheless, safeguarding trade secrets can occur through various avenues, such as, breach of contract claims when a non-disclosure agreement is present or implied, other confidentiality obligations, common-law actions for breach of confidence, or statutory measures for protecting trade secrets.[256]

4.112. A common law claim for breach of confidence relies on the premise that when information is received in confidence, one cannot take unfair advantage of that information or prejudice the individual who entrusted the information. This principle is upheld in both Scotland and England.[257]

4.113. For information to meet the criteria, it must possess the "necessary quality of confidence" and be "disclosed in circumstances importing an obligation of confidence", such as those stipulated by a contract, inferred from the context of disclosure, or inherent in the relationship between the parties, such as that of employer and employee.[258] Nevertheless, especially in employer/employee dynamics, there are constraints on the extent to which information can be safeguarded post-termination of the relationship. Specifically, the information must maintain a sufficiently high level of

---

[256] DLA Piper, "DLA Piper's Guide to Going Global – Intellectual Property and Technology- United Kingdom" 9 (February 9, 2023), *available at*: file:///C:/Users/UNDER%20SECRETARY/Downloads/DLA-Piper-Guide-to-Going-Global-IPT-United-Kingdom.pdf (last visited on February 20, 2024).

[257] Scottish Law Commission No. 90, *Breach of Confidence* 49 (December, 1984), *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scotlawcom.gov.uk/files/5712/8015/1448/26-07-2010_1437_886.pdf (last visited on February 20, 2024).

[258] DLA Piper, "DLA Piper's Guide to Going Global – Intellectual Property and Technology- United Kingdom" 11 (February 9, 2023), *available at*: file:///C:/Users/UNDER%20SECRETARY/Downloads/DLA-Piper-Guide-to-Going-Global-IPT-United-Kingdom.pdf (last visited on February 20, 2024).

confidentiality, with exceptionally sensitive trade secrets potentially being safeguarded indefinitely.[259]

4.114. Confidential information and trade secrets receive protection under both common law and equity, although Scottish law doesn't acknowledge the notion of equity. With the Trade Secrets (Enforcement, etc.) Regulations 2018 in the UK, there's a considerable overlap, as these regulations now also safeguard trade secrets.[260]

4.115. These Regulations define a 'trade secret'[261] as information that:

a. Is secret (i.e., is not generally known or readily accessible to persons within circles that deal with such information);
b. Has commercial value as it is secret; and
c. Has been subjected to reasonable steps by the person in control to keep it a secret.

4.116. The interpretation of "reasonable steps" will evolve through court applications of this law. Simply labelling something as a trade secret is unlikely to suffice on its own.[262]

4.117. The Regulations prohibit the unauthorized acquisition, use, or disclosure of trade secrets, including unauthorized access. "Unlawful" denotes actions that are unauthorized or contrary to honest commercial practices.[263]

---

[259] Tom Scourfield, Joel Vertes, "Trade Secret Laws and Regulations in the UK CMS Law", (2022) *available at*: https://cms.law/en/int/expert-guides/cms-expert-guide-to-trade-secrets/united-kingdom (last visited on February 20, 2024).

[260] Scottish Law Commission No. 90, *Breach of Confidence* 5 (1984), *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scotlawcom.gov.uk/files/5712/8015/1448/26-07-2010_1437_886.pdf (last visited on Feb 20, 2024).

[261] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (2018 No. 597), s. 2.

[262] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (2018 No. 597), s. 2.

[263] Tanya Aplin and Richard Arnold, "UK Implementation of the Trade Secrets Directive" *J. Schvosbo, T. Minssen and T. Riis (Eds), the Harmonisation and Protection of Trade Secrets in the EU – an Appraisal of the EU Directive* 65-85 (2020), *available at*: http://dx.doi.org/10.2139/ssrn.3393593 (last visited on February 20, 2024).

4.118. The Regulations also affirm that trade secrets are infringed upon through their unauthorized acquisition, use, or disclosure. Given that only one of these actions is necessary for infringement, it's conceivable for infringement to occur even if a trade secret was lawfully acquired but later used or disclosed unlawfully.[264]

4.119. Furthermore, in accordance with UK law, damages aim to reimburse for incurred losses. The Regulations specify that financial compensation should not exceed the royalties or fees that would have been payable if the individual had acquired a license to utilize the trade secret in question, for the duration during which the use of the trade secret could have been restricted.[265]

4.120. UK courts are proficient and accustomed to employing various measures to uphold confidentiality during court proceedings. These measures may include closed hearings, declarations designating specific evidence as confidential, and restricting access to information through "confidentiality clubs."[266]

4.121. The Regulations explicitly mandate that trade secrets maintain confidentiality both during and after legal proceedings. They prohibit anyone involved in trade secret proceedings (including parties, lawyers, experts, and court officials) from utilizing or disclosing the trade secret or

---

[264] "Trade Secrets: An International Perspective on Their Protection and Tips to Mitigate Disclosure Risk" *K&L Gates* (2022), *available at*: https://www.klgates.com/Trade-Secrets-An-International-Perspective-on-Their-Protection-and-Tips-to-Mitigate-Disclosure-Risk-12-19-2022 (last visited on February 20, 2024).
[265] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (2018 No. 597), s. 16(2).
[266] Herbert Smith Freehills, "UK: Definition and Protection of Trade Secrets and Undisclosed Know-How to Be Harmonised Across Europe" (2014), *available at*: https://hsfnotes.com/employment/2014/01/10/uk-definition-and-protection-of-trade-secrets-and-undisclosed-know-how-to-be-harmonised-across-europe/ (last visited on February 20, 2024).

any information claimed to be a trade secret.[267] Additionally, the Regulations authorize the court to limit access to a document or hearing and to redact its judgment.[268]

### *R. United States of America*

4.122. Trade secrets, which encompass various types of confidential information, are widely recognized as valuable assets for both U.S. businesses and the overall economy.[269] Examples range from search engine algorithms to soft drink recipes. Laws safeguarding trade secrets have been implemented by Congress and state legislatures. Federal and State courts consistently handle numerous trade secrets cases, with over a thousand filings annually in U.S. district courts in recent years.[270]

4.123. The safeguarding of trade secrets involves a blend of state and federal regulations, which outline a range of civil and criminal penalties for the "misappropriation" of trade secrets, defined as "the improper acquisition, disclosure, or use of a trade secret."[271]

4.124. While traditionally safeguarded primarily by state regulations, trade secrets have increasingly fallen under the purview of federal civil and criminal statutes. During the 117th Congress, legislators introduced multiple bills pertaining to trade secrets, predominantly aimed at mitigating the perceived threat of trade secret theft by foreign governments and agents.

---

[267] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (2018 No. 597), s. 10(1).
[268] The Trade Secrets (Enforcement, Etc.) Regulations 2018 (2018 No. 597), s. 10(5).
[269] Suzana Nashkova, "Defining Trade Secrets in the United States: Past and Present Challenges – a Way Forward?" 54 *IIC* 634-672 (2023).
[270] Research GUIDES, "Trade Secret Laws", *available at*: https://law.gwu.libguides.com/tradesecrets/primary#s-lg-box-20480258 (last visited on February 19, 2024).
[271] Legal Information Institute, Cornell Law School, "Trade Secret", *available at*: https://www.law.cornell.edu/wex/trade_secret (last visited on February 19, 2024).

This focused discussion presents an outline of how trade secrets are defined and safeguarded within the framework of U.S. legislation. Additionally, it explores specific bills introduced during the 117th Congress pertaining to this subject matter.[272]

4.125. Protection of trade secrets in the United States of America is broadly covered under the following legislations:

a. Uniform Trade Secrets Act of 1985
b. Economic Espionage Act of 1996
c. Defend Trade Secrets Act of 2016

**i. State Laws**

4.126. State statutes typically grant trade secret holders the ability to initiate legal action and secure compensation or injunctive measures in cases of trade secret misappropriation. In the majority of states, along with the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, civil litigation related to trade secrets is regulated by the Uniform Trade Secrets Act (UTSA), an Act initially published in 1979 and subsequently enacted, albeit with certain modifications, on a state-by-state basis. The only exceptions to the adoption of UTSA are North Carolina, which has implemented a comparable statute, and New York, where claims of trade secret misappropriation are regulated by common law principles. While state courts typically hold jurisdiction over UTSA claims, plaintiffs have the option to file specific UTSA lawsuits in U.S. district courts.[273]

---

[272] Congressional Research Service, "An Introduction to Trade Secrets Law in the United States" 1 (2018), *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sgp.fas.org/crs/secrecy/IF12315.pdf (last visited on February 19, 2024).

[273] Sharon K. Sandeen and Christopher B. Seaman, "Toward a Federal Jurisprudence of Trade Secret Law," 32 *Berkeley Technology Law Journal* 829-914 (2017).

### ii. Defend Trade Secrets Acts

4.127. In 2016, Congress enacted the Defend Trade Secrets Act (DTSA), establishing a fresh civil remedy for cases of trade secret misappropriation within the scope of federal law. DTSA does not supplant state statutes like UTSA; instead, it introduces a complementary avenue for plaintiffs to bring forth trade secret misappropriation lawsuits in federal court if "the trade secret is related to a product or service used in interstate or foreign commerce."[274]

4.128. It is argued that DTSA has enhanced safeguards for trade secret proprietors by facilitating simpler access to federal courts and permitting expedited seizure of assets in certain situations to recover pilfered trade secrets but some critics also argue that DTSA largely duplicates UTSA and has not succeeded in achieving nationwide consistency in trade secrets legislation. For example, federal courts have exhibited inconsistency regarding whether DTSA empowers them to prohibit employees from accepting new roles that could potentially lead to the "inevitable disclosure" of their previous employers' trade secrets, highlighting a divergence in states' laws.[275]

---

[274] House of Representatives Report 114–529, "Defend Trade Secrets Act of 2016" 6, *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.congress.gov/114/crpt/hrpt529/CRPT-114hrpt529.pdf (February 19, 2024).

[275] House of Representatives Report 114–529, "Defend Trade Secrets Act of 2016" 12, *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.congress.gov/114/crpt/hrpt529/CRPT-114hrpt529.pdf (February 19, 2024). The Committee notes that courts interpreting State trade secret laws have reached different conclusions on the applicability of the inevitable disclosure doctrine. Compare *PepsiCo, Inc.* v. *Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995) (''A plaintiff may prove a claim of trade secret misappropriation by demonstrating that the defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets''), with *Whyte* v. *Schlage Lock Co*., 125 Cal. Rptr. 2d 277, 281 (Ct. App. 2002) (rejecting explicitly the inevitable disclosure doctrine under California law).

4.129. A possible distinction between DTSA and UTSA lies in their respective extents of extraterritorial jurisdiction (i.e., applicability to conduct outside the United States).[276]

4.130. A bill introduced during the 117th Congress, named the Protect American Trade Secrets Act of 2021 (H.R. 4327), had the potential to broaden the extraterritorial jurisdiction of DTSA by enshrining that DTSA "shall apply to conduct occurring outside the United States and impacting United States commerce."[277]

### iii. Section 337 of the Tariff Act of 1930

4.131. Apart from pursuing legal action in state and federal courts, owners of trade secrets have the option to file specific misappropriation claims with the U.S. International Trade Commission (ITC) under Section 337 of the Tariff Act of 1930.[278]

4.132. The ITC has the authority to issue injunctions halting the importation of products detrimental to U.S. industries, especially those manufactured using unlawfully obtained trade secrets. This relief can be mandated by the ITC even if the misappropriation occurs beyond the borders of the United States.[279]

---

[276] Fisher Phillips, "A Key Difference Between the DTSA and UTSA: "Continued Misappropriation" Continues to be a Viable Claim" *Lexology*, April 3, 2017, *available at*: https://www.lexology.com/library/detail.aspx?g=9bb141e2-4366-498b-8ffd-51bdb801cc3e (last visited on February 19, 2024).

[277] Protect American Trade Secrets Act of 2021 (H.R.4327), *available at*: https://www.congress.gov/bill/117th-congress/house-bill/4327/text?r=7&s=1 (last visited on February 19, 2024).

[278] Panel Report L/6439-36S/345, "United States - Section 337 of the Tariff Act of 1930" 4 (January 16, 1989), *available at*: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wto.org/english/tratop_e/dispu_e/gatt_e/87tar337.pdf (last visited on February 19, 2024).

[279] Congressional Research Service RL34292, "Intellectual Property Rights and International Trade" (2020), *available at*: chrome-

4.133. During the 117th Congress, a proposed legislation known as the Secrets Act of 2021 (S. 2067)[280] aimed to establish a distinct mechanism permitting the ITC to scrutinize and prevent the importation of goods manufactured using trade secrets unlawfully acquired "by a foreign agent or foreign instrumentality" for reasons of national security.

### iv. Economic Espionage Act

4.134. The Economic Espionage Act of 1996 (EEA) criminalized the unlawful acquisition of trade secrets, whether for foreign espionage or commercial motives, under federal law. According to this legislation, economic espionage involves unlawfully obtaining a trade secret with the intention to serve the interests of any foreign government, entity, or agent. Convictions under this offense could result in substantial fines imposed on both individuals and entities, as well as potential prison terms of up to 15 years. Commercial theft, as defined by this statute, involves the unlawful acquisition of a trade secret with the intent to harm its owner. Offenders may face penalties including fines and imprisonment for up to 10 years.[281]

4.135. Unfortunately, the EEA has failed to prevent trade secret theft and foreign economic espionage. While the Computer Crime and Intellectual Property Section of the United States Department of Justice has performed admirably, the strain on governmental resources is overwhelming. In the absence of a federal civil cause of action, American companies lack sufficient means to

---

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://crsreports.congress.gov/product/pdf/RL/RL34292 (last visited on February 19, 2024).

[280] Secrets Act of 2021 (S. 2067), *available at*: https://www.congress.gov/bill/117th-congress/senate-bill/2067#:~:text=This%20bill%20expands%20the%20authority,a%20foreign%20agent%20or%20instrumentality. (last visited on February 19, 2024).

[281] U.S. Department of Justice, Criminal Resource Manual 1000-1499, "1122. Introduction to the Economic Espionage Act" (2015), *available at*: https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act (last visited on February 19, 2024).

safeguard their trade secret assets in today's global economy, which transcends international borders.[282]

### v. Considerations for Congress

4.136. The 117th Congress deliberated on various bills related to trade secrets, including those mentioned earlier (H.R. 4327 and S. 2067).[283] These bills primarily tackled the perceived risk of misappropriation by individuals outside the United States. One such proposal as introduced was the Combating Chinese Purloining (CCP) of Trade Secrets Act (S. 1245)[284], which focused on increasing relevant criminal penalties, imposes visa and immigration-related restrictions, and sets out other provisions to deter espionage, theft of trade secrets, and improper interference with U.S. elections by foreign persons, with a particular focus on China.

4.137. Several bills proposed during the 117th Congress aimed to institute penalties, such as immigration constraints, against individuals who are not U.S. citizens and engage in trade secret theft. The CCP Act[285] and the Stop Theft of Intellectual Property Act of 2021 (S. 1409)[286] would have classified individuals who contravene the Economic Espionage Act (EEA) and

---

[282] R. Mark Halligan, *Protecting U.S. Trade Secret Assets in the 21st Century*, 6:1 Landslide (September/October 2013), *available at:* https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2013-14/september-october-2013/ (last visited on February 19, 2024).

[283] Protect American Trade Secrets Act of 2021 (H.R.4327), *available at*: https://www.congress.gov/bill/117th-congress/house-bill/4327/text?r=7&s=1 (last visited on February 19, 2024); Secrets Act of 2021 (S. 2067), *available at*: https://www.congress.gov/bill/117th-congress/senate-bill/2067#:~:text=This%20bill%20expands%20the%20authority,a%20foreign%20agent%20or%20instrumentality. (last visited on February 19, 2024).

[284] CCP Trade Secrets Act (S. 1245), *available at*: https://www.congress.gov/bill/117th-congress/senate-bill/1245 (last visited on February 19, 2024).

[285] CCP Trade Secrets Act (S. 1245), *available at*: https://www.congress.gov/bill/117th-congress/senate-bill/1245 (last visited on February 19, 2024).

[286] Stop Theft of Intellectual Property Act of 2021 (S.1409), *available at*: https://www.congress.gov/bill/117th-congress/senate-bill/1409/all-info#:~:text=Introduced%20in%20Senate%20(04%2F28%2F2021),-Stop%20Theft%20of&text=This%20bill%20makes%20the%20misappropriation,entry%20into%20the%20United%20States (last visited on February 19, 2024).

specific other statutes as inadmissible and subject to deportation under U.S. immigration regulations. Likewise, the Protecting American Intellectual Property Act of 2022 (S. 1294)[287] aimed to prohibit or rescind entry visas for individuals determined by the President to have knowingly participated in, profited from, or assisted in trade secret theft deemed "a significant threat to the national security, foreign policy, or economic well-being or financial stability of the United States."

### *S. Yemen*

4.138. The applicable legislation in Yemen is the Patents, Utility Models, Integrated Circuit Layouts and Undisclosed Information Act, 2011.

4.139. Chapter 4 of the Act deals with undisclosed information. Article 29, 30, 31 and 32 define the contours of what information is protected. The general provision of mandatory licenses is not applicable to undisclosed information and only applies to patents, utility models and IC layouts.[288] There is a general penal provision imposing fine up to 500,000 Rial on any one violating provisions of the Act including those pertaining to Undisclosed Information.[289]

4.140. In addition to this penalty, holder of such undisclosed information can file a case demanding compensation for an offence under the Act, including those relating to undisclosed information.[290]

---

[287] Protecting American Intellectual Property Act of 2022 (S. 1294), *available at:* https://www.congress.gov/bill/117th-congress/senate-bill/1294#:~:text=This%20bill%20imposes%20sanctions%20on,a%20U.S.%20individual%20or%20entity (last visited on February 19, 2024).

[288] Act relating to Patents, Utility Models, Layout Designs of Integrated Circuits and Undisclosed Information, 2011 (Yemen), art. 33.

[289] *Id.* art. 37.

[290] *Id.* art. 38.

### *T. European Union*

4.141. The EU Trade Secrets Directive 2016/9431,[291] (hereinafter "EU Directive") was adopted on June 8, 2016 and came into force on July 5, 2016. While the EU Directive came in the year 2016, its idea was first mooted in 2013 with an initial proposal followed by second proposal in 2014[292] and a compromise text in 2015[293]. The EU Directive required Member States to implement its provisions by transposition into their domestic legal framework latest by June 9, 2018. The EU Directive serves as a broad framework within which members states are required to provide national laws on the subject matter. This directive aims to standardize aspects of substantive and procedural laws concerning trade secrets across EU Member States. Articles 2 to 5 outline definitions such as 'trade secret', 'trade secret holder', 'infringer', and 'infringing goods', and also clarify what is lawful and unlawful acquisition, use, and disclosure of trade secrets, along with exceptions. Further, Articles 6 to 15, constituting the majority of the directive, address measures, procedures, and remedies against unauthorized acquisition, use, or disclosure of trade secrets.

4.142. The EU Directive adopts conceptual ambivalence on the aspect of trade secret protection being aligned with intellectual property rights or unfair competition law.[294] In defining what amounts to lawful and unlawful acquisition, use and disclosure of trade secrets in Articles 3 and 4

---

[291] Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *available at*: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0943&rid=4.

[292] Bianca Fox, "Tripping Over the EU Trade Secret Directive: "Reasonable Steps" to Get Back on Track" 19 *Chi.-Kent J. Intell. Prop.* 67 (2020), *available at*: https://scholarship.kentlaw.iit.edu/ckjip/vol19/iss1/11 (last visited on February 14, 2024).

[293] Davide Arcidiacono, "The Trade Secrets Directive in the International Legal Framework" 1 *European Papers* 1073 (2016), *available at*: https://www.europeanpapers.eu/en/europeanforum/trade-secrets-directive-international-legal-framework (last visited on February 14, 2024).

[294] Tanya Aplin, "The Limits of Trade Secret Protection in the EU" in Sharon K. Sandeen, Christoph Rademacher *et.al.* (eds.), *Research Handbook on Information Law and Governance* 175 (Edward Elgar Publishing, 2021).

respectively, reference has been made to "honest commercial practices" which shows that the EU Directive exhibits a clear tilt towards the realm of unfair competition rather than an intellectual property like conception. This is further evident from recital 2 of the Directive which describes protection of trade secrets as 'a complement or as an alternative to intellectual property rights. This is in line with the conceptual understanding on the nature of trade secrets/confidential information that has emerged in Europe over time. An overwhelming majority of EU member states protect trade secrets under the regime of unfair competition combined with criminal sanction.[295] They generally do not treat trade secrets as either property or intellectual property.[296]

4.143. The EU Directives are instructive on certain procedural aspects. While members are free to adopt their own rules on limitation, the maximum duration of limitation period has been prescribed as 6 years.[297] Article 9 imposes an obligation to maintain confidentiality with respect to trade secret or confidential information that parties become aware of on account of participation in proceedings. Further, this confidentiality requirement remains in force even after such legal proceedings have terminated. The Article addresses other aspects pertaining to confidentiality of proceedings, restricting access to documents submitted before the court and making available non-confidential version of any judicial decision.

4.144. Certain other notable aspects include usage of the word "trade secret holder" instead of "owner"[298] and that Article 1 itself permits that

---

[295] Tanya Aplin, "Right to Property and Trade Secrets" in C Geiger (ed.), 421 *Research Handbook on Human Rights and Intellectual Property* (Edward Elgar, 2015), *available at*: https://ssrn.com/abstract=2620999 (last visited on February 14, 2024).
[296] *Id.*
[297] Directive (EU) 2016/943, art. 8.
[298] Directive (EU) 2016/943, art. 2(2).

member states may provide more far-reaching protection so far as there is compliance with specified Articles of the EU Directive that exhibits a minimum harmonization approach[299]. Further, recital 5 acknowledges the binding nature of the TRIPS Agreement on EU member states. Accordingly, the definition of trade secret in Article 2(1) has been lifted from Article 39.2 of the TRIPS Agreement. Furthermore, Article 6(1) obligates Member States establish measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets. Thus, under the EU Directive, no criminal liability or sanctions have been mandated. Another notable aspect that ties in with the minimum harmonization approach reflected in Article 1 is that while the EU Directive seeks to harmonize the law, such endeavour is only partial as certain key issues like employee and ex-employee liability remain unregulated. [300]

[299] Davide Arcidiacono, "The Trade Secrets Directive in the International Legal Framework" 1 *European Papers* 1073 (2016), *available at*: https://www.europeanpapers.eu/en/europeanforum/trade-secrets-directive-international-legal-framework (last visited on February 14, 2024).

[300] Tanya Aplin, "The Limits of Trade Secret Protection in the EU" in Sharon K. Sandeen, Christoph Rademacher *et.al.* (eds.), *Research Handbook on Information Law and Governance* 175 (Edward Elgar Publishing, 2021).

## 5. TRADE SECRETS: PREVAILING LEGAL POSITION IN INDIA

### *A. Applicable Laws*

5.1. India is a signatory to the TRIPS Agreement and thus has an obligation to protect "undisclosed information". However, Article 39 of the TRIPS Agreement does not mandate any particular framework to be adopted to ensure adequate protection. Only a minimum criterion specifying the kind of information that ought to be protected and against what sort of practices the protection has to be ensured have been mentioned. Thus, India did not adopt any specific legislation as in the case of other intellectual property rights that fall within the ambit of the TRIPS Agreement and continues to provide protection under common law and contract law, as was the position prior to the adoption of the TRIPS Agreement in 1994.

5.2. In India, there is no singular law addressing the issue of misappropriation of trade secrets. There is a patch-work of remedies/laws available to the holder of trade secrets to vindicate its rights in protecting such information. In such a scenario, protection that has been extended to trade secrets is largely judge-made law.[301] It is perhaps owing to the case-law driven nature of trade secret protection that introduces inconsistency and uncertainty in law. Courts over the years have protected trade secrets on basis of principles of equity, and at times, upon a common law action of breach of confidence, which is in effect amounts to a breach of contractual obligation.[302] Thus, as it stands now, trade secrets are protected under principles equity, common law action of breach of confidence and

---

[301] Chandni Raina, Working Paper - Trade Secret Protection in India: The Policy Debate, Centre for WTO Studies 9 (September, 2015), *available at:* https://wtocentre.iift.ac.in/workingpaper/Trade%20Secret%20Protection%20in%20India-%20The%20policy%20debate.pdf (last visited on January 18, 2024).

[302] *Fairfest Media Ltd.* v. *ITE Group PLC & Ors.*, (2015) 3 ICC 75 : (2015) 2 CHN 704.

contractual obligations.[303] The Indian Contract Act, 1872 and the Specific Relief Act, 1963 apply to contractual matters. Further, an overwhelming majority of trade-secret disputes are employer-employee disputes and fall within the realm of Section 27 of the Indian Contract Act, 1872.[304]

5.3. In addition to these, liability can also arise under the provisions of the Indian Penal Code, 1860[305] such as Section 379 for theft; Section 405 to 409 against criminal breach of trust; Section 417 for cheating; and Section 418 for Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect. Since the Bharatiya Nyaya Sanhita, 2023[306] has been enacted, the corresponding provisions under Section 303 for theft; Section 316 against criminal breach of trust; and Section 318 against cheating can be possibly invoked. Further, where computer resources or electronic records are in issue, the provisions of the Information Technology Act, 2000[307] viz. Section 43 on penalty and compensation for damage to computer, computer system, etc.; Section 66 against computer related offences; Section 66B providing punishment for dishonestly receiving stolen computer resource or communication device; Section 72 providing penalty for breach of confidentiality and privacy; and Section 72A on punishment for disclosure of information in breach of lawful contract can also come into play. Further, third parties can also be liable under the Information Technology Act unless they are exempted by virtue of Section 79.

---

[303] Md Zafar Mahfooz Nomani and Faizanur Rahman, "Intellection of Trade Secret and Innovation Laws in India" 16 *Journal of Intellectual Property Rights* 341 (2011).
[304] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).
[305] Act No. 45 of 1860.
[306] Act No. 45 of 2023.
[307] Act No. 21 of 2000.

### *B. Judicial Interpretation and Precedents*

5.4. The law on protection of trade secret or confidential information, in the absence of any specific law, is largely driven by judicial precedents. An obligation to maintain confidentiality may arise in three ways – by the existence of contract or contractual provisions, under equity, or by the effect of a statute such as the Official Secrets Act, 1923.[308]

#### i. Defining Trade Secrets and Confidential Information

5.5. The first aspect that one observes is the attempt by courts at defining trade secrets. Courts in their decisions have made reference to the various definitions of "trade secret" or "confidential information". For instance, the definition of "trade secret" as defined in Black's Law Dictionary[309] which reads:

> *"a formula, process, device or other business information that is kept confidential to maintain an advantage over the competitors. It is the information which includes formula, pattern, compilation, programme, device, method, technique or process. That derives independent economic value from not being generally known or readily ascertainable by others who can obtain economic value from its disclosure or use."*[310]

5.6. In *American Express Bank, Ltd.* v. *Priya Puri*,[311] the Delhi High Court made the following observations while defining what constitutes trade secrets or confidential information:

> *"32. Regarding alleged confidentiality about the customers' names and addresses and their financial portfolios, it is being canvassed*

---

[308] *Tarun Wadhwa* v. *Saregama India Ltd.*, (2021) 88 PTC 423.
[309] *Bombay Dyeing and Manufacturing Co. Ltd.* v. *Mehar Karan Singh*, (2010) 7 Mah LJ 48 : (2010) 5 AIR Bom R 573.
[310] Black's Law Dictionary, 9th ed., at 1633.
[311] (2006) 3 LLN 217 : (2006) 110 FLR 1061.

*that since it is confidential, the plaintiff has an exclusive right to deal with these customers. Reliance has been placed by the plaintiff on Lansing Linde, Ltd. v. Kerr, [(1991) 1 All E.R. 418], to contend as to what constitutes trade secrets and confidential information. Defining what constitutes trade secrets and confidential information Lord Staughton held as follows:*

> *"a trade secret is information which, if disclosed to a competitor, would be liable to cause real or significant harm to the owner of the secret. I would add first, that it must be information used in a trade or business, and secondly that the owner must limit the dissemination of it or at least not encourage or permit widespread publication."*

*It (trade secrets) can thus include not only secret formulae for the manufacture of products but also, in an appropriate case, the names of customers and the goods which they buy."*

### ii. Trade Secrets, Confidential Information & Contracts

5.7. In the first category of cases where there is a contract, the cause of action is grounded in breach of contract and the Indian Contract Act, 1872 is the applicable law. Majority of such contractual disputes before the Indian courts are employer-employee disputes wherein there is either a non-compete clause or a Non-Disclosure Agreement ("NDA") and its breach is alleged. However, it cannot be said that there can be no incidents of contracts where breach of confidence can be claimed.[312] Where there is no explicit clause, confidence may be implied and breach of such confidence would be adjudged within the contours of such a contract.

5.8. When it comes to employer-employee disputes, the main issues revolve around enforcement of a non-compete clause to prevent an employee from

---

[312] *Tarun Wadhwa* v. *Saregama India Ltd.*, (2021) 88 PTC 423.

joining a competitor on the ground that information may be divulged.[313] While Section 27 of the Indian Contract Act, 1872 would prohibit enforcement of such a restrictive clause as being in restraint of trade, decisions have been rendered on both sides of the spectrum. For instance, the Supreme Court in *Niranjan Shankar Golikari v The Century Spinning & Mfg Co.*[314] upheld a non-compete clause which prevented the employee from joining a competitor during the original period/duration of the contract, which was five years in the present instance. The Court was of the opinion that such a clause was not a restraint within the meaning of Section 27. In a subsequent judgment, the Supreme Court distinguished between negative covenants during the course of employment and negative covenants after employment.[315] The Court held that negative covenants during the course of employment were permissible, however, post-termination such covenants were void in the eyes of the law. This interpretation of restraint of trade during the post-contractual period has been uniform, consistent and unchanged from 1874 till 2006, followed by all the High Courts in India, and expressly approved and re-affirmed by the Supreme Court.[316] Thus, in an overwhelming majority of decisions, the courts have denied injunctive relief to employers for restraining their former employee from joining a competitor and have held such restrictions on the employee post-termination to be void and unenforceable.[317] Further, the doctrine of restraint of trade is not confined solely to employment

---

[313] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

[314] 1967 AIR SC 1098.

[315] *Superintendence Company of India* v. *Krishna Murgai*, AIR 1980 SC 1717 : 1981 (2) SCC 246.

[316] *Percept D'Mark (India) (P) Ltd.* v. *Zaheer Khan*, (2006) 4 SCC 227.

[317] *Oakes & Company* v. *Jackson and Anr.*, I.L.R. 1 Madras 134; *The Brahmaputra Tea Co. Ltd.* v. *E. Scarth* I.L.R. 11 Calcutta 545; *Pragji Soorji* v. *Pranjiwan Tooljaram* 5 Bom LR 878; *Krishan Murgai* v. *Superintendence Co. of India*, AIR 1979 Delhi 232; *G.R.V. Rajan* v. *Tube Investments of India Ltd*, (1995) 1 LW 274; *Sandhya Organic Chemicals (Private), Ltd.* v. *United Phosphorous, Ltd.*, A.I.R. 1997 Guj. 177; *Ambiance India (Private), Ltd.* v. *Naveen Jain*, 2005 (4) L.L.N. 606; *Pepsi Foods, Ltd.* v. *Bharat Coca Cola Holdings (Private), Ltd.*, 81 (1999) D.L.T. 122; *American Express Bank, Ltd.* v. *Priya Puri*, (2006) 3 LLN 217 : (2006) 110 FLR 1061; *Stellar Information Technology Pvt Ltd* v. *Rakesh Kumar & Ors.*, (2016) 234 DLT 114.

contracts but is equally applicable to other types of contracts as well.[318] Thus, licensing agreements or other business agreements wherein such confidential information is shared and non-disclosure clauses are included in the contract are equally governed by Section 27.

5.9. Confidentiality agreements and Non-Disclosure Agreements are entirely permissible under law.[319] In fact, the importance of such agreements for business and commerce in today's highly globalised world cannot be overstated. Such clauses are a regular feature of commercial arrangements and are based upon the trust, honesty and confidential relationship between the parties.[320] However, what is impermissible and struck down by courts in an attempt to enforce a covenant in restraint of trade in the guise of such an agreement or clause.[321] Confidentiality clauses cannot be expanded to such an extent that they include information in the public domain and such an attempt is nothing but trying to restrain trade as nothing proprietary or confidential is actually sought to be protected.[322] An employee cannot restrict competition by preventing his employee from joining a competitor but he can protect his confidential information and secrets.[323]

5.10. Another aspect that is often brought before courts is the use of information that an employee may retain in his mind or a skill imparted during employment which may be used in future employment. In this regard, the courts have noted that nothing in law can prevent a person from acquiring knowledge which makes him a better employee for future employment and

---

[318] *Percept D'Mark (India) (P) Ltd.* v. *Zaheer Khan*, (2006) 4 SCC 227.
[319] *Fairfest Media Ltd.* v. *ITE Group PLC*, (2015) 3 ICC 75 : (2015) 2 CHN 704.
[320] *Anindya Mukherjee* v. *Clean Coats Pvt. Ltd.*, (2011) 1 Mah LJ 573 : (2011) 3 Bom CR 70.
[321] *M/s. Stellar Information Technology Private Ltd.* v. *Mr. Rakesh Kumar & Ors.*, (2016) 234 DLT 114.
[322] *Id.*
[323] *Herbert Morris Ltd.* v. *Saxelby*, (1916) 1 AC 688 : 114 LT 618 cited in *Superintendence Co. of India* v. *Krishan Murgai*, (1981) 2 SCC 246.

he is only prevented from divulging confidential information which he has received as an employee to competitor or any third party.[324] Employees perform a range of function and are exposed to a variety of information in the course of their employment, all of which is not confidential in nature. An employee cannot be restrained from using the business acumen that they acquire during their employment.[325] The observations of Lord Shaw in *Herbert Morris Ltd. v. Saxelby*,[326] as quoted by the Bombay High Court in *V.M. Deshpande* v. *Arvind Mills Company Ltd.*,[327] become relevant:

> *"Trade secrets, the names of customers, all such things which in sound philosophical language are denominated objective knowledge—these may not be given away by a servant; they are his mister's property, and there is no rule of public interest which prevents a transfer of them against the mister's will being restrained. On the other hand, a in man's aptitude, his skill, his dexterity his manual or mental ability—all those things which in sound philosophical language are not objective, but subjective—they may and they ought not to be relinquished by a servant; they are not his mister's property; they are his own property; they are himself. There is no public interest which compels the rendering of those things dormant or sterile or unavailing; on the contrary, the right to use and to expand his powers is advantageous to every citizen, and may be highly so for the country at large. This distinction which was also questioned in argument, is just as plain as the other."*
>
> (emphasis added)

In light of the above, it can be safely concluded that the inevitable disclosure doctrine that has been applied in the US does not apply in the Indian context. The inevitable disclosure doctrine permits an employee to restrict the employment of his ex-employee with a competitor despite failing to establish that the employee has taken or threatens to use trade

---

[324] *V. M. Deshpande* v. *Arvind Mills Company Ltd.*, ILR 1946 Bom 89 : (1946) 48 Bom LR 90.
[325] *Ambiance India (Private) Ltd.* v. *Naveen Jain*, (2005) 81 DRJ 538 : (2005) 122 DLT 421.
[326] [1916] 1 A.C. 688.
[327] ILR 1946 Bom 89 : (1946) 48 Bom LR 90.

secrets. Under this doctrine, the employee may be injuncted from such employment by "demonstrating the employee's new job duties will inevitably cause the employee to rely upon knowledge of the former employer's trade secrets."[328]

5.11. It must be noted that when it comes to analyzing the validity of such clauses, the courts cannot traverse beyond the words of Section 27 of the Indian Contract Act and there is no scope of assessing the reasonability of such clauses. Such clauses in their operation being in restraint of trade, whether partial or complete, are void.[329] The observations of the Supreme Court in *Superintendence Company of India (P) Ltd.* v. *Krishan Murgai*[330] become relevant in this regard:

> *"26. Now, so far as the present case is concerned, the law is to be found in section 27 of the Contract Act 1872, which reads:*
>
> > *"27. Agreement in restraint of trade void-Every agreement by which any one is restrained from exercising a lawful profession, trade or business of any kind is to that extent void.*
> >
> > *Exception: One who sells the goodwill of a business may agree with the buyer to refrain from carrying on a similar business, within specified local limits, so long as the buyer or any other person deriving title to the goodwill from him, carries on a like business therein, provided that such limits appear to the Court reasonable, regard being had to the nature of the business."*
>
> *The section is general in terms, and declares all agreements in restraint void pro tanto, except in the case specified in the exception.*
>
> *27. The question whether an agreement is void under section 27 must be decided upon the wording of that section. There is nothing in the wording of section 27 to suggest that the principle stated*

[328] *Whyte* v. *Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1446 (2002).
[329] *Wipro Limited* v. *Beckman Coulter International S.A.*, 131 (2006) DLT 681.
[330] (1981) 2 SCC 246.

*therein does not apply when the restraint is for a limited period only or is confined to a particular area. Such matters of partial restriction have effect only when the fact fall within the exception to the section.*"

(emphasis added)

### iii. Trade Secrets and Equitable Relief

5.12. In absence of a contact between the parties, courts have allowed action based on equitable principles of breach of confidence.[331] When disclosure in made during negotiations that may have not resulted in a formal contract, the remedy will lie in equity.[332] The earliest decision wherein relief was granted based on breach of equitable duty of confidence is *John Richard Brady* v. *Chemical Process Equipments Pvt Ltd.*[333] wherein reliance was placed on the English case of *Saltman Engineering Co Ltd & Others* v. *Campbell Engineering Co Ltd.*[334] The decision of *Saltman Engineering* has been relied on a catena of cases[335] and hence the Indian law closely resembles the English law and applies the same tests.[336] While, the *John Richard Brady* case related to confidential information on technology, the principle of breach of equitable duty of confidence has also been applied in multiples context such as movie or series concept note,[337] trading

---

[331] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

[332] *See, Fairfest Media Ltd.* v. *ITE Group PLC*, (2015) 3 ICC 75 : (2015) 2 CHN 704, relying on *Seagar* v. *Copydex*, 1967 (2) All ER 415; and *Lac Monarch* v. *International Corona*, (1990) F.S.R. 441.

[333] AIR 1987 Del 372.

[334] [1948] 65 RPC 203.

[335] *Zee Telefilms Ltd & Film & Ors.* v. *Sundial Communications Pvt. Ltd*, (2003) 3 Mah LJ 695; *Anindya Mukherjee* v. *Clean Coats Pvt. Ltd.*, (2011) 1 Mah LJ 573 : (2011) 3 Bom CR 70; *Hi-Tech Systems & Services Ltd.* v. *Suprabhat Ray & Ors.*, AIR 2015 Cal 261 : (2016) 1 ICC 584.

[336] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

[337] *Zee Telefilms Ltd & Film & Ors.* v. *Sundial Communications Pvt. Ltd.*, (2003) 3 Mah LJ 695; *Anil Gupta & Anr.* v. *Kunal Das Gupta & Ors.*, AIR 2002 Del 379; *Urmi Juvekar Chiang* v. *Global Broadcast News Ltd.*, (2007) 6 AIR Bom R 240 : 2007 (109) Bom LR 981; *Beyond Dreams Entertainment Pvt. Ltd.* v. *Zee Entertainment Enterprises Ltd.*, (2016) 5 Bom CR 266 : (2015) 62 PTC 241.

information,[338] client/customer list,[339] database,[340] drawings,[341] industrial/engineering designs[342] etc.

5.13. In a case of breach of confidence, the plaintiff ought to satisfy the four-fold test as followed in *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd.*[343] and *Narendra Mohan Singh* v. *Ketan Mehta*[344], relying on the English case of *CMI Centers for Medical Innovation GMBH and Anr.* v. *Phytopharm PLC.*[345] This was also affirmed in *Tarun Wadhwa* v. *Saregama India Ltd.*[346] Thus, in an action based on breach of confidence, the plaintiff must:

(i) identify clearly the information relied on;

(ii) show that it was handed over in circumstances of confidence;

(iii) show how it was information that had to be treated as confidential; and

(iv) show that it was used or threatened to be used without consent.[347]

5.14. Thus, the burden of proof to precisely identify the confidential information lies on the plaintiff, failing which the claim for relief may not succeed.[348] With respect to the information, it has to be shown that it is "confidential". This in itself is a two-part query wherein it has to be first determined if the information is such that it can be a subject matter of protection under equity

---

[338] *SEBI* v. *Kanaiyalal Baldevbhai Patel*, (2017) 15 SCC 1.
[339] *Burlington Home Shopping Pvt. Ltd.* v. *Rajnish Chibber*, 61 (1996) DLT 6; *Diljeet Titus* v. *Alfred A. Adebare*, 2006 SCC OnLine Del 551 : (2006) 130 DLT 330 : (2006) 32 PTC 609.
[340] *Tech Plus Media Private Ltd.* v. *Jyoti Janda*, (2014) 60 PTC 121.
[341] *Indiana Gratings Pvt. Ltd. & Anr.* v. *Anand Udyog Fabricators Pvt. Ltd. & Ors.*, (2009) 39 PTC 609.
[342] *Polymer Papers Ltd.* v. *Gurmit Singh*, (2002) 25 PTC 327.
[343] (2003) 3 Mah LJ 695 : (2003) 5 Bom CR 404 : (2003) 105(3) Bom LR 678 : (2003) 27 PTC 457.
[344] (2015) 64 PTC 260.
[345] (1999) Fleet Street Reports 235.
[346] (2021) 88 PTC 423.
[347] *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd*, (2003) 3 Mah LJ 695 : (2003) 5 Bom CR 404 : (2003) 105(3) Bom LR 678 : (2003) 27 PTC 457.
[348] *SaNOtize Research and Development Corp.* v. *Lupin Limited and Others*, 2022 SCC OnLine Bom 6596; *Sirmour Remedies Private Limited & Anr.* v. *Kepler Healthcare Private Limited & Ors*, 2014 SCC OnLine Cal 2703 : (2014) 2 Cal LT 357.

and the secondly if the information is confidential i.e., not in the public domain. With respect to the first requirement on the nature of information sought to be protected, it has been held that the information must not be vague[349] and it must be sufficiently developed so that it is capable of being realised as an actuality.[350] With respect to the second element, of the information being confidential, it is required that the information must not be known to the public. Simply labelling information as confidential, would not devolve upon that information characteristics of being a secret. General knowledge of facts or information that competitors in business have knowledge over cannot be treated as confidential.[351] Confidential information can be a combination of elements, characteristics and components which were in the public domain. If the information is neither unique nor novel, but merely a compilation of existing materials or information that is freely available, or widely practiced, then there is no question of confidentiality.[352] Thus, it becomes important to decipher the contours of public domain. With respect to what is "public domain", it would comprise matters already known to the public. Public domain has been defined as:

> "**49.** "*Public domain*" is defined in *Black's Law Dictionary*, Eighth Edition at page 1265 thus:—
>
> "*When copyright, trademark, patent, or trade secret rights are lost or expire, the intellectual property they had protected becomes part of the public domain and can be appropriated by anyone without liability for infringement.*"
> "*Public domain is the status of an invention, creative work, commercial symbol, or any other creation that is not protected by*

[349] Michael Spence, *Intellectual Property* chap. 6 (Oxford University Press, 2007).
[350] *Anil Gupta* v. *Kunal Dasgupta*, ILR (2002) 1 Del 250 : AIR 2002 Del 379 : (2002) 97 DLT 257 : (2002) 25 PTC 1; *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd.*, (2003) 3 Mah LJ 695 : (2003) 105 (3) Bom LR 678; *Tarun Wadhwa* v. *Saregama India Ltd.*, (2021) 88 PTC 423; *Fraser* v. *Thames Television Ltd.*, (1983) 2 All E.R. 101.
[351] *Star India Pvt. Ltd.* v. *Laxmiraj Seetharam Nayak*, (2003) 3 LLN 106 : (2003) 3 Bom CR 563.
[352] *Emergent Genetics India (P) Ltd.* v. *Shailendra Shivam*, (2011) 125 DRJ 173 : (2011) 47 PTC 494.

*any form of intellectual property. Public domain is the rule: intellectual property is the exception. J. Thomas McCarthy,* McCarthy on Trademarks and Unfair Competition *1.01 [2], at 1-3 (3d ed. 1996).*"[353]

5.15. Further, since confidential information may incorporate elements of what already exists in the public domain, it becomes imperative to determine under what circumstances will something existing in the public domain transform into confidential information. In this regard the often-quoted[354] observations of Megarry J in *Coco v. AN Clark (Engineers) Ltd*[355] become relevant:

> "……*Something that has been constructed solely from materials in the public domain may possess the necessary quality of confidentiality: for something new and confidential may have been brought into being by the application of the skill and ingenuity of the human brain. Novelty depends on the thing itself, and not upon the quality of its constituent parts. Indeed, often the more striking the novelty, the more commonplace its components. Mr. Mowbray demurs to the concept that some degree of originality is requisite. But whether it is described as originality or novelty or ingenuity or otherwise, I think there must be some product of the human brain which suffices to confer a confidential nature upon the information: and, expressed in those terms, I think that Mr. Mowbray accepts the concept.*
>
> *The difficulty comes, as Lord Denning, M.R. pointed out in the Seager case on page 931, when the information used is partly public and partly private; for then the recipient must somehow segregate the two and, although free to use the former, must take no advantage of the communication of the latter. To this subject I must in due course return. I must also return to a further point, namely, that where confidential information is communicated in circumstances of confidence the obligation thus created endures, perhaps in a modified form, even after all the information has been published or is ascertainable by the public; for the recipient must*

---

[353] *Bombay Dyeing and Manufacturing Co. Ltd.* v. *Mehar Karan Singh*, (2010) 7 Mah LJ 48.
[354] *Tarun Wadhwa* v. *Saregama India Ltd.*, (2021) 88 PTC 423; *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd*, (2003) 3 Mah LJ 695; *Jyoti Kapoor and Anr.* v. *Kunal Kohli and Ors.*, (2015) 6 Bom CR 54.
[355] [1968] FSR 415.

*not use the communication as a spring-board (see the Seager case, pages 931 and 933). I should add that, as shown by Cranleigh Precision Engineering Ltd. v. Bryant, [1965] 1 WLR 1293; [1966] R.P.C. 81, the mere simplicity of an idea does not prevent it being confidential (see pages 1309 and 1310). Indeed, the simpler an idea, the more likely it is to need protection."*[356] (emphasis added)

Thus, confidential information may contain elements already in the public domain, however, the information must be a result of the application of skill or mind so to produce something that is already not known.[357] The quality of content is not the determinative aspect but what matters is that the information is novel in the sense that it is not known to the public.

5.16. In many of the cases involving breach of confidence, there is a claim of copyright involved as well. It is thus relevant to understand the fine but important distinction between copyright and trade secrets or confidential information. While confidential information may include mere ideas but these do not form part of the subject matter of copyright which protects only the expression of such ideas.[358] Further, copyright exists over expressions that have been fixed or reduced to a permanent form, however, law of confidence protects communication, oral or written. While copyright is a right *in rem*, breach of confidence can only be brought against those who received the information in confidence, hence it is a right *in personam*. The duration of copyright is finite as restricted by Sections 22 to 29 of the Copyright Act, 1957.[359] However, there is no restriction on

---

[356] (1969) R.P.C. 41, as cited in *Tarun Wadhwa* v. *Saregama India Ltd.*, (2021) 88 PTC 423.
[357] *See, Anindya Mukherjee* v. *Clean Coats Pvt. Ltd.*, (2011) 1 Mah LJ 573 : (2011) 3 Bom CR 70, citing *Faccenda Chicken Ltd.* v. *Fowler*, (1985) 1 All ER 724; and *Saltman Engineering Co. Ltd.* v. *Compbell Engineering Co. Ltd.*, (1963) 3 All ER 413.
[358] *Burlington Home Shopping Pvt Ltd v Rajnish Chibber*, 61 (1995) DLT 6 : 1995 (35) DRJ 335.
[359] Act No. 14 of 1957.

the term of trade secrets or confidential information and it can continue to exist so long as the underlying information remains confidential.[360]

5.17. The Bombay High Court in *Tarun Wadhwa* v. *Saregama India Ltd.*[361], against the backdrop of differentiating between copyright and confidential information, explained in clear terms what amounts to "confidential" and when an obligation arises. The Court observed that:

> *"30. Breach of confidentiality and copyright infringement are closely tied. The former is frequently claimed for matters that cannot be the subject of copyright infringement. An idea, in particular, cannot be the subject of a copyright infringement action; but it may be the subject of breach of confidentiality. Either may yield a broadly similar injunction. There is no copyright in India except as provided by the Copyright Act, 1957. But this is not in derogation of a claim of breach of trust or confidence.*
>
> .....
>
> *32. An obligation of confidence arises when confidential information is shared or communicated or otherwise is to the knowledge of a person in circumstances where he has notice, explicit or implicit, or must be held to have agreed, that the information is indeed confidential. That person would then be restrained from using or disclosing this confidential information without the permission or license, express or implied, of the person who gave or shared it. Where there is a contract — which may be written or oral, express or implied — the obligation stems from the spelt-out terms of the contract. But the obligation exists in equity too, and is rooted in the legal concept of the duty to act in good faith. The respecting of that which is confidential has been said to be a general rule in the public interest.*
>
> .....
>
> *34. Confidence law is perhaps wider than copyright law. It protects the substance of ideas and information, irrespective of the mode of communication. There is no copyright in an idea, but only in the form of its expression. Copyright is a right in rem, but a confidence obligation is entirely in personam. Copyright has a statutorily*

[360] *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd.*, (2003) 3 Mah LJ 695.
[361] (2021) 88 PTC 423.

*defined term. Confidence does not. There is no copyright except as provided by the statute, and infringement is also prescribed by statute. A confidence obligation is one in contract or equity (or both). There are statutory defences to a copyright infringement action. These do not apply to a breach of confidence action. The distinction between copyright and confidence assumes importance where, say, a manuscript has been submitted for publication. An obligation not to use the submitted manuscript may be implied and enforced under confidence law, and may extend to a plot or a developed idea that may not otherwise be protected by copyright.*

*..... .....*

*40. Therefore, the 'confidential information' — that which is not in the public domain — must be accurately and specifically identified, and protection must be sought only in respect of that. A generalized statement is never enough. In Beyond Dreams Entertainment Pvt. Ltd. v. Zee Entertainment Enterprises Ltd.[2], a learned Single Judge of this Court summarized the components of confidentiality, inter alia holding that the confidential information must be clearly identified.*

*..... .....*

*42. Essential, therefore, to any case of confidentiality are precision, originality and completeness of disclosure. The precise identification must be in the plaint. The confidential information must be proprietary. It must, in short, be original. This is not the originality of expression that is the subject of copyright law; it may be the originality of idea, and it is used here in contradistinction to whispering in alleged confidence matters that are already known. Those are never subjected to the doctrine. Any confidential information by definition must be outside the public domain. It must also be sufficiently developed to an extent that lends itself to realization. All these elements must co-exist. It is not enough for a plaintiff to say, for instance, that everything is original, or that some things are original and some things are not but not identify them. Therefore : for a cause of action in breach of confidence to succeed there must be precision, there must be originality, and there must be completeness. All the required elements of confidentiality must be shown. It is not enough to show only some of them.*

*43. The springboard doctrine is really an extension or a result of the breach of confidence principle. It says that a matter communicated — and, I would add, communicable — in circumstances of*

*confidence cannot be used by a defendant as a springboard to bring forth a rival work.*"[362]

(emphasis added)

5.18. The four-fold criteria affirmed in *Zee Telefilms Ltd.*[363] not only requires the information to qualify the criteria of being capable of protection and being confidential, but further requires that such information has to be transmitted in a fashion that an obligation of confidence arises between the parties. Such a duty arises when "*confidential information comes to the knowledge of a person in circumstances where he has notice, or is held to have agreed, that the information is confidential, with the effect that it would be just in all the circumstances that he should be precluded from disclosing the information to others.*"[364] This would be a factual inquiry and has to be found in the circumstances specific to each particular case.

5.19. An equally important aspect is that the duty of confidentiality also extends to third-parties.[365] In this regard, it has been held that "'*the obligation of confidence rests not only on the original recipient, but also on any person who received the information with knowledge, acquired at the time or subsequently, that it was originally given in confidence.*"[366] This ties in perfectly with the "springboard" concept enunciated by Roxburgh, J *Terrapin Ltd.* v. *Builders' Supply Company (Hayes) Ltd. And Ors.*[367] and

---

[362] *Id.*

[363] *Zee Telefilms Ltd.* v. *Sundial Communications Pvt. Ltd*, (2003) 3 Mah LJ 695.

[364] *See, Fairfest Media Ltd.* v. *ITE Group PLC*, (2015) 3 ICC 75 : (2015) 2 CHN 704, citing with approval the observations made by Lord Griffiths in *Personal Management Solutions Limited & Anr.* v. *Brakes Bros. Limited & Ors.*, (2014) EWHC 3495 (QB).

[365] *AIA Engineering Pvt Ltd* v. *Bharat Dand and Ors.*, (2007) 2 GCD 1100 : (2007) 48 (4) GLR 3303.

[366] *Zee Telefilms Ltd & Film & Ors.* v. *Sundial Communications Pvt. Ltd.*, (2003) 3 Mah LJ 695; Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

[367] [1967] RPC 375.

affirmed in Roskill J in *Cranleigh Precision Engineering Ltd.* v. *Bryant* reported[368], which goes as follows:

> *"As I understand it, the essence of this branch of the law, whatever the origin of it may be, is that a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public."*[369]

### iv. Trade Secrets and Criminal Liability

5.20. In terms of criminal liability, the picture remains unclear. Criminal prosecution in cases relating to confidential information are usually initiated under Sections 375, 381, 405, 408 and 418 of the IPC. While there are cases wherein the High Courts have quashed the complaint before trial,[370] this does not rule out the possibility of trial being allowed in the circumstances particular to a case[371] and depending on the interpretation of a court. Many a times, the provisions of the Information Technology Act, 2000 pertaining to computer resources and electronic records are invoked.[372]

5.21. In a case before the Gujarat High Court, the complaint was quashed on the ground that customer lists are not trade secrets or property and on the conceptual aspect that trade secrets are not "property" when claimed under

---

[368] [1964] 3 ALL E.R. 289

[369] *Terrapin Ltd.* v. *Builders' Supply Company (Hayes) Ltd. & Ors*, [1967] RPC 375.

[370] *Pramod, son of Laxmikant Sisamkar & Uday Narayanrao Kirpekar* v. *Garware Plastics and Polyester Ltd & Anr.*, (1986) 3 Bom CR 411; *Hemal R Shah* v. *State of Gujarat*, Special Criminal Application No. 1171 of 2009 before the High Court of Gujarat (27 December, 2010).

[371] *Narayan Chandra Mukherjee & Ors.* v. *State of Bihar & Anr.*, (2001) 49 (1) BLJR 680.

[372] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

an equitable relief. However, there is still the possibility of such cases falling within ambit of applicable penal provision on crime against property under the IPC. In *Birla Corpn. Ltd.* v. *Adventz Investments & Holdings Ltd.*,[373] pertaining to taking away of document containing confidential information, the Court while holding documents to be corporeal property being capable of being subjected to theft held that "*information contained in a document, if replicated, can be the subject of theft and can result in wrongful loss, even though the original document was only temporarily removed from its lawful custody for the purpose of extracting the information contained therein.*"[374] Information on prosecution and conviction in these matters is scant[375] and thus the applicability of criminal law to misappropriation confidential information remains obscure.

### v. Trade Secrets and Freedom of Speech & Expression

5.22. Another category of cases that have been presented before the courts is when equitable duty of breach of confidence, which extends to third parties, comes in conflict with fundamental right to speech and expression under Article 19(1)(a). This issue arose before the Delhi High Court in the matter of *Petronet LNG Ltd.* v. *Indian Petro Group*.[376] In addition to the claim of breach of confidentiality, the right to privacy was also claimed which was rejected by the Court as it was being claimed against a non-state actor. The Court also clarified that rights under Article 19 are not available to artificial or juristic personalities, however, shareholders or directors can claim relief by establishing that the impugned action impairs their rights.

---

[373] (2019) 16 SCC 610 : (2020) 2 SCC (Civ) 713.
[374] *Id.*
[375] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).
[376] (2009) 158 DLT 759.

The Court in this case endeavoured to strike a balance between duty of maintaining confidentiality and the fundamental right to free speech and expression. The Court observed that larger public interest justified the publication of such material and it was disinclined to grant an injunction. The following observations of the court become relevant:

> *"86. In view of above conclusions, it is held that the plaintiff has been unable to substantiate its claim for confidentiality or that the information in regard to the news items complained against are of such sensitive nature as to warrant prior restraint of their disclosure. On the other hand, the defendants, in the opinion of the Court, have been able to show public interest in news reporting and discussion about the plaintiff's functioning—in the areas sought not to be interdicted by the kind of injunction sought. Clearly, the grant of injunction would destroy the very essence of press freedom and the right of the general public to be informed about the functioning of an entity in which 50% stake is held by the Central Public Sector Undertakings.*
>
> *87. This Court, while recollecting the judgment of the Supreme Court in S. Rangarajan, Virendra, Rajgopal as well as that of the US Supreme Court in Sullivan, is of the opinion that the public interest in ensuring dissemination of news and free flow of ideas, is of paramount importance. The news or information disclosure of which may be uncomfortable to an individual or corporate entity but which otherwise fosters a debate and awareness about functioning of such individuals or bodies, particularly, if they are engaged in matters that affect people's lives, serve a vital public purpose. Very often, the subject of information or news—i.e. the individual or corporation may disagree with the manner of its presentation. If it contends that such presentation tends to defame or libel, it is open for the entity or individual to sue for damages. In the case of a corporate entity, unless the news presented is of such a sensitive nature that its business or very existence is threatened or would gravely jeopardize a commercial venture, the Courts would be slow in interdicting such publication. The Constitution's democratic framework, depends on a free commerce in ideas, which is its life blood. In the words of Walter Lippmann newspapers are "the bible of democracy". Justice Holmes (Abrams v. US, 250 US 616 (1919)) characterized the discussion of public matters as essential to see that*

*"the ultimate good desired is better reached by a free trade in ideas". Even more poignantly, one of the principal architects of the American Constitution, James Madison, (1751-1836) wisely stated that:*

> *"Nothing could be more irrational than to give the people power, and to withhold from them information without which power is abused. A people who mean to be their own governors must arm themselves with power which knowledge gives. A popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy, or perhaps both."*

(emphasis added)

### vi. Trade Secrets and RTI Act, 2005

5.23. The Right to Information Act, 2005[377] ("RTI Act") has been enacted to ensure the free dissemination of information to the citizens in order to ensure transparency and accountability in the working of every public authority in India. However, every information is not subject to disclosure under the RTI Act, 2005. In order to gain regulatory approvals, commercial entities are often required to submit information with Regulatory and other governmental bodies and such information is quite often confidential in nature. In such situations, RTI Act, 2005 can be used to gain access to such sensitive and confidential information by business competitors. It is precisely to address any such situation that Section 8(1)(d) finds place in the statute.[378] Section 8 provides certain instances wherein the public authority is exempt from the obligation to disclose the information sought by a citizen under the RTI Act. Sub-clause (d) of Section 8 exempts disclosure of information qualifying as commercial confidence, trade secrets or intellectual property that gives competitive advantage to a third-

[377] The Right to Information Act, 2005 (Act No. 22 of 2005)
[378] *Id*, sec. 8(1)(d).

party and the disclosure of which would harm the same.[379] However, there is exception incorporated within the provision itself which enables the competent authority to disclose such information in larger public interest. Further, any particular information which is exempt from disclosure at a particular point in time may not continue to remain exempt indefinitely.[380] If disclosure would not adversely impact the competitive position of a third party, then such disclosure may not be exempt from the purview of disclosure. Section 8(d) reads as under:

> *"8. Exemption from disclosure of information.— (1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—*
>
> *..... .....*
>
> *(d) information including commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless the competent authority is satisfied that larger public interest warrants the disclosure of such information; ..."*[381]

5.24. Section 8(2) again reiterates the position that a public authority may allow access to information wherein public interest in disclosure outweighs the harm to the protected interests.[382] The sub-section is a *non-obstante* clause and has overriding impact on sub-section (1) of Section 8. Thus, even if some information is claimed to be confidential or a trade secret, the same can be revealed by the public authority if there is a greater public interest at stake in its disclosure. Section 8(2) reads as under:

> *"8. Exemption from disclosure of information.—..... .....*
>
> *(2) Notwithstanding anything in the Official Secrets Act, 1923 (19 of 1923) nor any of the exemptions permissible in accordance with sub-*

---

[379] *Id.*
[380] *ICAI* v. *Shaunak H. Satya* (2011) 8 SCC 781 : (2011) 4 SCC (Civ) 504.
[381] *Id.*
[382] *Id*, sec. 8(2).

*section (1), a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interests.*[383]"

5.25. There does remain a grey area on account of sub-clause (3) of Section 8 which mandates that any information relating to any occurrence, event or matter which has taken place, occurred or happened twenty years before the date on which any request is made under section 6 shall be provided to person requesting such information.[384] Section 8(3) reads as under:

> *"8. Exemption from disclosure of information.—.... ....*
> *(3) Subject to the provisions of clauses (a), (c) and (i) of sub-section (1), any information relating to any occurrence, event or matter which has taken place, occurred or happened twenty years before the date on which any request is made under section 6 shall be provided to any person making a request under that section:*
>
> *Provided that where any question arises as to the date from which the said period of twenty years has to be computed, the decision of the Central Government shall be final, subject to the usual appeals provided for in this Act."*

5.26. Whether this can apply to trade secrets or confidential information that is protected for more than 20 years is something that needs to be explored. On a plain reading of the provision, it seems to be the case that a particular piece of information that may be otherwise exempt from disclosure, may have to be disclosed if the application is made after twenty years.[385]

5.27. In addition to this, the legislation under which regulatory approval is being sought may also impose an obligation on the relevant authority to maintain confidentiality of such data.

---

[383] *Id.*
[384] *Id*, sec. 8(3); *ICAI* v. *Shaunak H. Satya* (2011) 8 SCC 781 : (2011) 4 SCC (Civ) 504.
[385] *ICAI* v. *Shaunak H. Satya* (2011) 8 SCC 781 : (2011) 4 SCC (Civ) 504.

### C. *Previous Attempts at Policy and Legislation*

5.28. India took a principled stand against inclusion of trade secrets or confidential information within the purview of the TRIPS Agreement during the negotiations. India in its written communication addressed to the GATT secretariat during the Uruguay Round stated that:

> *"46. Trade Secrets cannot be considered to be intellectual property rights. The fundamental basis of an intellectual property right is its disclosure publication and registration, while the fundamental basis of a trade secret is its secrecy and confidentiality. The laws of many developing countries clearly stipulate that the term "licensor" and "licensee" should not be applied to a transaction involving the supply of confidential know-how, and only expression such as "supplier" and the "recipient" should be used because such know-how cannot be regarded as a licensable light. The observance and enforcement of secrecy and confidentiality should be governed by contractual obligations and the provisions of appropriate Civil Law and not by intellectual property law.*
>
> *47. Since trade secret cannot be regarded as an intellectual property, it is beyond the mandate of the Negotiating Group to consider this matter."*[386]

5.29. Post the TRIPS Agreement, India amended its existing IP laws and even enacted new statutes in order to fulfil its obligations under the TRIPS Agreement. However, in light of the flexibility provided under the Article 39 of the TRIPS Agreement itself and considering the then prevailing position and framework sufficient, no law on trade secrets was brought in. Thus, protection of trade secrets continued to be governed under common law principles, breach of confidentiality, equity, contract and general provisions of the IPC, as the case may be.

---

[386] Communication from India, 'Standards and principles concerning the availability scope and use of Trade-Related Aspects of Intellectual Property Rights' MTN.GNG/NG11/W/37 (10 July 1989), *available at*: https://docs.wto.org/gattdocs/q/UR/GNGNG11/W37.PDF (last visited on Januray 28, 2024).

5.30. However, post-1995, the nature and size of the Indian economy changed greatly. Considering the changing requirements of the economy and demands from the industry, certain steps were initiated by the Indian Government to consider the issue of adequacy of protection of trade secrets in India.

### i. The National Innovation Bill, 2008

5.31. The Department of Science & Technology had released a draft on a legislation called "The National Innovation Bill, 2008". The draft Bill however did not address trade secrets in a stand-alone manner but in the context of spurring innovation.[387] The Preamble to the draft Bill read "*An Act to facilitate public, private or public-private partnership initiatives for building an Innovation support system to encourage Innovation, evolve a National Integrated Science and Technology Plan and codify and consolidate the law of confidentiality in aid of protecting Confidential Information, trade secrets, and Innovation.*"[388] Thus, codifying and consolidating the laws on confidential secrets and trade secrets was one of the three objectives of the draft.[389]

5.32. The Chapter IV titled "Confidentiality and Confidential Information And Remedies And Offences" comprising Section 8 to 14, was dedicated to protection of confidential information.[390] The draft used the term "confidential information" and the criteria for protection seemed to be in

---

[387] Naveen Gopal, "Revisiting the National Innovation Bill of 2008" 5 *International Journal of Law Management & Humanities* 322 (2022), *available at*: https://doij.org/10.10000/IJLMH.113785.
[388] *Id.*
[389] Dr. Md. Zafar Mahfooz Noman and Dr. Faizanur Rahman, "Innovativeness & Competitiveness under Trade Secret Laws in India" 2 *Manupatra Intellectual Property Reports* 131 (2015).
[390] Abhijeet Kumar and Adrija Mishra, "Protecting Trade Secrets in India" 18 *The Journal of World Intellectual Property* 335 (2015).

line with Article 39 of the TRIPS Agreement.[391] Further, the Bill appeared to be heavily influenced by the US law especially given how confidential information was defined incorporating illustrations given under 1(4) of the Uniform Trade Secrets Act, 1985.[392] Moreover, the definition of misappropriation was also borrowed from Section 1(2) of the UTSA.[393] Though, there was a heavy influence of the US law, only information that has actual commercial value was protected and not negative knowledge as is the case in the US. This was in line with the position adopted by the Indian courts.

5.33. Further, the Bill imposed very onerous obligations on third-parties receiving information on investigating whether they are receiving information through authorised channels or not. The burden on the receipt was much higher than the minimum standard prescribed under Article 39 of the TRIPS Agreement. Further, certain key definitions such as what would amount to "improper means" and what is "public domain" were also not defined thereby leaving some scope for confusion and varied judicial interpretation.

5.34. Another aspect that is important to consider is the exceptions that were provided under the Bill. While there was a specific clause incorporating independent creation as an exception to misappropriation, however, there was no specific enumeration for reverse engineering which is considered fair and is a significant limiting doctrine which allows balancing of both the vested private and public interests. Reverse engineering is understood as a permitted honest commercial practice even without being mentioned

---

[391] *Id.*
[392] Naveen Gopal, "Revisiting the National Innovation Bill of 2008" 5 *International Journal of Law Management & Humanities* 322 (2022), *available at*: https://doij.org/10.10000/IJLMH.113785.
[393] *Id.*

specifically and it does not find a specific reference in the TRIPS Agreement. However, companies often try to stop reverse engineering by incorporating anti-reverse engineering clauses in licensing agreements such as clip-warp agreements in case of software.[394] The Bill also incorporated the "disclosure in public interest" exception, however, there were no indicators that the Courts must keep in mind while adjudicating whether there should be disclosure in public interest making the provision vague.[395]

5.35. The Bill, however, could not make it past the phase of infancy and was not tabled in the Parliament.[396]

### ii. US Interventions

5.36. In the year 2016, India and US released a joint statement wherein both Government *inter alia* affirmed that they were committed to strong protection of trade secrets in their respective countries and to continue engagement on effective trade secret protection mechanisms.[397] India also undertook to conduct a further study on various legal approaches to protection of trade secrets.[398]

---

[394] Yang Chen, "Enforceability of Anti-Reverse Engineering Clauses in Software Licensing Agreements: The Chinese Position and Lessons from the United States and European Union's Laws" 42 *U. Pa. J. Int'l L.* 783 (2022).
[395] Dr. Md. Zafar Mahfooz Noman and Dr. Faizanur Rahman, "Innovativeness & Competitiveness under Trade Secret Laws in India" 2 *Manupatra Intellectual Property Reports* 131 (2015).
[396] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).
[397] India and United States Joint Statement on the Trade Policy Forum (October 20, 2016), *available at*: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2016/october/%E2%80%8BIndia-US-Joint-Statement-TPF (last visited on February 3, 2024); Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).
[398] India and United States Joint Statement on the Trade Policy Forum (October 20, 2016), *available at*: https://ustr.gov/about-us/policy-offices/press-office/press-releases/2016/october/%E2%80%8BIndia-US-Joint-Statemet-TPF (last visited on February 3, 2024).

5.37. Apart from Government level cooperative engagements and dialogue, the lack of adequate legal measures for protection of trade secrets is often cited in the annual Special 301 Reports released by the Office of the United States Trade Representative and India is a regular mention in the priority watchlist[399] which identifies trading partners that do not adequately or effectively protect and enforce IP rights.

### iii. National Intellectual Property Rights Policy, 2016

5.38. The Department of Industrial Policy & Promotion (DIPP) had released the National Intellectual Property Rights Policy, 2016 to spur creativity and stimulate innovation in India.[400] The National IPR Policy sought to lay a roadmap for the future of IPRs in India. While the policy did lay down broad policy goals, however, it stopped short of providing any concrete or definite solutions on many issues that were identified.[401] The Policy outlined seven broad objectives, the third one being legal and legislative framework under which it was envisaged to establish strong and effective IPR laws which balance the interests of right owners with larger public interest. One of steps to be taken towards the achievement of this goal was to identify important areas of study and research for future policy

---

[399] Office of the United States Trade Representative, 2023 Special 301 Report 23, 53 & 56 (2023), *available at*: https://ustr.gov/sites/default/files/2023-04/2023%20Special%20301%20Report.pdf; Office of the United States Trade Representative, 2022 Special 301 Report 23, 53 & 56 (2022), *available at*: https://ustr.gov/sites/default/files/IssueAreas/IP/2022%20Special%20301%20Report.pdf; Office of the United States Trade Representative, 2021 Special 301 Report 22 & 51 (2021), *available at*: https://ustr.gov/sites/default/files/files/reports/2021/2021%20Special%20301%20Report%20(final).pdf; Office of the United States Trade Representative, 2020 Special 301 Report 6, 18 & 51 (April, 2020), *available at*: https://ustr.gov/sites/default/files/2020_Special_301_Report.pdf; Office of the United States Trade Representative, 2019 Special 301 Report 7, 18 & 52 (April, 2019), *available at*: https://ustr.gov/sites/default/files/2019_Special_301_Report.pdf.

[400] Government of India, National Intellectual Property Rights Policy (Department of Industrial Policy & Promotion, Ministry of Commerce and Industry, May, 2016), *available at*: https://ipindia.gov.in/writereaddata/Portal/Images/pdf/2016-_National_IPR_Policy-2016__English_and_Hindi.pdf (last visited on February 17, 2024).

[401] Prashant Reddy T., "The 'Other IP Right': Is It Time to Codify the Indian Law on Protection of Confidential Information?" 5 *Journal of National Law University Delhi* 1 (2008).

development including protection of trade secrets.[402] However, no concrete steps were taken in pursuance of the same in the years that followed release of the policy.

### iv. Parliamentary Standing Committee Report

5.39. The Department Related Parliamentary Standing Committee on Commerce in its 161st Report undertook a review of the intellectual property rights regime in India.[403] The Report was submitted to both houses of the Parliament in 2021. In the Report, the Committee pointed out the "challenges in strengthening the country's IPR regime, the related procedural and substantive constraints, legal aspects and other issues, such as low awareness of IPR, counterfeiting and piracy, IP financing, and IPRs in agriculture and pharmaceutical sector, etc." The Committee *inter alia* considered the question whether there is need for a separate law on trade secrets or amending the Indian Contract Act, 1872 would suffice the purpose of adequate legal protection. The Committee in the context of trade secrets made the following recommendation:

> *"17.4 The Committee underlines that securing data and maintaining its confidentiality in business and trade is of paramount importance for companies possessing secret formulas, business strategies, algorithms, etc. Also, a separate statute or framework for trade secret protection in India is imperative in wake of rising frauds and misappropriation in digital world. In this regard, the Committee recommends the Department to consider enacting a separate legislation or a framework for protection of trade secrets. It further recommends the Department to examine the relevant and best*

---

[402] Government of India, National Intellectual Property Rights Policy 10 (Department of Industrial Policy & Promotion, Ministry of Commerce and Industry, May, 2016), *available at*: https://ipindia.gov.in/writereaddata/Portal/Images/pdf/2016-_National_IPR_Policy-2016__English_and_Hindi.pdf (last visited on February 17, 2024).

[403] The Department Related Parliamentary Standing Committee on Commerce, 161st Report on Review of the Intellectual Property Rights Regime in India (July, 2021).

*practices being followed in statutes of various countries for their implementation in India."*[404]

5.40. After 2021, no specific measures have been initiated by the Government or in the Parliament to consider the subject of trade secret protection in India.

### *D. Indian Position on Data Exclusivity*

5.41. As far as India is concerned, under the Drugs and Cosmetics Act, 1940 and the Insecticides Act, 1968, the government agencies have the power to demand data for the purpose of granting approval of the marketing of drugs and insecticides. They do in fact demand data for this purpose. There is no express provision in these Acts providing protection for the data submitted to the authorities. It is evident that as per Article 39(3) India has an obligation to provide some form of protection to the confidential test data submitted to the authorities.[405]

5.42. The Indian Drugs and Cosmetics Rules, 1945, under Rule 122E, provides for data exclusivity for a "new drug" for a total period of 4 years from the date of approval.

5.43. In India, a "new drug" is not defined solely as a patented drug but rather as a drug that has not been extensively used in the country.[406] This includes products not recognized or licensed in India, recently licensed and approved drugs for marketing, combinations of drugs previously approved individually but marketed as a combination, as well as vaccines and drugs

---

[404] *Id*, at 44.
[405] Dr. N S Gopalakrishnan and Benoy K. Kadavan, "Study on Testdata Protection in India" *Centre for Intellectual Property Rights Studies, School of Legal Studies, Cochin University of Science & Technology, Cochin* (2003).
[406] *Id.*

derived from Recombinant DNA (r-DNA). Similar to the United States, Indian law mandates that applicants for new drugs must undergo rigorous testing and clinical trials. However, this requirement can be waived in cases of "public interest" or if the new drug has been approved and marketed for several years in other countries.[407] Such waivers are standard practice to prevent redundant trials in different jurisdictions, which can increase costs and delay the introduction of the drug to the market.

5.44. Unlike the United States, drug approval in India is not linked to patent protection. This means that in the US, any application by a generic drug manufacturer will only be evaluated if it does not pertain to a drug covered by an existing patent.[408] This linkage often leads to delays in the entry of generic drugs into the market. While such linkage may be advantageous for countries with a predominant presence of innovator companies, like the United States, it poses a disadvantage for countries with a thriving generic drug industry, such as India.

5.45. In India, when considering granting marketing approval for a drug, the Drug Controller primarily evaluates whether the drug has undergone safety testing elsewhere and if the data submitted to demonstrate safety in another jurisdiction would be sufficient for the drug to be introduced in India.

5.46. In 2004, the Department of Chemicals and Petrochemicals (DCPC), Ministry of Chemicals and Fertilizers, Government of India, established an Inter-Ministerial Committee as a Consultative group. This Committee was tasked with recommending the actions to be taken by the Government

---

[407] *Id.*

[408] G. Lee Skillington & Eric M. Solovy, "The Protection of Test and Other Data Required by Article 39.3 of the TRIPS Agreement" 24 *Northwest Journal of International Law* 34 (2003).

concerning Article 39.3 of the TRIPS Agreement. Additionally, the Committee aimed to assess whether data exclusivity for agrochemicals, traditional medicines, and pharmaceuticals could be encompassed within the existing legal framework or if new legislation was necessary for this purpose.

5.47. In this context, the Satwant Reddy Report on Article 39.3 of the TRIPS Agreement recommended that there was no requirement for 'data exclusivity' under Article 39.3, and it was not in India's national interest to implement such exclusivity. The report highlighted that the flexibility within the provisions of the TRIPS Agreement permitted a country to determine suitable methods for safeguarding test data.[409]

5.48. In *Bayer Corp. v. Union of India*,[410] Bayer approached the Hon'ble Supreme Court to prevent the grant of marketing approval to Cipla for a drug meant to treat renal cell cancer. Bayer argued that the TRIPS Agreement necessitated the establishment of patent linkage to prevent the Drug Controller from approving the marketing of drugs whose patent was not owned by the applicant, Cipla. However, the Delhi High Court had rejected Bayer's argument earlier, citing the 'Bolar' provision in Section 107A of the Indian Patents Act. The Supreme Court sustained the judgment of the Delhi High Court and rejected the applicability of patent linkage in India.[411]

---

[409] Satwant Reddy & Gurdial Singh Sandhu, *Report on Steps to be taken by Government of India in the context of Data Protection Provisions of Article 39.3 of TRIPS Agreement*, Government of India, 38 (2007), *available at*: https://chemicals.gov.in/sites/default/files/Reports/DPBooklet%5B1%5D.pdf. (last visited Feb. 22, 2024).
[410] WP(C) No.7833/2008.
[411] *Id.*

## 6. ECONOMIC ESPIONAGE

6.1. Economic espionage is the act of deliberate acquisition of confidential information from domestic companies and government entities to benefit a foreign State.[412] While the difference between industrial and economic espionage can appear to be quite blurred but there is a key differentiating factor between the two – the actor. While industrial and economic espionage may sometimes overlap, theoretically they are mutually exclusive.[413] In economic espionage, the activities are driven at the behest of a foreign state as opposed to a private entity. Such a foreign government may carry out these activities themselves or through agents by sponsoring the same.[414] In this age of internet and technology, such sensitive information stored in electronic form is rendered even insecure.[415]

6.2. Espionage by no means is a recent phenomenon. It has been carried on since centuries. The British theft of tea production from China,[416] escape of the secret of silk and porcelain from China,[417] theft of the secret design of Cartwright's power loom from England by Francis Cabot Lowell which propelled the industrial revolution in the United States of America, etc. have been some notable examples.[418] In fact, during early phases of the American republic, technology piracy was aggressively encouraged by the

---

[412] Mark E. Danielson, "Economic Espionage: A Framework for a Workable Solution" 10 *Minn. J.L. Sci. & Tech.* 503 (2009), *available at:* https://scholarship.law.umn.edu/mjlst/vol10/iss2/5 (last visited on February 22, 2024).
[413] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 13 (Cambridge University Press, 2005).
[414] Mark E. Danielson, "Economic Espionage: A Framework for a Workable Solution" 10 *Minn. J.L. Sci. & Tech.* 503 (2009), *available at:* https://scholarship.law.umn.edu/mjlst/vol10/iss2/5.
[415] *Id.*
[416] Sarah Rose, "The Great British Tea Heist" *Smithsonian Magazine* (March 9, 2010), *available at:* https://www.smithsonianmag.com/history/the-great-british-tea-heist-9866709/ (last visited on February 22, 2024).
[417] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 12 (Cambridge University Press, 2005).
[418] Christopher Klein, "The Spies Who Launched America's Industrial Revolution" *History* (January 10, 2019), *available at*: https://www.history.com/news/industrial-revolution-spies-europe (last visited on February 22, 2024).

Federal and State Governments and it was this theft that propelled the industrial revolution in America.[419]

6.3. In its traditional conception, espionage meant acquisition of enemy's military secrets by employing spies.[420] History is replete with examples of such espionage, for instance, England's use of spies to uncover the military information that helped them defeat the Spanish Armada in 1588; and the use of spies by the Allies during World War II to defeat the Axis powers.[421] In the present era, the States have a greater role to play in the economy. Further, the competition has shifted slightly and there is a race to develop better technology. Critical areas like computer chips, tele-communication technology such as 6G, space technology, drugs to cure diseases such as cancer etc. are the new focal points of the competition between States to hold power. Currently, the focus of espionage has largely pivoted towards technology, production methods, and proprietary information, which may have both civilian and military applications.[422] Territorial, colonial and military conquests have largely been replaced by an economic war wherein each State tries to outrun the other in order to lead the way forward.[423] The new age arms race is intelligence agencies spending sizeable capital each year towards economic espionage efforts, and counterintelligence agencies spending equally trying to thwart those efforts.[424]

---

[419] Doron S. Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power* xviii (Yale University Press, 2004).

[420] Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 127 (1998), *available at:* https://surface.syr.edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024).

[421] Edwin Fraumann, "Economic Espionage: Security Missions Redefined" 57 *Public Administration Review* 303 (1997), *available at*: https://doi.org/10.2307/977311.

[422] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 19 (Cambridge University Press, 2005).

[423] Interagency OPSEC Support Staff, *IOSS Intelligence Threat Handbook: Economic Espionage* 29 *(2004), available at: https://irp.fas.org/threat/handbook/index.html* (last visited on February 22, 2024).

[424] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 21 (Cambridge University Press, 2005).

6.4. In such a situation, the line between national security and economic security has been blurred and the two are often conflated. In fact, guarding economic security is now a prominent constituent element of ensuring national security.[425] In the post-Cold War era, national security and economic security have come to be intrinsically linked.[426] Further, States are often involved in gathering economic intelligence that they pass on to their domestic companies so as to ensure that their industries and consequently their economies maintain competitive advantage over others.[427] The end result of economic security coming to play a dominant role in defining national security is that economic espionage is the front line of a new world economic war.[428]

6.5. Against the change in nature of espionage, especially when States are no longer just employing spies but corporates and other agents or organisations, there can be great difficulty in ascertaining whether the act is being committed under the sponsorship of a foreign government or not.[429] Myriad electronic as well as physical modes of snooping are employed in order to successfully conduct such espionage. These activities include, but are not limited to, eavesdropping through wiretapping, bugging offices, or capturing cellular telephone conversations; penetrating a computer or any digital system through hacking into the network, hard drive, or software; using direct illegal observation and surreptitious

---

[425] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 8 (Cambridge University Press, 2005).
[426] Edwin Fraumann, "Economic Espionage: Security Missions Redefined" 57 *Public Administration Review* 303 (1997), *available at*: https://doi.org/10.2307/977311.
[427] Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 127 (1998), *available at*: https://surface.syr.edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024); Hedieh Nasheri, *Economic Espionage and Industrial Spying* 17-21 (Cambridge University Press, 2005).
[428] Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 127 (1998), *available at*: https://surface.syr.edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024).
[429] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 13 (Cambridge University Press, 2005).

photography; using surveillance and reconnaissance; trespassing on a competitor's property; stealing proprietary information contained in drawings and documents or on digital storage devices such as pen-drives; hiring a competitor's employee who has the specific knowledge desired; bribing a supplier or employee; planting an agent or 'mole' on the competitor, whose true identity is hidden and whose true task is to compromise key employees, tap into the computer databases, and intercept all communications with the goal of ferreting out confidential research, technologies, and information; conducting false employment interviews with competitor's employees who have knowledge of trade secrets, etc.[430]

6.6. There are a variety of reasons that serve as a stimulus for countries to indulge in economic espionage of other nations: to accelerate modernisation, keep their secret service agents employed, ensure more effective global competition and profitable businesses of their companies, promote national security, etc.[431]

6.7. The impact of economic espionage is predominantly adverse. Economic espionage diminishes the worth of assets in the targeted state[432], disrupts trade between the targeted state and potential buyers[433], discourages innovation, and jeopardizes a business's hard-won competitive edge,

---

[430] Edwin Fraumann, "Economic Espionage: Security Missions Redefined" 57 *Public Administration Review* 304 (1997), *available at*: https://doi.org/10.2307/977311 (last visited on February 22, 2024); Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 135-137 (1998), *available at*: https://surface.syr edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024).

[431] Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 133-135 (1998), *available at*: https://surface.syr.edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024).

[432] Susan W. Brenner & Anthony C. Crescenzi, "State-Sponsored Crime: The Futility of the Economic Espionage Act", *28 Hous. J. Int'l L.* 389, 448-49 (2006).

[433] Peter Schweizer, "The Growth of Economic Espionage: America is Target Number One", *75 Foreign Aff.* 9, 12 (1996).

hindering economic progress. It has the potential to sabotage current business plans, derail profit projections, and be a determining factor in the survival or extinction of a business. The costs of research may need to be recovered through higher prices for customers. Businesses, already facing challenges from lower overseas production costs, may become unviable when considering the additional costs resulting from these thefts. On a broader scale, economic espionage can have a lasting impact by weakening existing military alliances and trade coalitions. Comparisons between economic espionage and warfare have been drawn, as both pose threats to the security and stability of sovereign nations. [434]

6.8. As long as nations persist in engaging in economic espionage activities, the global economy will face significant repercussions. Numerous scholars and journalists have made efforts to gauge the financial impact of economic espionage on society. However, estimating these costs has proven to be challenging, primarily because the international business sector tends to avoid discussing them openly. Companies are generally hesitant to acknowledge substantial financial losses caused by foreign espionage, particularly when their shareholder support is crucial, and the revelation of such losses might lead to a withdrawal of support.[435] Apart from direct monetary setbacks, companies also encounter other consequences arising from economic espionage, including unemployment and the reduction or complete loss of contracts.[436]

---

[434] Mark E. Danielson, "Economic Espionage: A Framework for a Workable Solution" 10 *Minn. J.L. Sci. & Tech.* 507 (2009), *available at:* https://scholarship.law.umn.edu/mjlst/vol10/iss2/5.

[435] See, Anthony Boadle, "Canada Spy-Catcher Says High-Tech Firms Targeted", *The Reuter European Bus. Report* (1994).

[436] John J. Fialka, *War By Other Means: Economic Espionage In America* 6 (W.W. Norton & Company, 1997).

6.9. In an era where power is derived from wealth, there is a growing concern that obtaining economic information could result in the destabilization of international security, transforming current economic rivals into potential military adversaries in the future. Consequently, society lives in constant apprehension of economic espionage. The act of economic espionage has the potential to undermine the motivation to innovate. Individuals are hesitant to generate new ideas if there is a substantial risk that those ideas will be pilfered, utilized, and marketed by competitors. This not only leads to competitors taking credit for ideas rightfully belonging to the original creators but also reaping financial benefits from them, leaving the innovators with nothing. Such a scenario significantly hampers creative endeavours.[437] Economic espionage poses a particular risk to intellectual property rights, which have emerged as the most prized asset in the realm of global business. IPRs, whether acquired legitimately or through theft for financial gain, play a crucial role in today's competitive market economy. Given the escalating pace and cost of technological advancements and the increasing transparency of national borders, IPRs have become a subject of international concern and debate.[438]

6.10. Acknowledging the harm inflicted on U.S. businesses by economic espionage, the Congress enacted the Economic Espionage Act, which came into force on 11th October, 1996.[439] Before its establishment, there was no federal law specifically addressing economic espionage. The said Act criminalizes the copying or controlling of trade secrets with the intent to (i)

---

[437] Karen Sepura, "Economic Espionage: The Front Line of a New World Economic War" 26 *Syracuse Journal of International Law and Commerce* 138 (1998), *available at*: https://surface.syr.edu/cgi/viewcontent.cgi?article=1417&context=jilc#:~:text=Journalist%20and%20business%20consultant%20Sam,CJ%20INT'L%2C%20Mar (last visited on February 22, 2024).
[438] Hedieh Nasheri, *Economic Espionage and Industrial Spying* 10 (Cambridge University Press, 2005).
[439] 18 U.S.C. §§ 1831-1839 (2000).

benefit a foreign government, instrumentality, or agent[440], or (ii) with the intent to convert a trade secret for the economic benefit of a person other than the rightful owner.[441] The first section, Section 1831, prohibits economic espionage, while the second, Section 1832, prohibits industrial espionage. A "trade secret" is generally defined as business information which the owner has taken "reasonable measures" to keep secret and is not "generally known" or "readily ascertainable" to the general public through proper means.[442] Further, the Act prescribes mandatory forfeiture of the fruits of the offence[443] and any property used to facilitate the offence[444] to the U.S. Government. The Act also applies to any conduct occurring outside the United States, provided that he offender must be a citizen of the United States or an organization organized under U.S. laws, or an act in furtherance of the offence must be committed in the United States.[445]

6.11. As regards the United Kingdom, modern national security law in the UK has developed in a series of cycles, prompted by the changing legal landscapes and the emergence of new and different threats to the state and its interests. The recently enacted National Security Act, 2023 (hereinafter, "NSA 2023") replaces the Official Secrets Acts of 1911, 1920 and 1939, but notably leaving the Official Secrets Act of 1989 extant. The NSA 2023 aims at updating, rationalising, and expanding the various offences which the 1911, 1920 and 1939 Acts contained and introducing new rules aimed at the same broad end of countering the threat posed to the UK by the efforts of hostile states and their proxies.[446] The NSA 2023 creates a

---

[440] 18 U.S.C. § 1831.
[441] 18 U.S.C. § 1832.
[442] 18 U.S.C. § 1839(3)(A)-(B).
[443] 18 U.S.C. § 1834(a)(1).
[444] 18 U.S.C. § 1834(a)(2).
[445] 18 U.S.C. § 1837(1)-(2).
[446] P.F. Scott, ""State Threats", Security, and Democracy: The National Security Act 2023" *Legal Studies* 1–17 (2023), *available at*: https://www.cambridge.org/core/journals/legal-studies/article/state-threats-security-and-

number of measures to enable UK law enforcement and intelligence agencies to deter, detect and disrupt the full range of modern-day state threats. The Act updates and introduces offences related to espionage, sabotage, foreign interference and influence, prohibited places, financial property and investigation powers, additional police powers of arrest and detention, and preparatory conduct.[447] A noteworthy feature of the Act is that it covers the Foreign Influence Registration Scheme (FIRS), which is a two-tier scheme that increases transparency of foreign power influence in UK politics and provides greater assurance around the activities of certain foreign powers or entities that are a risk to UK safety or interests.[448]

6.12. In India, the Official Secrets Act, 1923 primarily deals with the protection of sensitive governmental information and enables maintaining the confidentiality of certain categories of information. The Act is designed to safeguard certain specified documents, information, and materials which are sensitive to national security and interests. It prohibits their disclosure to unauthorized individuals or entities. The Act applies to both government officials and civilians.[449]

6.13. The 1923 Act stipulates punishments for spying, interfering with the prohibited areas, invasion of restricted military establishments, sharing secret information without due consent, unauthorized use of uniforms, withholding information and unauthorized falsification of reports and documents.[450] It is pertinent to note that the Act nowhere defines the term

---

democracy-the-national-security-act-2023/F6F6FE6151AA836056DDE36BCC5E94DE (last visited on February 25, 2023).

[447] Ministry of Defence, Industry Security Notice Number 2024/01 (January 31, 2024), *available at*: https://assets.publishing.service.gov.uk/media/65ba6951c75d300012ca0ff3/ISN_2024-01_National_Security_Act_2023-O.pdf.

[448] *Id.*

[449] The Official Secrets Act, 1923 (Act 19 of 1923), s. 1.

[450] *Id*, ss. 3, 4, 5, 6, 7.

"secret". As a result, the authorities can classify any document as a 'secret document'. In 1989, a Committee was set-up by the Government in order to review certain ambiguities contained in the Official Secrets Act, 1923, wherein a major task was to define the term 'official secret'. However, the said Committee could not provide a conclusive definition for the same.[451] Section 5 of the Officials Secrets Act, 1923 punishes both the person communicating the information, and the person receiving the information. Additionally, it also punishes the one who retains the same or who fails to take reasonable care of the secret.

6.14. Enacted during the colonial era, the 1923 Act may not fully address contemporary challenges relating to information security and intellectual property rights. The Act revolves around the terms 'secret', 'prohibited place' and 'national security', which primarily covers incidents related to defence, army, arsenal, military, navy or air establishments. Thus, what this Act basically encompasses within its ambit are instances of political espionage, which may not comprehensively include other categories of espionage such as economic espionage. The 1923 Act predominantly focuses on protecting government information and does not adequately address the protection of trade secrets or confidential business information in the private sector. This limitation leaves gaps in legal protections for businesses against misappropriation of valuable proprietary information by foreign entities.

6.15. Instances of intellectual property theft and infringement, including the misappropriation of trade secrets, have been reported across various industries in India. While the existing intellectual property laws provide

[451] R. Ramachandran, "Public access to Indian geographical data", 79 *Current Science Association* 459 (2000).

some level of protection for proprietary information, the enforcement of these laws and the prosecution of offenders can be challenging. The Official Secrets Act, 1923 may not always be suitable for addressing cases of economic espionage involving theft or misuse of trade secrets and other intellectual property by non-state actors or private entities as well as foreign governments, highlighting the need for specialized legal mechanisms to safeguard intellectual property rights. There are other important organisations which lie in the vulnerable ambit of data secrecy and its protection. Several scientists have highlighted the importance of protecting data secrecy and the threat is to such an extent that it has been said that our "country's space programme, or for that matter other strategic programmes, may no longer be immune to outside preferences."[452]

6.16. There is no doubt that a lot of Indian companies are at a threat of loss of data or trade secrets. A study by the Associated Chambers of Commerce and Industry of India (ASSOCHAM) stated that more than a third of the companies surveyed across different sectors were involved in some form of espionage to gain advantage over competitors. Nearly 80 percent of the chief executives spoken to had used or were using detective agencies and surveillance systems to spy on current and former employees."[453]

6.17. An annual risk survey conducted by the Federation of Indian Chambers of Commerce and Industry (FICCI) in 2014 stated that 'business espionage' was tagged as the ninth biggest threat to Indian companies. It further stated that only 15-20 percent of corporate espionage cases are actually detected. Another survey was conducted by KPMG, wherein it was revealed that

---

[452] S. Dhawan, T. N. Seshan, *et.al.*, "ISRO 'Espionage Case'"32 *Economic and Political Weekly* 554 (1997).

[453] Pranjoy Guha Thakurta, "Booming business of corporate espionage", *The Hindu Business Line*, Jan. 24, 2018.

losses incurred due to economic espionage are as high as 13%. It was also stated that due to the inherent nature of corporate espionage, there is no reporting leading to absence of cases in this regard.[454]

6.18. The aforesaid studies and surveys illustrate the complex challenges associated with economic espionage in India and the limitations of the Official Secrets Act, 1923 in effectively addressing modern threats to all forms of intellectual property and sensitive business information. There is a need to modernize the legislation to align with current technological advancements and global developments for protecting sensitive information, specifically related to intellectual property. A separate dedicated law on economic espionage would provide businesses and other important institutions with the requisite legal framework to protect their confidential information from unauthorized use or disclosure, especially by any foreign entity.

[454] Shilpa Phandis, Mini Joseph Tejaswi, "Corporate Espionage on the rise in India", *The Economic Times*, Sep. 24, 2010.

## 7. CONSULTATIONS HELD BY THE COMMISSION

7.1. Conscious of the possible and wide-ranging impact of a law on trade secrets, the Commission thought it fit to engage with a wide range of stake-holders. Consequently, the Commission held broad consultative meetings with members from the judiciary, academia, domain experts, industry as well as the Government. These deliberations brought to attention multiple aspects and concerns which were instrumental in shaping the Commission's views on the issue. During consultation meetings the Commission posed the same broad questions to the invitees, for instance, if and how the prevailing position in India had proved to be inadequate in protecting trade secrets; whether India should enact a specific law on trade secrets and what should be the contours and content of such law; and should any limitations in the nature of government use or compulsory licensing be introduced in such a law etc. During the meetings other ancillary and related issues that came up were also addressed and discussed.

### *A. Judicial Perspective*

7.2. **Hon'ble Ms. Justice Prathiba M. Singh** was part of the IPD Committee which was instrumental in establishing the IP Division at the High Court of Delhi in 2021 post the dissolution of the Intellectual Property Appellate Board (IPAB). She was also a member of the IPR Think Tank that was tasked with drafting India's first "National IPR Policy" in 2015. In light of her extensive expertise and contributions to the field of IPR, the Commission invited her to express her understanding and views on the subject of enacting a trade secret legislation in India. The following important points came up during the discussion: