Regulation of Corporate Espionage: Legislative and Judicial Approaches

Dr. Manjinder Gulyani and Dr. Navninderjit Singh

Abstract- Economic offences may not seem as grave as other offences. Yet they have serious consequences and may jeopardise various rights. So, it is very important to prevent these offences and to provide remedies in case of any transgressions. When the corporators compete with their rivals, they sometimes intrude in the space they are not allowed to. They breach and infringe the ethical and legal limits both physically and in the cyberspace. Although, they can collect the Competitive Intelligence of the competitors' strategies and their products. But they can't do it using unfair and illegal means. There is a very fine ethical line between Competitive Intelligence and Corporate Espionage. Crossing that fine line might end up in civil or/and criminal liability. So, the paper basically concentrates upon the concept of Corporate Espionage.

Keywords: Corporate Espionage, Competitive Intelligence, Liability, Regulation.

I. INTRODUCTION

It is a normal tendency to be curious about one's rivals and competitors. People use various techniques to stay updated regarding the dynamics of the other companies. Nowadays, they use internet to see what is going on with their rival companies. There are apparently many modes and ways to fetch that kind of information. Since we are moving towards an information driven society where information is traded to keep tabs on the rival's information security has become very significant. According to the experts, knowledge theft is very alarmingly increasing and it's a kind of enemy that is not easy to combat.

The corporations keep collecting the information of the products and launches of their adversaries. This collection of information is termed as competitive intelligence. And with the help of internet, the exercise becomes effortless. Initially, the countries or corporate needed physical access, money to bribe and various dangerous meeting locations to accomplish that task. Rothke, Ben. (2001) observes that thanks to internet, nowadays, many unpredicted and misconfigured networks make the job of spying so easy that the spies can do it sitting within the four walls of their home.

The information, the rivals are generally interested in, is of commonly in the form of patterns, designs, inventions, manuscripts, production details financial details or marketing strategies.

Dr. Manjinder Gulyani, Associate Professor, Institute of Law, Kurukshetra University, Kurukshetra, Haryana, India

Navninderjit Singh, Assistant Professor, Punjabi University Patiala-147002, Punjab, India

As per the Budiono, Gatut & L. Nyoman, Sawitri Ni. (2017) the concept of transparency and openness with the customers, makes it imperative to disperse more information and make it easy for the competitors to collect any data. The companies that cause to commit espionage generally require sensitive information owned by a rival company. Two preconditions that are required to commit such act are- opportunity and incentive.

II. MERITS OF CORPORATE ESPIONAGE

Some experts have identified some positive effects of Corporate Espionage, which may be listed as under:

- The formulation of new products.
- Improvement in product quality and design.
- Innovation to stay relevant in the market.

III. DEMERITS OF CORPORATE ESPIONAGE

It is very expensive to engage in constant surveillance. According to the study of Budiono, Gatut& L. Nyoman, Sawitri Ni. (2017) in Canada it has been reported that billions are spent on corporate espionage.

It is morally and ethically wrong to divulge the secrets of the employer.

Companies and their employees are at constant risk and vulnerable at times.

There are chances of loss of market share.

The loss of business is very obvious effect of corporate espionage.

The profits are also affected prejudicially in the process.

Further, Rothke, Ben. (2001) observes that the balance of trade is weakened.

IV. DEFINITION AND MODES OF COMPETITIVE INTELLIGENCE (ETHICAL CORPORATE ESPIONAGE)

The collection of information from legal sources obtained ethically forms competitive intelligence. The main sources of competitive intelligence are websites, news archives, marketing brochures, tradeshows and conferences etc. The modes of collection of competitive intelligence are discussed hereunder:

In accordance with Winkler, Ira S. (1997) the researchers, and sometimes the experts, are hired to participate in launch events, conferences or tradeshows to understand the know-how or to analyse the marketing strategies.

- Further, the targeted companies are acquired along with the technology. So, it is a legal way of acquiring technological information to end the competition.
- Winkler, Ira S. (1997) observes that the corporations that are working in foreign countries they employ natives and train them. Then sometimes the branch in particular country is closed and the employees with confidential information join another corporation. Their experience and knowledge are used by the rivals.
- During the joint ventures also, the information is required to be shared. Sometimes the companies aspiring to enter the foreign market are lured to share their technology as a part of joint venture as indicated in a study by Winkler, Ira S. (1997).
- As indicated earlier, too many sources of open source information knowingly or unknowingly are transmitted to the competitors. These may include newspaper articles, annual reports, court papers and patent filings. It is found that many review patent filings are by foreign nationals and third party research firms. Thus, all plethora of information reaches the hands of the rivals.
- Many ex-employees of rivals are hired by the competitors. They don't intend to reveal any confidential information. Budiono, Gatut & L. Nyoman, Sawitri Ni. (2017) consider that the transfer of the knowledge is inevitable in their present position. They use their previously acquired knowledge in many ways and hence their knowledge is shared.
- In addition to it, social media also provides ample chances to collect information of the competitors ethically and legally. The consumer sentiments and opinions are available on blogs, Facebook pages, Twitter handles etc. Discussion blogs also provide valuable insights. The promotional strategies are scattered all over the social media including Instagram, FB and Twitter etc. The celebrity pages and influencers' blogs/pages publicly display the promotional strategies.
- As per Dey, Lipika & Haque, Sk & Khurdiya, Arpit & Shroff, Gautam (2011) many major airlines are fixing their prices in accordance with the information which they obtained from their competitors from their websites.
- Google alerts also help to provide the updates. Although this information is raw and a lot of noise in terms of unnecessary details is found. But as discussed by Dey, Lipika & Haque, Sk & Khurdiya, Arpit & Shroff, Gautam (2011) the experts minimize that noise by using different algorithms.

V. MODES AND METHODS OF CORPORATE ESPIONAGE

Corporate Espionage is committed when the sensitive information of a company is obtained illegally. Some of the popular modes of Corporate Espionage are discussed hereunder:

- Technical security is not taken up properly as a part of the project. Sometimes, the project needs special kind of security protocols. But it is left for the security team and they just follow the regular security measures which leave the information as vulnerable.
- Firewalls etc. mechanisms work well for the cyber-attacks, but most of the times insiders compromise the availability of the confidential information. Some corporations get their people recruited in their competitors' organization. These people are employed in the targeted company or with someone who has access to the company.
- Espionage is strategic and includes physical, personal, operational and technical security breach. Industrial spies know how to bypass any strong part of the security program to attack an organization at its weak point.
- Industrial spies access various sources of the unprotected information, like discarded copies, copying machines and the unprotected computers mostly.
- Computer hacking, phone tapping or cryptanalysis are some ways through which the sensitive information is collected for the rivals.

It is not necessary for the spy to be appointed at a senior position. As analysed by Winkler, Ira S. (1997) sometimes, they may obtain an odd job of a janitor or something and not much background check is done in such cases. Resultantly, the security is compromised.

The senior executives also report that they travel for work. Then their hotel rooms are bugged or surveillance is done and their phones are tapped.

The information is gathered by accessing places unnoticed by the data owner. As one of the studies of Budiono, Gatut & L. Nyoman, Sawitri Ni. (2017), the incentive might be gifts, money, sex, seduction or threats in extreme cases.

VI. REGULATION OF CORPORATE ESPIONAGE

It is not easy to detect corporate espionage. Even if it is detected, it is not easy to prove. Further, in many countries it is a civil wrong only. In USA, however, the special legislation was enacted in 1996 with the title Economic Espionage Act, 1996. Earlier, the action was through IPR's like misappropriation of trade secrets or as an unfair trade practice. But this Statute made corporate espionage as a Federal offence.

The salient features of the legislation are-

If a person uses a trade secret for his benefit, or for others' benefit knowingly or intentionally, it is a federal crime.

If someone receives, buys or possesses the stolen trade secret information knowingly, it is an offence.

It defines trade secrets very widely and includes forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether how stored or compiled, memorised physically, electronically, graphically, photographically, or in writing.

In India, However, no special legislation has been enacted so far. As per the NCRB (National Crime Record Bureau) report of 2015, most of the cyber-crimes were registered for greed/financial gain accounting for 33.3% (3,855 out of 11,592 cases) followed by fraud/illegal gain (9.6%) (1,119 cases).

The wrong of corporate espionage is dealt with under a variety
of laws. The Copyright law protects a few breaches, but it is very difficult to prove. In the case of **Genetics India Private Limited V. Shailender Sinha** 2011(47) PTC 494 the court observed that the precondition for institution of such suit and seeking relief is that the information was confidential. Further, if the information is not unique and novel, it is just a compilation of existing techniques or materials freely available, and hence the relief can't be given in such cases.

Then there are some provisions of Indian Penal Code that may be invoked to give rise to the criminal liability. The provisions for criminal breach of trust, fraud and theft of secret information may be invoked in such circumstances.

Finally, the Information Technology Act, 2000 carries some provisions to invoke liability in case of acquiring confidential information. Section 72-A is, inter alia, most significant provision in this behalf.

Under **Section 43** of the IT Act, a person without the permission of owner or the person in charge. If-

- Accesses the system or network.
- Downloads, copies or extracts data.
- Introduces computer containment or virus.
- Damages computer common data or programs.
- Disrupts the computer or network.
- Denies access to computer, system or network.
- Charges the services availed by tampering with the computer, system or network.
- Destroys, conceals, destroys or alters information.
- Steals, conceals, destroys or causes the same.

is liable to pay damages by way of compensation to the person affected.

Thus, this provision is very significant in terms of regulation, prevention, and remedy of espionage. However, it is pertinent to mention that this provision does not make any of the acts mentioned above as a penal wrong. It only provides for damages as a remedy. But the penal provisions for these acts are mentioned in **Section 66**, where the imprisonment up to three years and fine up to five Lakh rupees have been mentioned.

Section 65 provides a penalty by way of imprisonment of three years and fine up to two lakh rupees if a person tempers with computer source documents. It penalises the act of concealments, destruction or alteration of computer source code.

If a person receives stolen computer resources or communication device knowingly, the punishment of imprisonment up to three years with a fine up to one lakh rupees may be imposed under **section 66-B** of the Act.

If someone tries to steal identity through electronic signature, password, etc., the punishment of imprisonment up to three years and fine up to one Lakh rupees has been prescribed under Section **66-C**. So, if a spy tries to steal a rival's information through stolen identity, penalty under Section 66-C may be imposed.

As per **section 67-C**, the intermediaries are also supposed to be cautious about safety of the information. The lapse may attract imprisonment up to three years and fine as well.

For the investigation of an offence, interalia, the government is authorised under **Section 69** to order the interception, monitor or decryption of any information generated, transmitted or received in any computer resource. **Section 69-B** empowers the central government to analyse and to prevent. Any intrusion or spread of computer containment.

And then the most significant provision that might prove crucial in regard to curb the menace of corporate or cyber espionage is **section 72-A** which provides punishment for disclosure of information in breach of lawful contract. The punishment includes imprisonment up to three years and fine up to five Lakh rupees.

Further, **Section 74** penalises knowingly publishing, for fraudulent purposes, any information with an imprisonment of up to two years and fine up to one lakh rupees.

Under **Section 76**, the computer, computer system or drives, etc. obtained illegally may be confiscated.

Section 77 further makes it clear that compensation, penalty or confiscation will not interfere with any penalty etc. in any other law. So, it cannot be claimed that penalty may be imposed only under IT act and not under IPC concurrently.

The abetment of any of these offences is punishable with same penalty as the offence itself under **Section 84-B** and for attempt to commit any such offence may be punishable with half of the longest term of imprisonment and fine or both under **Section 85-C**. The main defence for these offences maybe the use of due diligence or taking any action in good faith.

Rule 25 (4) of IT (procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009 direct to keep strict confidentiality in respect of any direction for interception, monitoring or decryption issued by the competent authority under the Act. The intermediaries or its employees are prohibited from using the contents of any information which has been intercepted, monitored or decrypted.

Rule 5 of IT (procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009 also mandates the same thing.

VII. IMPORTANT CASE STUDIES

As per the study of Ashwini. Kumar, Shubham (June 2020), in **Unilever v. Proctor and Gamble** the matter was mutually resolved where P&G admitted in 2001 to launch a spy mission for their competitor Unilever. Interestingly, they admitted to go through the Unilever's trash in search of documents.

In **Opal v. Volkswagen** eightexecutives of In **Opel vs. Volkswagen** eight executives of Opel, including the chief of production, moved to Volkswagen with confidential information. After a long litigation as discussed by Ashwini. Kumar, Shubham. (June 2020), Volkswagen agreed to pay 100 million dollars to GM Motors, the parent company of Opel and an order of 1 billion worth car parts. Thus, the matter was resolved.

In the matter of **IBM V. Hitachi**, according to Ashwini Kumar, Shubham (June 2020), Hitachi agreed to

pay 300 million dollars to IBM for the possession of inside information through the IBM's workbooks.

According to the Rothke, Ben. (2001). the **Russian supersonic plane** allegedly looks similar to a plain named Concorde by the Britain and France. This aircraft named Konkordski is outcome of industrial espionage if we believe the experts' view.

Then there is a landmark case of conflict between **General Motors and Volkswagen**. A former General Motors employee, Jose Lopez, had stolen various designs and trade secrets who was lured by Volkswagen. As a study of Rothke, Ben. (2001). General motor tried to Sue Volkswagen in USA but the remedy was only as civil action. Lopez further sold the secrets to some European firms. The German government finally took criminal action against him.

Another interesting cases as discussed by Budiono, Gatut & L. Nyoman, Sawitri Ni. (2017) is that of when Britain tried to enter into the business of tea in 1848, which was monopolised by China. So, the East India Company hired a botanist and one Robert Fortune, who smuggled the seeds and the related traditional knowledge to India and China's monopoly was thus compromised.

In another instance, as reported by Freeh Louis.(1998) was regarding new **Gillette Razor Design.** In this case Davis, who was assigned as the lead process control engineer for designing new shaving system, was removed from the position later. Then, allegedly, he sent confidential drawings to various competitors, including Warner, Lambert, and others.

Further, the case of **Eastman Kodak trade secrets case** is no less interesting as per the report of Freeh Louis.(1998). In this case, a retired employee named Harold C. Warder established his own consulting company after retirement. He allegedly had business with 60 other Kodak ex-employees who were consulting for competitors. He took away with him many drawings, plans, manuals, etc. He pled guilty and was sentence to one year of imprisonment and three months of home confinement and also fine of $30,000.

Then in the case of **Avery Dennison v. Four Pillars Adhesive Products**, the father and daughter based in Taiwan were convicted for theft of highly sensitive and valuable proprietary information and data of over a period of eight years from 1989 to 1997. As per Freeh Louis (1998), the penalty of $1,50,000 and $1,60,000 was imposed on them.

In **Awadhesh Kumar Paras Nath Pathak versus State of Maharashtra and others,** Criminal application number 2562 of 2019 (a case pending in Mumbai High Court) applicant who was technical manager of Cosmos Film Limited Company for almost 22 years, resigned in 2018, then got employed in Jindal Poly Films Limited. It was alleged that when the applicant left the firm, he returned the company's laptop. But he took huge information which was stored in the laptop in a folder named as personal data in his pen drive. Due to many other complaints, respondent number 2 in this case, checked the folder and it was found that it contained enormous data of the company. It was contended by applicants that IT Act being a special legislation has overriding effect to cover the criminal acts mentioned under IPC. So, accordingly, the matter was referred to the larger bench to resolve the following questions:

- Whether Section 43 read with Section 66 of IT act covers the cases where the person-in-charge of computer was induced to give information by cheating.
- Whether Section 72 covers the ingredients of Section 406, 408, 409 IPC, where the information (electronic) is misappropriated.
- Whether the criminal acts with common intention are covered under Section 43 and 72 of IT Act.

This matter is pending before Court, but in my opinion, the offences above mentioned are distinct offences and the applicants may be charged both under IT Act an IPC.

VIII. SUGGESTIONS

As it is evident from the above mentioned discussion that the wrong of corporate espionage is very complex. So here are some suggestions to deal with it:

1. The first and foremost thing is to identify what kind of information is to be protected and thus there is a need to prioritize the same because not every information needs to be protected.
2. Very sensitive kind of information must be encrypted and may be hand carried.
3. The passwords must be changed frequently.
4. The written material must be shredded after use.
5. All strategies must be removed from boards etc. after the meetings.
6. Background checks of all employees is a must even the temporary staff.
7. The persons who have proprietary information, non disclosure agreements may be get signed from them.
8. The employees' complaints and problems must be taken seriously and resolved amicably.
9. In addition to it, physical security of workplace is very important to avoid any kind of infiltrations.
10. The temporary staff or consultants must be chosen carefully.
11. When a firm is experiencing losses, security budget is also cut. This makes the firm even more vulnerable. So, security must be taken as priority at all times.
12. As discussed by Rothke, Ben. (2001), security must be made an integral part of any design.
13. The security has to be holistic. All kinds of aspects like technical, operational, physical and personnel need to be taken care of.
14. Policies on restriction on use of open communication lines, internet and phone can prevent the compromising of the information.
15. Employees must be trained as to how and to whom the information is to be disclosed.
16. All the employees carrying sensitive information must wear access badges all the time.
17. Most importantly, statutory changes are also necessitated to deal with this offence more effectively. In that behalf it is suggested that a separate legislation may be enacted

with a definition of corporate espionage as a criminal wrong.

18. Further, it needs to be understood that the procedural law in case of this offence has to be different. Present procedural law including the Information Technology Act 2000 (India) is not sufficient to address the problems associated with this offence because the modus operandi in such cases is different than usual and the evidentiary weight required in present criminal jurisprudence is generally not available in the case of espionage.

IX. CONCLUSION

It is time for commercial information security professionals to realise that information security is more than just computer security. A comprehensive security programme, as indicated in the suggestions, which includes all security disciplines is the only effective countermeasure to a strategic industrial espionage attack.

REFERENCES

[1] Rothke, Ben. (2001). Corporate Espionage and What Can Be Done to Prevent It. *Information Systems Security*. *10*. 1-7. 10.1201/1086/43315.10.5.20011101/31716.3. https://doi.org/10.1201/1086/43315.10.5.20011101/31716.3

[2] Winkler, Ira S. Case Study of Industrial Espionage through Social Engineering. *National Computer Security Association* https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.115&rep=rep1&type=pdf

[3] Budiono, Gatut& L. Nyoman, Sawitri Ni. (2017). Strategic Business Espionage: An Ethics and Business Practices to Gain Opportunity or Community Problems. *Studies in Business and Economics. No. 12(1)* Doi 10.1515/Sbe-2017-0003 https://doi.org/10.1515/sbe-2017-0003

[4] Dey, Lipika& Haque, Sk&Khurdiya, Arpit & Shroff, Gautam. (2011). Acquiring competitive intelligence from social media. Proceedings of the 2011 Joint Workshop on Multilingual OCR and Analytics for Noisy Unstructured Text Data. 10.1145/2034617.2034621. https://doi.org/10.1515/sbe-2017-0003

[5] Freeh Louis.(1998) Notable Industrial Espionage Cases, https://www.wrc.noaa.gov/wrso/security_guide/industry.htm

[6] Ashwini. Kumar, Shubham. (June 2020) Astonishing Corporate Espionage Case Studies. *Startuptalky*

[7] Button, M. (2020). Editorial: economic and industrial espionage. *Security Journal*, *33*(1), 1-5. https://doi.org/10.1057/s41284-019-00195-5

[8] NCRB (2015). Cyber Crimes. Chapter 18. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Chapter%2018-15.11.16_2015.pdf

[9] Michael. (April 23, 2018). Differentiating Competitive Intelligence and Corporate Espionage. *National Business Investigations, Inc*.

[10] Kurian Anu& Sharma Pallavi.(2015) Corporate Espionage or Competitive Intelligence?*People Matters. https://www.peoplematters.in/article/leadership/corporate-espionage-or-competitive-intelligence-10995*

[11] Section 43 of IT Act- [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network,–

(a) accesses or secures access to such computer, computer system or computer network 7[or computer resource];

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceal, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;]

[12] [he shall be liable to pay damages by way of compensation to the person so affected.]

[13] Section 65 of IT Act- Tampering with computer source documents.–Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

[14] *Explanation.*–For the purposes of this section, ―computer source code‖ means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

[15] Section 66 of IT Act Computer related offences.–If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. Explanation.–For the purposes of this section,–

(a) the word ―dishonestly shall have the meaning assigned to it in section 24 of the Indian Penal Code (45 of 1860);

(b) the word ―fraudulently shall have the meaning assigned to it in section 25 of the Indian Penal Code (45 of 1860).

[16] 14. Section 66B of IT Act. Punishment for dishonestly receiving stolen computer resource or communication device.–Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

[17] 15. Section 66 C of IT Act. Punishment for identity theft.–Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

[18] 16. Section 66 D of IT Act. Punishment for cheating by personation by using computer resource.–Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

[19] 17. Section 67C of IT Act- Preservation and retention of information by intermediaries.–(*1*) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

[20] (*2*) any intermediary who intentionally or knowingly contravenes the provisions of sub-section (*1*) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.]

[21] Section 72 of IT Act- Penalty for Breach of confidentiality and privacy.–Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register,

correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

[22] Section 72 A of IT Act- Punishment for disclosure of information in breach of lawful contract.–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

[23] Section 84 C of IT Act- Punishment for attempt to commit offences.–Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence, or with both.