

Hacking, Data Theft and Corporate Espionage: What Indian Law Says

Introduction

The fast development of technology and digital infrastructure has changed the landscape of business today. Nowadays businesses hold large amounts of sensitive information digitally, for example, trade secrets, client lists, financial statements, plans for new products, source codes and strategic business data. Digitization has not only led to progress and new ideas but also to hazardous cyber security. Acts like hacking, stealing data, or spying on companies have become very common not only in India but worldwide. Besides financial damages, these crimes also lead to loss of reputation, customers' trust and even jeopardize national security.

In India, the major legislations that try to tackle cyber crimes are the Information Technology Act, 2000 together with the Indian Penal Code, 1860 and other business laws¹. Even if Indian statutes don't have a term "corporate espionage", the judiciary and law enforcement are increasingly viewing illegal access to confidential business information as a significant economic crime. Legally, as India is gearing up for an AI-led and digital e-economy, regulation of cybercrime is becoming a top priority².

Understanding Hacking under Indian Law

The word hacking is usually tied to the unauthorized entry into computers, networks, or digital devices to stealing, tampering, destroying, or using the information illegally. Hackers may want to harm individuals, companies, banks, or government institutions. Some common reasons why people resort to hacking are making money, competing with other businesses, spying on political activities, settling scores, or cyber terrorism.

Hacking in India is regulated by several sections from the Information Technology Act, 2000³. Section 43 of the act specifies what actions would amount to civil liability⁴. These include - a person who accesses a computer system without permission, downloads data, introduces viruses, or damages the system. Compensation can be claimed by the injured party for damages suffered from a breach in security.

Section 66 of the IT Act makes the unauthorized acts referred to in Section 43 when done intentionally or dishonestly a criminal offense⁵. If found guilty under this section, the offender may be sentenced to jail and fined. Indian courts have broadly interpreted these statutory offenses to cover unauthorized access, system manipulation, identity theft, and other malicious cyber activities.

The very first and most important hacking case in India was Suhas Katti case (*State of Tamil Nadu v. Suhas Katti, 2004*)⁶, which is considered as India's first conviction under the IT Act. The defendant was found guilty of defamation and obscenity on the internet through fake identities. This case mostly dealt with cyber harassment but at the same time it was a landmark in the development of cyber laws in India. Also the court's reliance on electronic evidence and digital investigations was the first time the judicial confidence was established.

¹ Government of India. (2000). *Information Technology Act, 2000*. Ministry of Electronics and Information Technology, Government of India; Government of India. (1860). *Indian Penal Code, 1860*. Ministry of Law and Justice, Government of India.

² NITI Aayog. (2021). Towards responsible AI for all. Government of India.

³ Government of India. (2000). *Information Technology Act, 2000*. Ministry of Electronics and Information Technology, Government of India.

⁴ Government of India. (2000). *Information Technology Act, 2000*, Section 43. Ministry of Electronics and Information Technology, Government of India.

⁵ Government of India. (2000). *Information Technology Act, 2000*, Section 66. Ministry of Electronics and Information Technology, Government of India.

⁶ *State of Tamil Nadu v. Suhas Katti*, C.C. No. 4680 of 2004.

Another landmark case will be the Shreya Singhal case (*Shreya Singhal v. Union of India, 2015*)⁷, wherein the Indian Supreme Court invalidated Section 66A of the IT Act since it imposed unreasonable restrictions on freedom of speech guaranteed under Article 19(1)(a) of the Constitution. It was a landmark case, which gave direction to the interpretation of cyber laws and ensured that the regulation of digital offences is not draconian and considers the constitutional rights of the citizens.

Data Theft and Unauthorized Access to Information

Data theft refers to the unauthorized copying, transfer, downloading, or misuse of electronic information belonging to another person or organization. Unlike traditional theft, the original information often remains with the owner while a copy is secretly taken. Nevertheless, the economic damage caused by data theft can be enormous.

Companies today rely heavily on confidential digital information such as:

- customer databases,
- manufacturing processes,
- pricing strategies,
- financial records,
- trade secrets,
- and proprietary software.

When such information is stolen, competitors may gain unfair commercial advantages, leading to serious financial and reputational harm.

While Indian legislation does not offer a clear statutory definition of **Data Theft**, a number of sections under the IT Act deal with unauthorized access and misuse of electronic information. **Section 72 of the IT Act** regards as an offence breach of confidentiality and privacy by persons who

⁷ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

gain access to electronic information through lawful authority but disclose it without consent⁸. Section 72A goes to the length of punishing the disclosure of personal information in violation of lawful contracts⁹.

Increasingly, Indian courts have been welcoming the idea that confidential business data is a type of asset having commercial value and, because of this, is entitled to protection. In *American Express Bank Ltd. v. Priya Puri* (2006), the court of law in Delhi dealt with matters concerned with confidential customer data and employment relations¹⁰. It recognized that although generally one cannot restrain a person from his or her professional skills Still legally confidential business information and trade secrets may be the subject of protection.

Same here, in *Diljeet Titus v. Alfred A. Adebare* (2006)¹¹, the court forbade two former employees who were also the defendants in the suit from launching any kind of misuse of databases of confidential clients and proprietary information that they had access to during the time of their employment. The ruling was a further support to the idea that it is feasible to safeguard electronic business information by way of injunctions and contractual obligations.

Recent cases originating from Pune and other technology centers have exemplified in a striking manner the rising concern about insider data theft. Per several published reports, the ex-employees were involved in the unauthorized transfer of confidential business information to competitor companies by the use of personal email accounts and external storage devices¹². At a time when physical security measures and technological defenses are being improved, insider threats have rendered themselves as one of the very significant worries not only for the security of the modern business enterprises.

Corporate Espionage and Insider Threats

Industrial espionage, more often known as corporate espionage, involves illegal or unethical ways of obtaining private business information for purposes of commercial gains. In contrast to general hacking, corporate espionage activities are typically well-planned and orchestrated. Competitor firms, ex-staff, consultants or insiders may end up pilfering trade secrets, production blueprints, client details and research information to seek out competitive advantages.

In fact, industrial espionage has moved to higher levels of sophistication with the aid of cloud computing, AI, and remote work setups. Workers who are given legitimate access to the company systems may go through the process of secretly duplicating sensitive files and delivering them to the rivals. Such types of insider threat are often not easily discovered since the person accidentally already has the authorized access credentials.

Indian law presently does not contain a separate statute exclusively governing trade secrets or corporate espionage. However, remedies are available through:

- the IT Act,
- contract law,

⁸ Government of India. (2000). *Information Technology Act, 2000*, Section 72. Ministry of Electronics and Information Technology, Government of India.

⁹ Government of India. (2000). *Information Technology Act, 2000*, Section 72A. Ministry of Electronics and Information Technology, Government of India.

¹⁰ *American Express Bank Ltd. v. Priya Puri*, 2006 SCC OnLine Del 638.

¹¹ *Diljeet Titus v. Alfred A. Adebare*, 2006 SCC OnLine Del 1368.

¹² Hindustan Times. (2023). Former employee booked for stealing confidential company data in Pune.

- intellectual property law,
- breach of confidentiality claims,
- and criminal law provisions relating to cheating and criminal breach of trust.

In *Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd.* (2003)¹³, the court acknowledged the necessity of safeguarding confidential business information and ruled that illegal use of secret ideas and materials can mean legal responsibility. Courts have regularly issued injunctions prohibiting ex-employees from revealing trade secrets or obtaining confidential business information. The increase of corporate spying has caused worries in the areas of national security and strategic industries. Technology companies, defence contractors, pharmaceutical companies, and financial institutions continue to be at great risk because of the very high commercial value of their data.

Role of Cyber Crime Cells and Digital Investigations

Indian law enforcement agencies have established specialized cybercrime units in major cities such as Mumbai, Bengaluru, Hyderabad, Delhi, and Pune to investigate cyber offences. These units examine:

- server logs,
- hard drives,
- cloud storage,
- metadata,
- email records,
- and digital communication trails.

Because electronic evidence can be manipulated or wiped easily, digital forensics are key in fighting cybercrime. As a result, courts are progressively according to forensic experts to prove the genuineness of electronic records as per Indian Evidence Act, 1872.¹⁴

It was in *Anvar P.V. v. P.K. Basheer* (2014)¹⁵ that the Supreme Court of India ruled that electronic evidence has to fulfil the requirements of Section 65B of the Evidence Act to be accepted by the courts, which is in fact a major step towards the clarification of the admissibility of electronic evidence.

Legal Challenges and Emerging Concerns

Even with the presence of laws related to cyberspace, India continues to experience many difficulties in imposing the rules on hacking and data theft efficiently. The Information Technology Act was initiated in the year 2000. It was a time when advanced AI, cloud computing, ransomware, and highly sophisticated cyber espionage were still to come. So, many of today's cyber threats are in the legal grey areas.

The absence of a specific law on trade secrets in India is another big issue. India does not have a law on trade secrets the way some foreign countries do. In fact, India mostly depends on the contractual agreements and equitable principles for protecting confidential information. This means that there is a

¹³ *Zee Telefilms Ltd. v. Sundial Communications Pvt. Ltd.*, 2003 (27) PTC 457 (Bom).

¹⁴ Government of India. (1872). *Indian Evidence Act, 1872*, Section 65B. Ministry of Law and Justice, Government of India.

¹⁵ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.

lack of clarity about how much protection proprietary business data can get.

On top of that, Artificial Intelligence has brought up new vulnerabilities of cybersecurity. For example, it is possible for AI systems to automatically make phishing emails, create digitally convincing fakes of real emails, mimic voices, and very quickly analyze stolen databases. And, this situation is being aggravated by the increase in remote work and cloud-based infrastructure usage, which is leading to the cyber criminals having more opportunities to launch attacks.

Conclusion

Among other issues that pose a grave threat to cyber law in India, hacking, data theft and corporate espionage can be cited. As the role of technology and digital technology continues to become more pronounced, the protection of confidential electronic information becomes an urgent issue for both legal and commercial reasons. Under the laws of India, especially those contained in the Information Technology Act, 2000, provision is made for the handling of issues pertaining to unlawful access, misuse of data and cyber crimes. Courts in India have also widened legal provisions regarding confidentiality by making use of injunctions.

Nevertheless, technological development has revealed various shortcomings in the law. The complex nature of cybercrime, insider attack and AI-assisted attacks indicate the urgent need for improved governance of cybersecurity, compliance systems in corporations, legislations regarding trade secrets and advanced investigative means in the digital world.

Cybersecurity has become a serious legal, economic and governance challenge and hence calls for the introduction of sound corporate controls, sensitization among employees, confidentiality measures and prompt legal responses.