

Regulations in India

India has a detailed and well-defined legal system in place. The Indian legal system is based on English common law. The Indian judicial system has a unified structure, with the Supreme Court, the High Courts and the lower Courts constituting a single judiciary.

Indian laws do not cover aspects related to the off shoring and the Internet, which have emerged recently. The arrival of the Internet resulted a new set of complex legal issues. This was followed by off shoring, which led to further complications. The Indian government has responded proactively in this sphere and has laid the foundations of the required legal framework. The first draft of the Information Technology (IT) Bill was introduced as early as 1999. The IT Act, which finally came into existence in 2000, includes laws and policies concerning data security and cyber crimes. Apart from the IT Act, the Indian Copyright Act of 1972 deals with copyright issues in computer programs.

At present, there are no data protection specific laws in India. However, in the absence of specific laws, the Indian Judicial System offers a few proxy laws and other indirect safeguards. In the following section, we briefly discuss the IT Act and other laws, which companies can use to safeguard proprietary information.

Information Technology Act, 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill, which has subsequently become known as the Information Technology Act, 2000. The Act covers cyber and related information technology laws in India. The IT Act has made amendments to the Indian Penal Code of 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act of 1891 and the Reserve Bank of India Act of 1934, to update them with the provisions of the Act. The information security issues under the IT Act are the following:

Section 43

According to Section 43 of the IT Act, if a person without the permission of the person in-charge of the computer system, accesses, downloads any data, introduces virus or causes denial of access, will be liable for a penalty of up to rupees 10 million.

Section 65: Tampering with Computer Source Code

Section 65 of the IT Act deals with the issue of tampering with computer source documents. According to Section 65, anyone who deliberately or purposely hides, destroys or alters any computer source code or induces someone else to do so shall be punishable with imprisonment up to three years, or with fine, which may go up to two lakh rupees, or with both

Section 66: Hacking

Section 66 of the IT Act deals with the issue of hacking. According to Section 65, hacking is committed if some one, with the intention of causing wrongful loss or damage (or with the knowledge that such damage or loss is likely to result) to the public / any person, destroys / deletes / alters any information residing in a computer resource, diminishes its value or utility, or affects it injuriously by any means. If a person commits hacking, he/she is liable to be punished with imprisonment up to three years, or with a fine, which may go up to two lakh rupees, or with both.

Section 72: Breach of Confidentiality and Privacy

Section 72 of the Act relates to the disclosure of certain information by any person who has gained access to such information in pursuance of a power granted under the Information Technology Act. In case a person who has secured access to any electronic record, book, register, correspondence, information, document, or other material discloses any of these to any other person, he will be punished with imprisonment for a term, which may extend to two years, or with a fine, which may go to ten lakh rupees, or with both.

The above provision does not apply to the disclosure of personal information regarding a person in a website or by his email service provider, etc.

Indian Contract Act, 1872

A contract is a legally binding agreement between two or more persons. For example, purchasing goods, engaging a builder to carry out work, borrowing money, or ordering goods or machinery from a manufacturer are all contracts. The terms of a contract are for the parties to decide. The basic rule is that the contracting parties must perform as specified in the contract. Violation of the terms of the contract or non-performance of one's obligations under the contract amounts to a breach of the contract. When a party to a contract commits a breach of the contract, the other party may resort to the following legal remedies:

Damages

The party, which suffers due to the breach of a contract, by the other party is entitled to receive compensation for any loss or damage caused to it. However, the loss or damage must be shown to the court to have arisen in the usual course due to the breach. In other words, compensation is not to be given for any remote and indirect loss or damage sustained by reason of the breach. Damages can also be recovered if it can be shown that it was known to the parties that a loss or damage resulting from the breach (at the time when the contract was made) is likely to result in a breach of the contract.

Where a sum has been named in the contract, to be paid in the case of a breach, or if the contract specifies a penalty, the party complaining of the breach is entitled (whether actual damage or loss is proved to have been caused) to receive a reasonable compensation not exceeding the amount agreed upon or, the stipulated penalty. A stipulation regarding an increased interest from the date of the default may be regarded as a penalty. The court is empowered to reduce it to an amount, it considers reasonable in the circumstances.

Specific Performance of the Contract

In certain special cases, the court may direct the "specific performance" of the contract against the party in default. In other words, the party in default may be directed to perform the very obligation, which he has undertaken, as per the terms of the contract. This remedy is discretionary and granted in exceptional cases.

The best way foreign firms can protect their data and intellectual property while off shoring work to India is through contracts. The Indian Contract Act 1872 provides adequate safeguards to foreign companies, provided both firms (Indian and foreign) agree to the contract. The companies off shoring work need to ensure that they enter an exhaustive Service Level Agreement (SLA) with their vendor, which covers various aspects of data security and confidentiality. This will help companies safeguard themselves in the case of any fraud or misconduct.

As mentioned above, damages are the best remedy, but due to the lengthy timelines of the Indian judicial system, companies should first try to obtain an injunction. It does not normally take more than a month to obtain an injunction. Obtaining damages is quite a difficult task, and at times takes several years.

Indian Penal Code

Section 406: Punishment for Criminal Breach of Trust

In case any person, who has been entrusted with property, or with any power over any property, dishonestly misappropriates the property, makes wrongful use of the property, dishonestly disposes off that property, or induces any other person to do so, such a person commits "criminal breach of trust". Under Section 406 of the Indian Penal Code, whoever commits criminal breach of trust shall be punished with imprisonment, which may extend to three years, or with a fine, or with both.

Section 420: Cheating and Dishonestly Inducing Delivery of Property

Section 420 of the Indian Penal Code (IPC) deals with cheating cases. Under the section, whoever cheats and consequently dishonestly induces a person to deliver any property (to any other person), or to alter or destroy the whole or any part of a valuable security, shall be punished with imprisonment, which may extend to seven years, and shall also be liable to a fine.

Indian Copyright Act

India has one of the most modern copyright protection laws in the world. A major development in the area of copyright was the amendment to the Copyright Act of 1957 in 1999, to make it fully compatible with the provisions of WTO's Trade-related Aspects of Intellectual Property Rights (TRIPS) Agreement. The Copyright (Amendment) Act, 1999, came into force on January 15, 2000.

The 1994 amendment of the Copyright Act of 1957 brought sectors such as satellite broadcasting, computer software and digital technology under Indian copyright protection.

The other important development during 1999 was the issuance of the International Copyright Order, 1999, which extended the provisions of the Copyright Act to nationals of all World Trade Organization (WTO) member countries.

As per the provisions of the Indian Copyright Act, 1957 and as amended in 1994-1995, any person who knowingly makes use of an illegal copy of a computer program shall be punishable. According to Section 63 B, copyright infringement attracts a minimum imprisonment of seven days. The Act further provides for fines, which shall not be less than fifty thousand rupees, but may go up to twenty lakh rupees, a jail term up to three years, or both¹.

Under Indian law, computer programs have copyright protection but no patent protection. A software program is an algorithm and patent law does not protect algorithms per se. The term

¹ Source: <http://stlc.iii.org.tw/asocio/india/india-1.htm>

'software' includes computer programs, databases, computer files, preparatory design material, and associated printed documentation such as users' manuals.

Consumer Protection Act, 1986

Consumer Protection Act came into force on April 15, 1986 to protect the consumers from exploitation and to save them from adulterated and substandard goods and deficient services. With regards to security, consumers can file a complaint with the court for “deficiency of service” such as disclosing proprietary information, personal information etc., without adequate authorization.

Specific Relief Act, 1963

According to Section 39 of the Specific Relief Act, 1963, a person can claim temporary and permanent injunctions against unauthorized disclosure of confidential information.

Government Initiatives

The Ministry of Information Technology in India has undertaken several initiatives to upgrade security standards. The following are some of them:

Standardization, Testing and Quality Certification (STQC) Directorate

Due to the international demand that Indian firms should have an international security standard accreditation, the Indian government has set up the Standardization, Testing and Quality Certification (STQC) Directorate (under the Department of Information Technology (DIT)). The Directorate has been able to set up to launch an independent third-party certification scheme for the Information Security Management System, as per BS 7799 Part 2, and has achieved international recognition in the form of accreditation from the RvA, Netherlands. The STQC Directorate provides services such as testing hardware and software products, product certification, and also training personnel in quality and security standards and processes.

Computer Emergency Response Team (CERT)

The Indian Computer Emergency Response Team (CERT-In) was established by the Department of Information Technology (DIT) to be a part of the international CERT community. CERT was set up to protect India's IT assets against viruses and other security threats. It performs the following functions:

- It serves as a central point, responding to computer security incidents and providing a reliable, trusted, 24-hour referral contact for emergencies.
- It disseminates best practices among System Administrators and Service Providers.
- It increases the awareness and understanding of information security and computer security issues among the Indian cyber user community.
- It alerts the community regarding the latest security threats in the form of advisories, vulnerability notes and incident notes.
- It serves as a coordinating centre among organizations, to solve computer security problems.
- It establishes linkages with similar organizations in the international arena.

- It performs R&D activities in collaboration with premier research and educational organizations regarding the security of existing systems and regarding evolving cyber security problems.

Information Security Technology Development Council (ISTDC)

The Ministry has recently set up the Information Security Technology Development Council (ISTDC). The main objective of this program is to facilitate, coordinate and promote technological advancements, and to respond to information security incidents, threats and attacks at the national level. ISTDC has been established for the following functions:

- To evaluate the cyber security project proposals received, and to provide recommendations for further processing by DIT
- To review on-going projects through monitoring committees and recommend any modification in scope, funding, duration, additional inputs, termination, transfer of technology, etc.
- To recommend follow-up action on completed projects – transfer of technology, initiation of next phase, etc.
- To form project review and steering groups of projects approved and funded by the DIT

Projects

The following are some R&D projects addressing current and future security needs, which have been initiated by the Indian government:

- Futuristic technologies in Secure Computer and Communication Infrastructure at the Tata Institute of Fundamental Research
- Information Security Management Training and Certification Kernel, ISM: TRACK, at STQC, New Delhi, which aims to increase security awareness and provide third-party certification services
- Development of core network security technologies for E-Commerce at C-DAC, Pune; Further, the group is also working on network security technologies such as C-DAC's Virtual Private Network (C-VPN), a crypto package (C-Crypto), and prototypes of eCommerce applications to showcase the other two technologies
- Development of Validated Security Processes & Methodologies for Web-based Enterprises at Jadavpur University, Kolkata
- Protocols and Standards for E-Cheque Clearing and Settlement at IDRBT at Hyderabad -- are working on the security challenges of online payment systems
- Design and Development of a Transparent Solution for Securing Networks and Systems at CDAC, Hyderabad.