

## **India's Information Technology Act, 2000**

By Pavan Duggal ( editorial advisor, Inomy.com, and advocate, Supreme Court of India)

*India's first cyber law makes punishable cyber crimes like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy, and publication of digital signature certificate false in certain particulars, says noted Supreme Court advocate Pavan Duggal.*

After months of waiting, the government finally got into its act and notified India's first Cyber Law. By means of a notification on October 17, 2000, the Indian government appointed 17th day of October 2000 as the date on which the provisions of the Information Technology Act, 2000 came into force. The Parliament had passed the IT Act, 2000 on May 17, 2000 and the said legislation received the assent of the President of India on 9th June 2000. Though the IT Act, 2000 technically became law of the land, yet it did not come into operation as section 1 (3) of the said Act specifically stipulated that it shall come into force on such date as the Government may, by notification, appoint.

The IT Act aims to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information and to facilitate electronic filing of documents with the government agencies.

In addition, the Central Government also notified two distinct kinds of Rules. These rules are The Information Technology (Certifying Authorities) Rules, 2000 and the Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000.

The Information Technology (Certifying Authorities) Rules, 2000 detail various aspects and issues concerning to Certification Authorities for digital signatures. These rules specify the manner in which information has to be authenticated by means of digital signatures, the creation and verification of digital signatures, licensing of certification authorities and the terms of the proposed licenses to issue digital signatures. The said rules also stipulate security guidelines for certification authorities and maintenance of mandatory databases by the said certification authorities and the generation, issue, term and revocation of digital signature certificates.

The said rules further mandate the audit of the operations of the Certification Authority and classify various kinds of information. The said Rules also have in Schedule II the Information Technology Security Guidelines, which mandate various guidelines for the implementation and management of Information Technology Security. The said Security Guidelines are a virtual Bible for all Certification Authorities for the security aspects of their operations.

The government has also specified the procedures relating to Cyber Regulations

Appellate Tribunal in the notified Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000. These rules specify how an application to the Cyber Regulations Appellate Tribunal has to be preferred along with relevant documents and application fee. It further stipulates how proceedings have to be conducted by the Tribunal. It has also elaborated on the powers of the Registrar of the Cyber Regulations Appellate Tribunal.

The government, by another notification of 17th October 2000, has also constituted the Cyber Regulation Advisory Committee. The committee shall advise the Central Government either generally as regards any rules or for any other purpose connected with the IT Act, 2000. The said committee shall also advise the Controller for Certifying Authorities in framing the regulations under this Act. It comprises, amongst others, the Minister of IT, various Secretaries of different Ministries, representatives from different trade bodies and technical bodies, director of the Central Bureau of Investigation, police chiefs from the states and the Controller of Certifying Authorities.

The overall net effect of all these notifications is that the IT Act, 2000 has come into operation. The information in the electronic format has been granted legal validity and sanction, digital signatures have been defined and made legal. It is now possible to retain information in an electronic format. Electronic contract has been recognized to be legal and binding. Some types of cyber crimes have been defined and made punishable offences like hacking, damage to computer source code, publishing of information which is obscene in the electronic form, breach of confidentiality and privacy and publishing digital signature certificate false in certain particulars and for fraudulent purpose.

The appointment of the Controller for Certifying Authorities has kicked off the process of licensing of Certifying Authorities in India. It is expected that in a couple of months, Certifying Authorities, duly licensed by the Controller, would begin operations of issuing digital signature certificates in India.

It has taken India nine Internet years to pass and notify the implementation of its first cyber law namely the Information Technology Act, 2000. The implementation of the IT Act is likely to throw up a gamut of complicated and complex legal issues as numerous areas have still not been covered under either the IT Act, 2000 or the various IT Rules. India has to face the challenges of cyberspace and its regulation in a very bold, prompt and decisive manner if it wants to become an IT superpower in the years to come.

Source: [Inomy.com](http://Inomy.com) 11/06/2000