A Primer on CYBER LAWS IN INDIA

Rajnish Kumar
National Academy of Indian Railways

Cyber law is important because it touches almost all aspects of transactions and activities on and involving the internet, World Wide Web and cyberspace. Every action and reaction in cyberspace has some legal and cyber legal perspectives.

Cyber law encompasses laws relating to

1. Cyber crimes
2. Electronic and digital signatures
3. Intellectual property
4. Data protection and privacy

In India, cyber laws are contained in the Information Technology Act, 2000 (IT Act) which came into force on October 17, 2000. The main purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government.

Information Technology Act, 2000

The IT Act, 2000 consists of 90 sections spread over 13 chapters [Sections 91, 92, 93 and 94 of the principal Act were omitted by the Information Technology (Amendment) Act 2008 and has 2 schedules.[Schedules III and IV were omitted by the Information Technology (Amendment) Act 2008].

Salient features of the Information Technology (Amendment) Act, 2008

1. The term 'digital signature' has been replaced with

'electronic signature' to make the Act more technology neutral.

2. A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.
3. A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
4. New Section to address data protection and privacy -Section 43
5. Body corporate to implement best security practices-Sections 43A &72A

Applicability and Jurisdiction of the Act

The Act will apply to the whole of India unless otherwise mentioned. It applies also to any offence or contravention there under committed outside India by any person.

If a crime is committed on a computer or computer network in India by a person resident outside India, then can the offence be tried by the Courts in India?

According to Sec.1(2) of Information Technology Act, 2000, the Act extends to the whole of India and also applies to any offence or contravention committed outside India by any person. Further, Sec.75 of the IT Act, 2000 also mentions about the applicability of the Act for any offence or contravention committed outside India. According to this section, the Act will apply to an offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves a

computer, computer system or computer network located in India.

Digital Signature under the IT Act, 2000

Digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.

Electronic Signature

Electronic signature has also been dealt with under Section 3A of the IT Act, 2000. A subscriber can authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable and may be specified in the Second Schedule. An Amendment to the IT Act in 2008 introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

E-Governance

E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000.

It provides for legal recognition of electronic records and Electronic signature and also provides for legal recognition of contracts formed through electronic means.

Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

Controller of Certifying Authorities (CCA)

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities (CAs) issue digital signature certificates for electronic authentication of users.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA.

Penalties and Offences

Cyber Crime	Brief Description	Relevant Section in IT Act	Punishments
Cyber Stalking	Stealthily following a person, tracking his internet chats.	43, 65, 66	3 years, or with fine up to 2 lakh
Cyber Pornography including child pornography	Publishing Obscene in Electronic Form involving children	67, 67 (2)	10 years and with fine may extends to 10 lakh
Intellectual Property Crimes	Source Code Tampering, piracy, copyright infringement etc.	65	3 years, or with fine up to 2 lakh
Cyber Terrorism	Protection against cyber terrorism	69	Imprisonment for a term, may extend to 7 years
Cyber Hacking	Destruction, deletion, alteration, etc in a computer resources	66	3 years, or with fine up to 2 lakh
Phishing	Bank Financial Frauds in Electronic Banking	43, 65, 66	3 years, or with fine up to 2 lakh

Cyber Crime	Brief Description	Relevant Section in IT Act	Punishments
Privacy	Unauthorized access to computer	43, 66, 67, 69, 72	2 years, or with fine upto 1 lakh

DATA PROTECTION and PRIVACY

The Section 43-A, dealing with compensation for failure to protect data was introduced in the ITAA -2008. As per this Section, where a body corporate is negligent in implementing reasonable security practices and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Thus the corporate responsibility for data protection is greatly emphasized by inserting Section 43A whereby corporates are under an obligation to ensure adoption of reasonable security practices. Further what is sensitive personal data has since been clarified by the central government vide its Notification dated 11 April 2011.

Sensitive personal data or information.- Sensitive personal data or information of a person means such personal information which consists of information relating to;-

(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

Thus the role of top management and the Information Security Department in organizations is very important in ensuring data protection, especially while handling the customers' and other third party data.

Reasonable Security Practices are

1. Site certification
2. Security initiatives
3. Awareness Training
4. Conformance to Standards, certification
5. Policies and adherence to policies
6. Policies like password policy, Access Control, email Policy etc
7. Periodic monitoring and review.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules have since been notified by the Government of India, Dept of I.T. on 11 April 2011. Any body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies containing managerial, technical, operational and physical security control measures commensurate with the information assets being protected with the nature of business. The International Standard IS/ISO/IEC

27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub rules.

In view of these rules not only IT companies but also those in the Banking and Financial, Services Sector especially those with massive computerized operations dealing with public data and depending heavily on technology have to be very careful and sensitive to data privacy.

Some Points

- The Indian Penal Code (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

- Digital Evidence is to be collected and proven in court as per the provisions of the Indian Evidence Act (as amended by the IT Act).

- In case of bank records, the provisions of the Bankers' Book Evidence Act (as amended by the IT Act) are relevant.

- Investigation and adjudication of cyber crimes is done in accordance with the provisions of the Code of Criminal Procedure and the IT Act.

- The Reserve Bank of India Act was also amended by the IT Act.

The Cyber Appellate Tribunal has, for the purposes of discharging its functions under the IT Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908. However, is not bound by the procedure laid down by the Code of Civil Procedure,

1908 but is guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules. The Cyber Appellate Tribunal has powers to regulate its own procedure including the place at which it has its sittings.

SEC 66A- Very Important

Punishment for sending offensive messages through communication service, etc.

Any person who sends, by means of a computer resource or a communication device,—

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Important Websites:

http://catindia.gov.in/Default.aspx **-**Cyber Appellate Tribunal

http://www.cert-in.org.in/ **-**Indian Computer Emergency Response Team

http://cca.gov.in/rw/pages/index.en.do **-**Controller of Certifying Authorities

http://deity.gov.in/content/cyber-laws

http://www.cyberlawsindia.net/

Rajnish Kumar
Professor (IT), National Academy of Indian Railways
pit@nair.railnet.gov.in
rajnishkumar@nair.railnet.gov.in