STATUS OF DEVELOPING CYBERCRIME LEGISLATION IN INDIA

A PRESENTATION

BY

PAVAN DUGGAL

ADVOCATE, SUPREME COURT OF

PRESIDENT, CYBERLAWS.NET

PRESIDENT, CYBERLAW ASIA

PRESIDENT, CYBERLAW INDIA

STATUS OF DEVELOPING CYBERCRIME LEGISLATION IN INDIA

- India has in place the Information Technology Act, 2000 – primarily an e-commerce enabling legislation, but enacted Chapter XI therein wherein certain activities were declared as Cybercrimes.

- These activities included damage to computer source code, hacking, publishing of obscene electronic information, breach of protected system, publishing digital signature certificates false in certain particulars or for fraudulent purposes.

- IT Act, 2000 is not an legislation dedicated to cyber crime.

CYBERCRIME LEGISLATION IN INDIA(Contd.)

The Council of Europe interacted with Chair ,Parliamentary Standing Committee on Information Technology of the Indian parliament and Indian Government and gave various suggestions to be incorporated so as to make the Indian legislation in sync with the basic principles and tenets of the Budapest Convention.

Consequently the Indian Information Technology Act, 2000 was amended by Information Technology (Amendment) Act 2008. These amendments have come into force from October 27, 2009.

Various new provisions have been added to make the Indian IT law in sync with the relevant principles of Budapest Convention.

CYBERCRIME LEGISLATION IN INDIA(Contd.)

- Comprehensive provisions have been added for monitoring and collection of traffic data or information through any computer resource.
- Various new cyber crimes have been added in line with the broad principles of the Budapest Convention.
- The Indian Information Technology Act, 2000 has been made more technology neutral by providing for the concept of electronic signatures.
- Provisions have been added for compensation in the event of negligent possessing, dealing or handling of sensitive personal data or information.
- Provisions on cyber security have been added along with obligations upon the relevant stakeholders, who are intermediaries, to follow reasonable security practices and procedures.

CYBERCRIME LEGISLATION IN INDIA(Contd.)

- Various kinds of crimes have been added in the context of use of communication devices and computers.
- Child pornography has been specifically targeted as a heinous crime punishable with five years imprisonment and fine.
- Liabilities of intermediaries and their obligations to retain data in connection with cybercrime and cyber security incidents are appropriately dealt with.
- Thus, the Indian legislation has benefited immensely from the relevant inputs provided by the Budapest Convention.
- However, any cybercrime legislation is a constantly involving legislation and India is continuing to look at further tweaking its legislation to be in sync with the times.

INDIAN INFORMATION TECHNOLOGY RULES 2011

- Under the amended Information Technology Act, 2000, the Government has issued the Information Technology Rules, 2011 including the Information Technology (Intermediary Guidelines) Rules, 2011.
- Lot of the said provisions under the Information Technology (Intermediary Guidelines) Rules, 2011 have taken inspiration from the ISP guidelines that was finalized as an outcome of the Octopus conferences.
- These Rules provide for obligations and duties on behalf of intermediaries to be complied with. Further obligations to maintain reasonable security practices and procedures and to protect sensitive personal data have been detailed therein. Further, various obligations have been put upon Cyber Cafes to ensure that cybercrime incidence at their level is reduced to the minimum.

- Council of Europe's Budapest Convention and subsequent work can continue to inspire nations to update their cybercrime legislations and help fight cybercrime.

A PRESENTATION

BY

PAVAN DUGGAL

ADVOCATE, SUPREME COURT OF

PRESIDENT, CYBERLAWS.NET

PRESIDENT, CYBERLAW INDIA

PRESIDENT, CYBERLAW ASIA