INFORMATION TECHNOLOGY ACT 2000

&

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

By

Vinay Pandya
System Analyst
The Maharaja Sayajirao University of Baroda, Vadodara

What is Law ?

Law is a system of rules, usually enforced through a set of institutions. It shapes politics, economics and society in numerous ways and serves as the foremost social mediator in relations between people. (wikipedia)

"The rule of law is better than the rule of any individual."

– Aristotle, 350 BC

Lady Justice depicts justice as a goddess equipped with three symbols of the rule of law: **a sword** symbolizing the court's coercive power; **scales** representing the weighing of competing claims; and **a blindfold** indicating impartiality.

Different Laws

- International law
- Constitutional and administrative law
- Criminal law
- Contract law
- Tort law
- Property law
- Equity and Trusts Law
- Civil law
- Religious law
- Labour Law
- Immigration Law
- . . . . . .
- Cyber Law, the latest among all laws

Cyber Law in India

- India defined its first ever Cyber Law on 9th June 2000 through Information Technology Act 2000.

- Amendments were made in this first act on 22nd December 2008 known as Information Technology (Amendment) Act 2008. *(effective from October 27, 2009)*

Why should India have a Cyber Law ?

Because we have Electronic Transactions

&

we have Cyber Crimes

Reasons

- Computers have gained popularity in every aspects of our lives, especially in financial transactions.
- Almost all transactions in **shares are in demat** form.
- Almost **all companies** extensively depend upon their computer networks and keep their **valuable data** in electronic form.
- **Government forms** including **income tax returns, company law forms** etc are now filled in electronic form.
- Consumers are increasingly using **credit cards** for shopping.
- Most people are using **email, cell phones and SMS messages** for communication.
- **Online banking & E-commerce** is becoming a way of life
- **Cyber crime cases** such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc are becoming common.
- Digital signatures and e-contracts are fast replacing conventional methods of transacting business.
- **Cyber Law is the law governing computers and the Internet.** In today's highly digitalized world, almost everyone is affected by cyber law.
- Without supportive, strong legal framework, E-governance or E-commerce is not possible.

What is a Cyber Crime ?

"Cyber Crimes are unlawful acts wherein computer is either a tool or a target or both", such as

a) Criminals can operate Anonymously over the Computer Networks
b) Hackers invade privacy
c) Hackers destroy "Property" in the form of Computer Files or Records
d) Hackers injure other computers users by destroying Information Systems
e) Computer pirates steal Intellectual Property
f) Various types of viruses exist & prevail in the computer systems

Classification of Cyber Crimes

which are dealt with by the IT Act along with others,

- Tampering with computer source documents
- Hacking
- Publishing of information, which is obscene in electronic form
- Child Pornography
- Accessing protected system
- Breach of confidentiality and privacy

as per cyber Crime Cell, Mumbai Police

Classification of Cyber Crimes

which are not dealt with or dealt mildly by the IT Act

- Cyber Stalking
- Cyber squatting
- Data Diddling
- Cyber Defamation
- Trojan Attack
- Forgery
- Financial crimes
- Internet time theft
- Virus/worm attack
- E-mail spoofing
- Email bombing
- Salami attack
- Web Jacking

Some Important Definitions & Amendments in the Act (Clause 2)

(a) ***"access"*** with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

(b) ***"addressee"*** means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(d) ***"affixing digital signature"*** with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

(f) ***"asymmetric crypto system"*** means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;

(g) ***"Certifying Authority"*** means a person who has been granted a licence to issue a Digital Signature Certificate under section 24;

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(h) ***"certification practice statement"*** means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;

'(*ha*) ***"communication device"*** means 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;';

(i) ***"computer"*** means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(j) ***"computer network"*** means the interconnection of one or more computers through—

(i) the use of satellite, microwave, terrestrial line or other communication media; and

(ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;

'(*j*) ***"computer network"*** means the inter-connection of one or more computers or computer systems or communication device through—

(*i*) the use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and

(*ii*) terminals or a complex consisting of two or more inter-connected computers or communication device whether or not the inter-connection is continuously maintained;';

(k) ***"computer resource"*** means computer, computer system, computer network, data, computer data base or software;

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(l) ***"computer system"*** means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;

(n) ***"Cyber Appellate Tribunal"*** means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48;

(n) ***"Cyber Appellate Tribunal"*** means the Cyber Appellate Tribunal established under sub-section (1) of section 48;

'(*na*) ***"cyber cafe"*** means any facility from where access to the internet is offered by any person in the ordinary course of business to the members of the public;

(*nb*) ***"cyber security"*** means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction;'.

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(o) ***"data"*** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

(p) ***"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;

(q) ***"Digital Signature Certificate"*** means a Digital Signature Certificate issued under subsection *(4)* of section 35;

(r) ***"electronic form"*** with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(s) ***"Electronic Gazette"*** means the Official Gazette published in the electronic form;

(t) ***"electronic record"*** means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

'(*ta*) ***"electronic signature"*** means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule and includes digital signature;

(*tb*) ***"Electronic Signature Certificate"*** means an Electronic Signature Certificate issued under section 35 and includes Digital Signature Certificate;';

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

*(u) **"function",*** in relation to a computer, includes logic, control, arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer;

’(ua) ***“Indian Computer Emergency Response Team”*** means an agency established under sub-section (*1*) of section 70B;’;

*(v) **"information"*** includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche:

Contd…..

Some Important Definitions & Amendments in the Act (Clause 2)

(w) ***"intermediary"*** with respect to any particular electronic message means any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message;

‘(*w*) ***“intermediary”,*** with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;’.

(x) ***"key pair",*** in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;

DIGITAL SIGNATURE

Definition

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact.

A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Contd…..

DIGITAL SIGNATURE (as in IT Act 2000, Ch.II - P.4)

3. Authentication of electronic records.

(1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation - For the purposes of this sub-section, "hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it

computationally infeasible—

(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;

(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

DIGITAL SIGNATURE

A **digital signature** or **digital signature scheme** is a type of asymmetric cryptography.

A digital signature scheme typically consists of three algorithms:

- A *key generation algorithm* that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm which, given a message and a private key, produces a signature.
- A *signature verifying algorithm* which given a message, public key and a signature, either accepts or rejects.

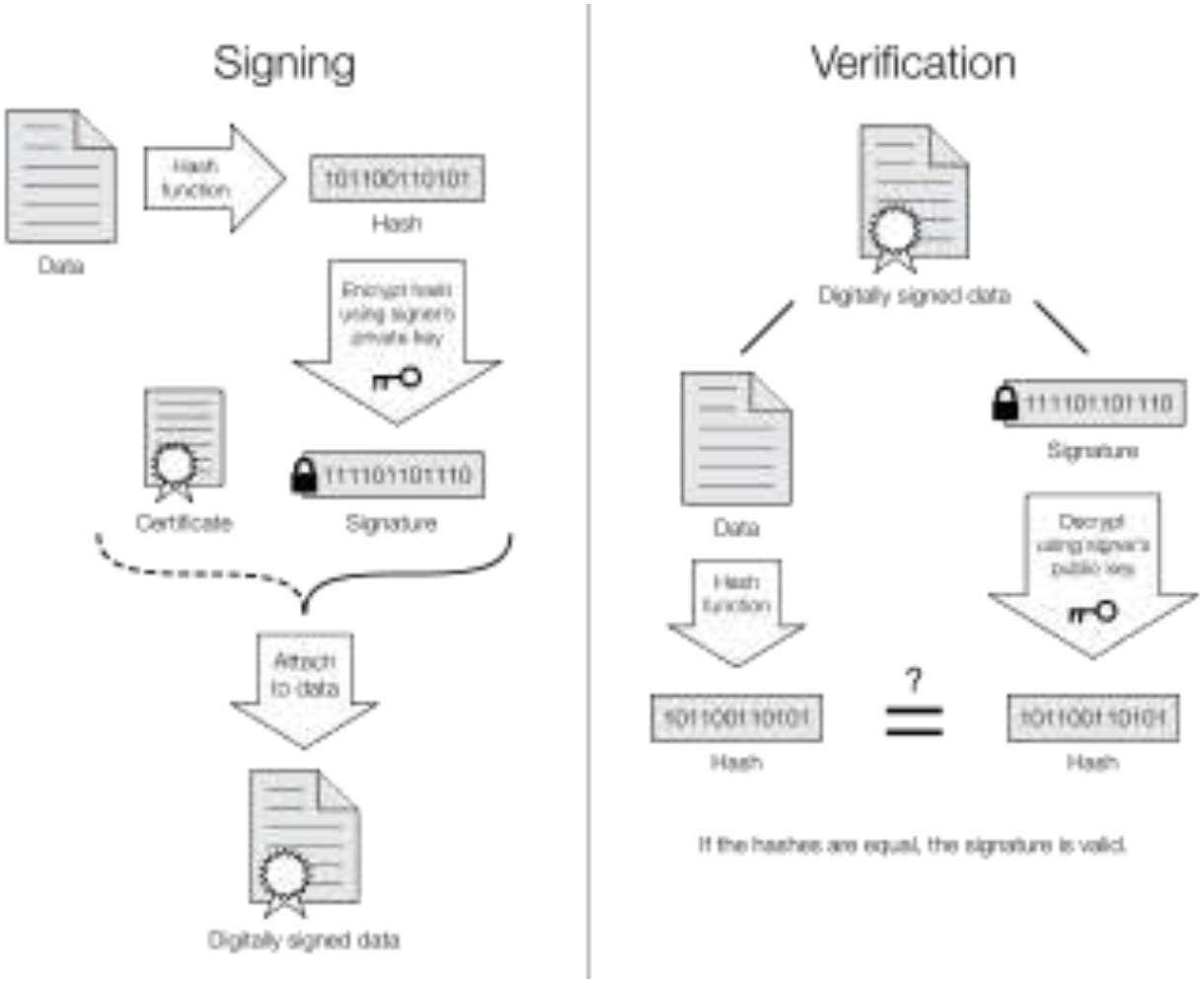
Two main properties are required.

a) A signature generated from a fixed message and fixed private key should verify on that message and the corresponding public key.

b) It should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Contd…..

DIGITAL SIGNATURE



Contd…..

DIGITAL SIGNATURE

Benefits

- **Authentication**
- **Integrity**

Limitations

- **Association of digital signatures and trusted time stamping**
- **Non-repudiation**
- **WYSIWYS (What You See Is What You Sign)** not guaranteed

DIGITAL SIGNATURE CERTIFICATE

What is a Digital Signature Certificate?

Digital signature certificates (DSC) are the digital equivalent (that is electronic format) of physical or paper certificates. Examples of physical certificates are drivers' licenses, passports or membership cards. Certificates serve as a proof of identity of an individual for a certain purpose; Likewise, a digital certificate can be presented electronically to prove your identity, to access information or services on the Internet or to sign certain documents digitally.

Why is Digital Signature Certificate (DSC) required?

Like physical documents are signed manually, electronic documents, for example e-forms are required to be signed digitally through Digital Signature Certificate. As per MCA21 project of Ministry of Company Affairs, all the company forms have to be filed electronically.

Contd…..

DIGITAL SIGNATURE CERTIFICATE

What are the different types of Digital Signature Certificates?

Class 1: These certificates do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.

Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

Who issues the Digital Signature Certificate?

A licensed Certifying Authority (CA) issues the digital signature. Certifying Authority (CA) means a person who has been granted a licence to issue a digital signature certificate under Section 24 of the Indian IT-Act 2000. The list of licensed CAs along with their contact information is available on www.mca.gov.in . You can obtained your DSC from LRA (Licensed Registration Authority) of MTNL www.digitalsignature.in

IT ACT 2000

Permits

- Legal recognition of electronic records.
- Legal recognition of digital signatures.
- Use of electronic records and digital signatures in Government and its agencies.
- Retention of electronic records.
- Publication of rule, regulation, etc., in Electronic Gazette.
- Sections 6,7 and 8 (above 3 sections) not to confer right to insist document should be accepted in electronic form.
- Power to make rules by Central Government in respect of digital signature.

IT ACT 2000

CHAPTER V

SECURE ELECTRONIC RECORDS AND SECURE DIGITAL SIGNATURES

Secure electronic record.

Secure digital signature. Amendment – Electronic Signature

Security procedure.

IT ACT - PENALTIES AND ADJUDICATION

(CHAPTER – IX)

ITAA 2008

The Information Technology (Amendment) Act, 2008 cover the following Legal Provisions for tackling cyber security related crimes and violations:-

Data Protection

- Corporate bodies to implement best practices to protect data
- Heavy Compensation to affected user (Section 43 A)

Breach of Confidentiality & Privacy

- Intermediary and service providers not to disclose personal information of subscriber/user acquired by them while providing services
- Penalties in form of Imprisonment and Fine (Section 72 A)

Pornography including child pornography (Section 67A and B)

Computer related offences

- Expansion of list of offences (Section 66 expanded)
- Identity theft (Section 66C)
- Phishing (Section 66D)
- Spoofing and SPAM (Section 66A)
- E-Commerce Frauds (Section 66 C and D)
- Violation of Privacy (Section 66 E)

Cyber Terrorism (Section 66F)

Monitoring of malicious traffic (Section 69)

Empowering of CERT-In to call for Information (Section 70B)

IT ACT - PENALTIES AND ADJUDICATION (CHAPTER – IX)

43. Penalty for damage to computer, computer system, etc.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network, — . . . . . .

he shall be liable to pay damages by way of ***compensation not exceeding one crore rupees*** to the person so affected.

'43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. . . . . .

Contd…..

IT ACT - PENALTIES AND ADJUDICATION (CHAPTER – IX)

44. Penalty for failure to furnish information return, etc.

If any person who is required under this Act or any rules or regulations made thereunder to—

(a) furnish any document, return or report to the Controller or the Certifying Authority fails to furnish the same, he shall be liable to a penalty **not exceeding one lakh and fifty thousand rupees** for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to **a penalty not exceeding five thousand rupees for every day** during which such failure continues;

(c) maintain books of account or records, fails to maintain the same, he shall be liable to **a penalty not exceeding ten thousand rupees for every day** during which the failure continues.

Contd…..

IT ACT - PENALTIES AND ADJUDICATION (CHAPTER – IX)

45. Residuary penalty.

Whoever contravenes any rules or regulations made under this Act, for .the contravention of which no penalty has been separately provided, shall be liable to pay **a compensation not exceeding twenty-five thousand rupees** to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Contd…..

IT ACT - PENALTIES AND ADJUDICATION (CHAPTER – IX)

46. Power to adjudicate.

(1)For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made thereunder the Central Government shall, subject to the provisions of sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer'for holding an inquiry in the manner prescribed by the Central Government.

for the words “direction or order made thereunder”, the words “direction or order made thereunder which renders him liable to pay penalty or compensation,” shall be substituted;

Contd…..

IT ACT - PENALTIES AND ADJUDICATION (CHAPTER – IX)

46.

"(*1A*). The adjudicating officer appointed under sub-section (*1*) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore:

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crore shall vest with the competent court.";

Contd…..

IT Act 2000 - THE CYBER REGULATIONS APPELLATE TRIBUNAL

IT Amendment Act 2008 - THE CYBER APPELLATE TRIBUNAL

OFFENCES & PUNISHMENTS

65.

O – Tampering with computer source documents

P – imprisonment upto 3 years OR fine which may extend upto Rs. Two lakh OR both

66.

O – Hacking with computer system

P – imprisonment upto 3 years OR fine which may extend upto Rs. Two lakh OR both

66.

O – Computer related offences

P – imprisonment upto 3 years OR fine which may extend upto Rs. Two lakh OR both

OFFENCES & PUNISHMENTS

66A.

O – Punishment for sending offensive messages through communication service, etc.

P – imprisonment upto 3 years AND with fine

66B.

O – Punishment for dishonestly receiving stolen computer resource or communication device

P – imprisonment upto 3 years OR fine which may extend upto Rs. one lakh OR both

66C.

O – **Punishment for identity theft.**

P –imprisonment which may extended upto 3 years AND fine which may extend upto Rs. one lakh

OFFENCES & PUNISHMENTS

66D.

O – Punishment for cheating by personation by using computer resource.

P – imprisonment upto 3 years AND with fine which may extend upto Rs. one lakh

66E.

O – Punishment for violation of privacy

P – imprisonment upto 3 years OR fine which may extend upto Rs. one lakh OR both

66F.

O – Punishment for cyber terrorism.

P – imprisonment which may extended upto imprisonment for life

OFFENCES & PUNISHMENTS

67.

O – Publishing of information which is obscene in electronic form

P – First conviction - imprisonment which may extended upto 5 years OR fine which may extend upto Rs. one lakh

Second & subsequent conviction - imprisonment which may extended upto 10 years OR fine which may extend upto Rs. two lakh

67.

O – Punishment for publishing or transmitting obscene material in electronic form.

P – First conviction - imprisonment which may extended upto 5 years OR fine which may extend upto Rs. one lakh

Second & subsequent conviction - imprisonment which may extended upto 10 years OR fine which may extend upto Rs. two lakh

OFFENCES & PUNISHMENTS

67A.

O – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

P – First conviction - imprisonment which may extended upto 5 years AND fine which may extend upto Rs. ten lakh

Second & subsequent conviction - imprisonment which may extended upto 7 years

67B.

O – Punishment for publishing or transmitting of material depicting childern in sexually explicit act, etc., in electronic form.

P – First conviction - imprisonment which may extended upto 5 years AND fine which may extend upto Rs. ten lakh

Second & subsequent conviction - imprisonment which may extended upto 7 years

OFFENCES & PUNISHMENTS

67C.

O – Preservation and retention of information by intermediaries.

P – First conviction - imprisonment which may extended upto 5 years AND fine which may extend upto Rs. ten lakh

Second & subsequent conviction - imprisonment which may extended upto 7 years

71.

O – Penalty for misrepresentation

P – imprisonment upto 2 years OR fine which may extend upto Rs. One lakh OR both

OFFENCES & PUNISHMENTS

72.

O – Breach of confidentiality & privacy

P – imprisonment upto 2 years OR fine which may extend upto Rs. one lakh OR both

72A.

O – Punishment for disclosure of information in breach of lawful contract.

P – imprisonment upto 3 years OR fine which may extend upto Rs. five lakh OR both

73.

O – Penalty for publishing Digital Signature Certificate false in certain particulars.

P – imprisonment upto 2 years OR fine which may extend upto Rs. one lakh OR both

OFFENCES & PUNISHMENTS

74.

O – Publication for fraudulent purpose.

P – imprisonment upto 2 years OR fine which may extend upto Rs. One lakh OR both

75.

O – Act to apply for offence or contravention commited outside India.

P – this Act shall 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.

APPREHENSIONS / Comments

How Effective it is to Curb Cyber Crimes?

Cyber Law In India - Where Are We Heading To?

IT Act has to be more deterrent - Justice Sirpurkar, Supreme Court

Your cyber crime-friendly legislation !!

We're Not Keeping Pace.

Amend IT Act 2000 to curb its draconian provisions – Kiran Karnik, NASSCOM

THANK YOU