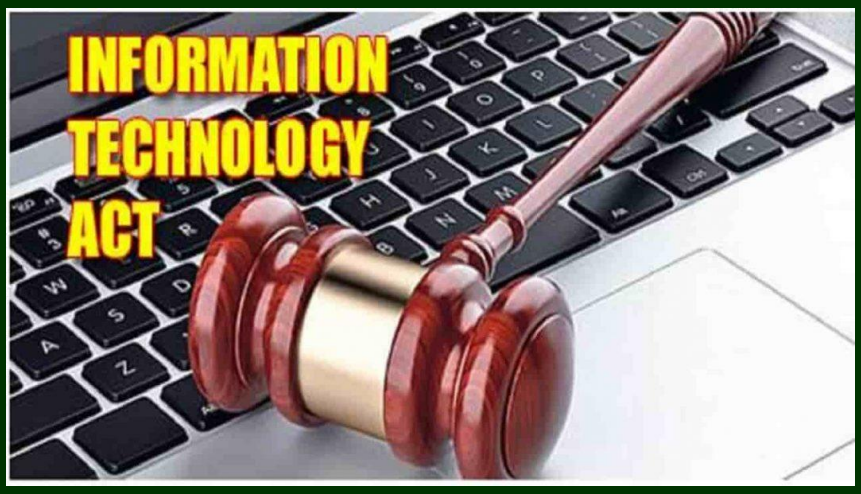


Presentation By:

Pramod Agrawal

Technical Director (IT&C and Planning Deptt.), PMU. DoIT&C

Agenda

1. Information & Communication Technology
2. Law & Act
3. Information Technology Act – 2000 (ITA-2K)
4. Reasons for coming into existence of ITA – 2000
5. Objectives of ITA – 2000
6. Advantages of ITA – 2000
7. Structure of ITA – 2000
8. Key terms of ITA – 2000
9. Salient features of ITA – 2000
10. Possible Cyber Crimes
11. Chapters of IT Act – 2000
12. Few detailed definitions of terms used in IT Act – 2000
13. Important sections & IPC Act under IT Act – 2000
14. Offences & Punishments under IT Act – 2000
15. Conclusion of IT Act – 2000
16. Amended IT Act – 2008
17. Impact of IT Act – 2000/2008
18. Case studies on ITA-2K
19. Suggestions in the existing IT Act
20. Q&A Session

Information & Communication Tech.

- Accumulating information using computing devices connected by some communication media
- Use of technology for:
  - Computing;
  - Storage;
  - Retrieval; and
  - Meaningful dissemination of information
- Communication through:
  - Wired
  - Wireless

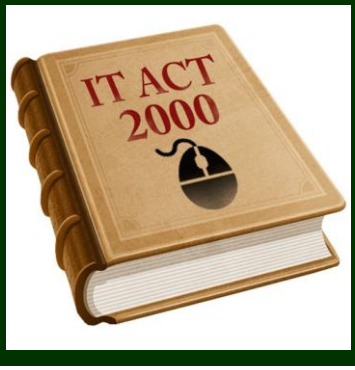
Law And Act ?

- **Law** is a system of rules,
- Usually enforced through a set of institutions & it shapes in:
  - Houses; and
  - Society in numerous ways.

- Serves as the foremost social mediator in relations between people.
- Law is supported by act which is thereafter by rules
- To maintain Law-and-Order in any sector, **Law**, **Act** & **Rules** are obligatory

Information Technology Act 2000:

- The **Information Technology Act, 2000 (ITA-2000)** was enacted with a view:
  - to give a fillip to the growth of electronic based transactions,
  - to provide legal recognition for e-commerce and e-transactions,
  - to facilitate e-governance,
  - to prevent computer-based crimes & ensure security practices,
  - legal recognition of electronic documents & digital signatures



Reasons for coming into existence ITA-2K

Numerous reasons:

- Extensive use of computers in banking & financial transactions
- Wide use of social media platforms
- All companies keeping their records in digital form
- Electronically filing of forms for any application
- Exponential use of plastic/digital money for shopping
- Communication thru Email, SMS etc.
- Purchasing of products thru E-commerce platforms
- Frequent use of Digital signatures and DSCs
- Pornography, viewing & creating obnoxious contents

Reasons for coming into existence ITA-2K

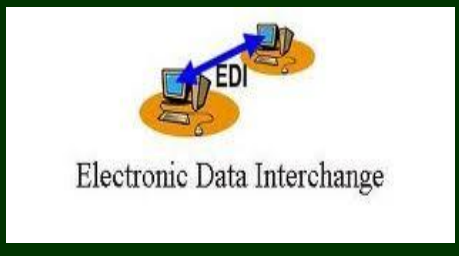
- Following have started in full swing & become common i.e. use of computers for payments:
  - online banking frauds,
  - credit card fraud,
  - source code theft, virus attacks, phishing, email hijacking
  - cyber sabotage, pornography bring malicious-ware
  - denial of service (DOS),
  - information hacking,
  - online share trading frauds, tax evasion etc.

Reasons for coming into existence ITA-2K

- These force into enactment of **ITA-2000** to protect
- IT Act 2000, is the law for governing computers and the Internet
- In today's highly digital world, almost everyone is affected by the Act.
- Without support, strong legal framework, E-governance or E-commerce or financial transactions or using social media platforms etc. are not possible.
- Thus, the **IT Act-2000** was notified on October 17, 2000.

Objectives of ITA-2K:

- To provide legal recognition for transactions:
  - Carried out by means of electronic data interchange (EDI), and other means of electronic communication, commonly referred to as "electronic commerce".
  - To facilitate electronic filing of documents with Government agencies and E-Payments.
  - The Act also provides for the constitution of the Cyber Regulations Advisory Committee, which shall advice the government as regards any rules, or for any other purpose connected with the said act.



Objectives of ITA-2K:

- Aim to amend the Indian Penal Code, Indian Evidence Act,1872, the Banker's Books Evidence Act 1891,Reserve Bank of India Act ,1934.
- Helpful to promote business with the help of internet.
- Is to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means
- It also set of rules and regulations which apply on any electronic business transaction.
- Safeguarding the interest of internet users
- Aims to provide legal sanctity to all electronic records and other activities carried out by electronic means

Advantages of ITA-2K:

- Helpful to promote e-commerce
- Enhance the corporate business through ICT
- High penalty for cyber crime
- Filling online forms
- Secure e-Transactions
- Record authentication
- Site legitimacy
- E-Record keeping

Structure of ITA-2K:

- Consists of **13 chapters** and **90 Sections**

India IT Act of 2000
(Information Technology Act)

Key Terms of ITA-2K:

- EDI, EFT, E-Commerce
- Digital Signature & Secured Electronic records
- Electronic Documents, filing, storing and retrieval
- Certifying authorities issuing DSC, SSL etc.
- Penalties and adjudication
- Cyber regulations appellate tribunal
- Offences & Penalty
- E-Governance
- Encryption & Decryption
- Computer Source Code
- Cyber Terrorism

Brief Salient Features of ITA-2K:

- The Act provides legal recognition to e-commerce, which facilitates commercial e-transactions
- It recognizes records kept in electronic form like any other documentary record
- The Act also provides legal recognition to digital signatures
- Cyber Law Appellate tribunal has been set up to hear appeal against adjudicating authorities
- The Act applies to any cyber offence or contravention committed outside India by a person irrespective of his/her nationality.
- SEBI had announced that trading of securities on the internet will be valid (amendment 2008)

Brief Salient Features of ITA-2K:

- The Indian Penal Code, 1860 was found insufficient to cater to the needs of new crimes emerging from Internet expansion. Even some of the traditional crimes such as conspiracy, solicitation, securities, fraud, espionage etc. are now being committed through Internet which necessitates a new law to curb them. It was in this background that the Information Technology Act, 2000 was enacted in India for prevention and control of cyber crimes.

Possible Cyber Crimes:

- **The Computer as a Target**
  - Using a computer to attack other computers.
    - e.g. Hacking, Virus/Worm attacks, DOS attack etc.

- **The Computer as a Weapon**
  - Using a computer to commit real world crimes.
    - e.g. Cyber Terrorism, IPR violations, CC frauds, EFT frauds, Pornography etc.
- **Unauthorized access & Hacking**
  - Any kind of access without the permission of either the rightful owner or the person in charge of a computer,
  - Every act committed towards breaking into a computer and/or network is hacking.

Possible Cyber Crimes:

- **Trojan Attack**
  - The program that act like something useful but do the things that are quiet damping. The programs of this kind are called as Trojans.
- **Virus and Worm attack**
  - A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus.
  - Programs that multiply like viruses but spread from computer to computer are called as worms.
- **E-mail related crimes**
  - Email Spamming, Bombing, Frauds
  - Sending threatening emails,
  - Defamatory emails
  - Sending malicious codes through emails

Possible Cyber Crimes:

- **Denial of Service attacks**
  - Flooding a computer resource with more requests than it can handle. This causes the resource to crash thereby denying access of service to authorized users.
  - Attempts to "flood" a network, thereby preventing legitimate network traffic
  - Attempts to disrupt connections between two machines, thereby preventing access to a service

Chapters of IT Act-2000:

- **Chapter-I (Definitions):**
  - "**computer**" means electronic, magnetic, optical or other high-speed date 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 relates to the computer in a computer system or computer network;
  - "**computer network**" means the inter-connection of one or more computers through-
    - (i) the use of satellite, microwave, terrestrial lime 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;

Chapters of IT Act-2000:

- "**computer system**" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable 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;
- "**data**" means a representation of information, knowledge, facts, concepts or instruction which are being prepared and is intended to be processed, is being processed or has been processed, and may be in any form (including computer printouts magnetic or optical storage media) or stored internally in the memory of the computer.

Chapters of IT Act-2000:

- "**electronic record**" means date, record or date generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro file;
- "**secure system**" means computer hardware, software, and procedure that-
  - are reasonably secure from unauthorized access and misuse;
  - provide a reasonable level of reliability and correct operation;
  - are reasonably suited to performing the intended function; and
  - adhere to generally accepted security procedures

Chapters of IT Act-2000:

- **Secure electronic record** – where any security procedure has been applied to an electronic record at a specific point of time, then such record shall be deemed to be a secure electronic record from such point of time to the time of verification
- "**Certifying Authority**" means a person who has been granted a license to issue a Digital Signature Certificate
- "**Controller**" means the Controller of Certifying Authorities appointed under sub-section (l) of section 17
- "**Cyber Appellate Tribunal**" means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48
- "**Electronic Gazette**" means the Official Gazette published in the electronic form;

Chapters of IT Act-2000:

- "**originator**" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;
- "**subscriber**" means a person in whose name the Digital Signature Certificate is issued;
- "**Act**" means the Information Technology Act, 2000; (21 of 2000);
- "**Agent**" means a person duly authorized by a party to present an application or reply on its behalf before the Tribunal;
- "**Application**" means an application made to the Tribunal under section 57;

Chapters of IT Act-2000:

- "**Legal practitioner**" shall have the same meaning as is assigned to it in the Advocates Act, 1961 (25 of 1971):
- "**Presiding Officer Registrar**" means the Presiding Officer of the Tribunal;
- "**Registrar of the Tribunal**" and includes any officer to whom the powers and functions of the Registrar may be delegated;
- "**Registry**" means the Registry of the Tribunal;
- "**Section**" means a section of the IT Act;
- "**Affixing digital signature**" means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;

Chapters of IT Act-2000:

- "**Digital signature**" means authentication of any electronic record by a subscriber by means of an electronic method or procedure ;
- "**Digital Signature Certificate**" means a Digital Signature Certificate issued under subsection (4) of section 35;
- "**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 film or similar device
- "**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;

Few Detailed Definitions of Terms:

- Electronics Records attributed to originator:
  - If it was sent by the originator himself.
  - By a person who had the authority to act on behalf of the originator in respect of that electronic record

    or
  - By an information system programmed by or on behalf of the originator to operate automatically.

Few Detailed Definitions of Terms:

- Acknowledgment of receipt:
  - Any communication by the addressee, automated or otherwise or
  - Any conduct of the addressee, sufficient to indicate to the originator that the electronic record has been received.
  - Where the originator has stipulated that the electronic record shall be binding only on receipt of an acknowledgement.

Few Detailed Definitions of Terms:

- The time of receipt of an electronic record shall be determined as follows:
  - If the addressee has designated a computer resource for the purpose of receiving electronic records.
  - Receipt occurs at the time when the electronic, record enters the designated computer resource.

    or
  - If the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.

Few Detailed Definitions of Terms:

- Appointment of Controller & other Officer (certifying officer):
  - Central govt. may appoint no, of deputy controllers and assistant controllers as it deems fit.
  - Controller shall perform the functions assigned to them by the controller under the general superintendence and control of the controller.
  - The qualifications, experience and T&C of service of controller shall be such as may be prescribed by the central govt..
  - There shall be seal of controller.

Few Detailed Definitions of Terms:

- Functions of controller:
  - Exercising supervision & Certifying public keys
  - Laying down the standards to be maintained by the certifying authorities.
  - Specifying the contents of written, printed or visual materials and advertisement.
  - Specifying the form and manner in which accounts shall be maintained.
  - Specifying the T&C subject to which auditors may be appointed.

Few Detailed Definitions of Terms:

- Duties of Subscribers:
  - Generating key pair:
    - The public key which corresponds to the private key of the subscribers which is to be listed in the certificate which the subscriber would generate the key pair by applying the security procedure.
  - Acceptance of digital signature certificate:
    - By accepting the certificate, the subscriber certifies to all who reasonably rely on the information contained in the certificate.

Few Detailed Definitions of Terms:

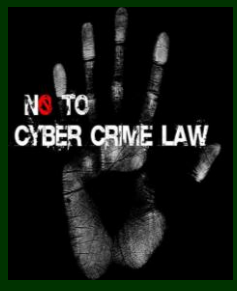
- Cyber regulations of Appellate Tribunal:
  - Establishment of cyber appellate tribunal.
  - Composition of cyber appellate tribunal.
  - Qualifications for appointment as presiding officer of the cyber appellate tribunal.
  - Term of officer.
  - Filling up of vacancies.
  - Orders constituting appellate tribunal to be final and not to invalidate.

Few Detailed Definitions of Terms:

- Digital Signature:
  - Subscriber authenticates electronic record by digital signature.
  - Digital signature uses asymmetric crypto system.
  - Equivalent to handwritten signature which acknowledges
- Digital Signature Certificate:
  - Certifying Authority to issue digital signature certificate.
  - Notice for Suspension & Revocation

Few Detailed Definitions of Terms:

- Offences:
  - Tampering with computer source document.
  - Hacking protected computer system.
  - Publishing obscene information.
  - Controller power & directions.
- Penalties:
  - Penalty to damage computer system & for misrepresentation
  - Penalty for failure to furnish information.



Chapters of IT Act-2000:

- **Chapter-II** (Digital Signature & Electronic Signature):
  - Act specifically stipulates that any subscriber may authenticate an electronic record by affixing his digital signature.
- **Chapter III (Electronics Governance):**
  - This chapter explains the detail that aims to promote use of e-governance electronic records and digital signatures acceptability in Government and its agencies. It provides for filing documents online with governmental authorities, grant of licenses /approvals and receipt/payment of money.
- **Chapter-IV (Acknowledgment of Electronic Rec.):**
  - This chapter gives for Regulation of CA. The Act envisages a CCA who shall perform the function of exercising supervision over the activities of the CA as also laying down standards and conditions governing the CA as also specifying the various forms and content of DSC

Chapters of IT Act-2000:

- **Chapter V (Structured Electronics Records):**
  - This chapter powers to organization for securing the electronic records and secure digital signature. They can secure by applying any new verification system
- **Chapter VI (Regulation Certifying Authorities):**
  - This chapter states that govt. of India will appoint controller of certifying authorities and he will control all activities of certifying authorities. “Certifying authority is that authority who issues digital signature certificate.”
- **Chapter-VII (Certificates):**
  - It details about the scheme of things relating to Digital Signature Certificates. The duties of subscribers are also enshrined in the said Act.

Chapters of IT Act-2000:

- **Chapter VIII (Duties of Subscribers):**
  - The duties of subscribers regarding digital signature certificate. It is the duty of subscriber to accept that all information in digital signature certificate that is within his knowledge is true
- **Chapter-IX (Penalty and Adjudications):**
  - The penalties on offence for damage to computer, computer systems etc. has been fixed as damages by way of compensation.
- **Chapter-X (The Appellate Tribunal):**
  - Establishment of the Cyber Regulations Appellate Tribunal, which shall be an appellate body where appeals against the orders passed by the Adjudicating Officers, shall be preferred.

Chapters of IT Act-2000:

- **Chapter-XI (Offences):**
  - It talks about various offences and the said offences shall be investigated only by a Police Officer not below the rank of Deputy Superintendent of Police. These offences include tampering with computer source documents, publishing of information, hacking which is obscene in electronic form.
- **Chapter XII (Intermediaries):**
  - Police officers have also power to investigate dangerous cyber crime under IPC 1860 , Indian Evidence Act 1872 and RBI Act 1934
- **Chapter XIII (Miscellaneous)**

Imp. Sections of IT Act-2000:

- Inspector level police officer has the right to investigate these cases under the IT Act, section 78:
  - **Section 65** - Trying to tamper with computer resources
  - **Section 66** - Trying to hack into the data stored in the computer
  - **Section 66B** - Provision of penalties for misappropriation of information stolen from computer or any other electronic gadget
  - **Section 66C** - Provision of penalties for stealing someone's identity
  - **Section 66D** - Provision of penalties for access to personal data of someone with the help of computer by concealing their identity
  - **Section 66E** - Provision of penalties for breach of privacy

Imp. Sections of IT Act-2000:

- **Section 66F** - Provision of penalties for cyber terrorism
- **Section 67** - Provisions related to the publication of offensive information
- **Section 67A** - Provision of penalties for publishing or circulating sex or pornographic information through electronic means
- **Section 67B** - Publication or broadcast of such objectionable material from electronic means, in which children are shown in obscene mode
- **Section 67C** - Provision of penalties for disrupting or blocking information by mediators
- **Section 70** - Provision for making objectionable access to a secured computer
- **Section 71** - Delivering data or data incorrectly

Imp. Sections of IT Act-2000:

- **Section 72** - Provisions related to mutual trust and privacy
- **Section 72A** - The provisions relating to making public the information violation of the terms of the Protocol
- **Section 73** - Publication of electronic signature certificate falls in certain particulars.

IPC Sections under IT Act-2000:

- Some of the important & pertinent sections from **IPC, 1860** shall also be included in this periphery:
  - **Section 506 -** Threatening via Social Media
  - **Section 420 -** Punishment of Cyber Fraud committed via Social Media or Any online platforms
  - **Section 463 -** Forging of Electronic Records & Email Spoofing
  - **Section 500 -** Defamation via misuse or un-authorized use of social media like Email abuse, Facebook abuse etc.

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
43	Damage to Computer, Computer system etc	Not Defined	Up to 1 Cr to the affected party
44A	For falling to furnish any document, return on report to the Controller or the Certifying authority	Not Defined	<=1.5 Lakhs per failure
44B	For falling to file any return or furnish any information or other document within the prescribed time.	Not Defined	<=5000 per day per failure
44C	For not maintaining books of account or records.	Not Defined	<=10000 per day per failure
45	Offences for which no penalty is separately provided	Not Defined	>=25000 to the affected party

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
65	Tampering with computer source code documents	3 years or/and	2,00,000
66	Hacking with computer system dishonestly or fraudulently	3 years or/and	5,00,000
66A	For sending offensive messages through	3 Years and	Fine
66B	For dishonestly receiving stolen computer resource or communication devices	3 years or/and	1,00,000
66C	Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	3 years and	1,00,000
66D	cheating by Personation by using computer resource	3 years and	1,00,000
66E	Violation of Privacy	3 years or/and	2,00,000

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
66F	Whoever- A. with intent to threaten the unity, integrity, security by (1) Denial of Access; (2) Attempting to Penetrate computer resource; & (3) Computer containment B. knowingly or intentionally penetrates and by means to cause injury to the interests of the sovereignty and integrity of India	Imprisonment for Life	Not Defined
67	Publish or transmit Obscene material - 1st time Subsequent Obscene in elec. Form	3 years and 5 years and	5,00,000 10,00,000

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
67A	Publishing or transmitting material containing Sexually Explicit Act - 1st time & Subsequently	5 years and 7 years and	10,00,000 10,00,000
67B	Publishing or transmitting material containing Children in Sexually Explicit Act - 1st time Subsequent	5 years and 7 years and	10,00,000 10,00,000
67C	Contravention of Retention or preservation of information by intermediaries	3 years and	Not Defined
68	Controller's directions to certifying Authorities or any employee's failure to comply knowingly or intentionally	2 years or/and	1,00,000
69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	7 Years and	Not Defined

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
69A	Failure to comply with directions for Blocking for Public Access of any information through computer	7 Years and	Not Defined
69B	Failure to comply with directions to Monitor and Collect Traffic Data	3 Years and	Not Defined
70	Protected system. Any unauthorized access to such system	10 years and	Not Defined
70B (7)	Failure to provide information called for by the *I.C.E.R.T or comply with directions	I year or	1,00,000
71	Penalty for Misrepresentation or suppressing any material fact	2 years or/and	100,000
72	Penalty for breach of confidentiality and privacy of el. records, books, information, etc without consent of person to whom they belong.	2 years or/and	100,000

Offences & Punishments under Act:

Section	Contents	Imprisonment Up to	Fine
72A	Punishment for Disclosure of information in breach of lawful contract	3 years or/and	5,00,000
73	Penalty for publishing False DSC	2 years or/and	1,00,000
74	Fraudulent Publication	2 years or/and	1,00,000

Conclusion of IT Act-2000:

- The fundamental approach of the Act is towards validating, legalising electronic & on-line transactions
- Legal framework against the offenders in the field of e-commerce, payment, signatures, social platform etc.
- Awareness must be created.
- It leaves various issues untouched
- The Parliament keeps amending the law & enacting new laws regularly
- That there are no reliable statistics on the problem
- **India is amongst few of the countries in the world which have legal framework for e-commerce and e-governance**

Amendments in IT Act in 2008:

- ITA-2K amended in **2008** & the bill effective from **05.02.2009**.
- The **Rules** frames under the Amended Act became effective from **27.10.2009**.
- **New section** in the amended **ITA-2008**:
  - Freedom of expression laws to be made stringent
  - Intermediary liability to be relaxed
  - New rules of privacy and surveillance
  - New changes with respect to data encryption
  - Consolidated list of penal provisions

Amended IT Act-2008:

- **Introducing Digital Signatures:**
  - With the passage of the IT (Amendment) Act,2008 India has become technologically neutral due to adoption of electronic signatures as a legally valid mode of executing signatures.
- **Introducing Corporate Responsibility (Sec. 43A):**
  - Corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of 'reasonable security practices' to maintain its secrecy, failing which they may be liable to pay damages/compensation.
- **Analysis of the Amended Sec. 43:**
  - The amended Act provides the distinction between 'contravention' and 'offence' (section 43 for contraventions and section 66 of the Act for offences). As per the Amendment Act, 2008, there is no ceiling limit for compensation under section 43 which was one crore rupees in the IT Act.

Amended IT Act-2008:

- **New Definitions Added:**
  - Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(ha)- "Communication device " and Section 2 (w) –"intermediary".
- **Emphasizing the legality of electronic documents:**
  - Newly added sections 7A and 10A in the amended Act reinforce the equivalence of paper based documents to electronic documents.
- **Update on the Power of Controller:**
  - The role of the Controller to act as repository of digital signatures has been repealed by the IT Amendment Act, 2008. This role has now been assigned to the Certifying Authority in Section 30 of the IT Act. The power of Controller to intercept information being transmitted through a computer resource, when necessary, in national interest is amended in Section 69.

Amended ITAct-2008:

- **Update on the role of Adjudicating Officer:**
  - As per the Section 46 in the amended ACT the Adjudicating officers have been conferred with powers of execution of orders passed by it, including order of attachment and sale of property, arrest and detention of accused and appointment of receiver. This empowers the office of Adjudicating officer and extends greater enforceability and effectiveness of its orders.
- **Changes in Cyber Appellate Tribunal:**
  - As per section 52 D, the tribunal would now consist of Chairperson and other members as appointed by the Central Government and their decision-making power.
- **New Addition to the list of Cybercrimes:**
  - Section 66 in the amended Act lists all the new cybercrimes for which no provisions existed in the IT Act,2000.

Amended IT Act-2008:

- **Update on Cyber crime prosecution:**
  - Section 67 talks about conviction for imprisonment for a term not exceeding 2 yrs or fine not exceeding one lac or both for not preserving information.
- **Blocking unlawful websites:**
  - Section 69A has been inserted in the IT amendments 2008 and gives power to Central government or any authorized officer to direct any agency or intermediary(for reasons recorded in writing) to block websites in special circumstances as applicable in Section 69 and its punishable offences.
- **Monitor of data traffic:**
  - Section 69 B confers on the Central government power to appoint any agency to monitor and collect traffic data or information, failing to extend cooperation in this respect is punishable offence.

Amended IT Act-2008:

- **Defining "Critical Information Infrastructure":**
  - The newly added Section 70 in the Amendment Act 2008 defines what is "critical information infrastructure" and encompasses the protection of information is equally important as is the maintaining of security and sovereignty of India.
- **Section 77, 78 and 80**
  - in the amended ACT talks about conferring power to investigate offences under the Act from DSP level to Inspector level which will be instrumental in quicker investigation in the cybercrime cases provided adequate tools and training is provided.
- **Liability of the intermediary modified:**
  - The amended Section 79 states that the intermediary shall not be liable for any third-party information if it is only providing access to a communication system.

Amended IT Act-2008:

- **Electronic Evidence Examiner:**
  - With amendments in 2008, Section 79 A is added that empowers the Central government to appoint any department or agency of Central or State government as Examiner of Electronic Evidence.
  - Penalty And Compensation for the Damage to Computer, System and other related devices

Impact of IT Act-2000/2008:

- Penalty and Compensation for the Damage to Computer, System and other related devices
- email is now a valid and legal form of communication in our country, which can be duly produced and approved in a court of law
- electronic commerce using the legal infrastructure provided by the Act
- Companies digital signatures to carry out their transactions online
- The Act also enables the companies to file any form, application or any other document electronically for interaction
- The IT Act enables companies legally to retain the said information in the electronic form which further can be usable at any place
- Electronic information given and received has a electronic time stamp
- Secure access of computer or web resources
- No identity theft, privacy, hacking, cyber frauds are allowed
- Downloaded copies are valid and legally accepted

Impact of IT Act-2000/2008:

- No computer can have virus over Internet which can infect another computers
- Denial of services is not allowed
- It elaborates on offenses, penalties, and breaches
- No obscene or socially unwanted or revealing any human physical image are not allowed and it is offence

Case Studies:

1. **Bazee.com case**
   - CEO of Bazee.com was arrested because a CD with objectionable material was being sold on the website. The CD was also being sold in the markets in Delhi.
2. **Pune Citibank MphasiS Call Center Fraud**
   - Under Sec 43 - Some ex-employees of BPO arm of MPhasiS Ltd MsourcE made a fraud against US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber crime cases that raised concerns of many kinds including the role of "Data Protection".
     The crime was obviously committed using "Unauthorized Access" to the "Electronic Account Space" of the customers. It is therefore firmly within the domain of "Cyber Crimes".
3. **Cyber Attack on Cosmos Bank**
   - Tthe Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain

Case Studies:

details of various VISA and Rupay debit cards.
The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred.
According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out.
This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

4. **Tampering with Computer Source Documents**
   - In a case of manipulation, Tata Indicom employees were taken into custody in relation to the tampering of the electronic 32-bit number (ESN) that is programmed into cell phones. The theft was for Reliance Intercom. In a verdict on a later date, the court said that since the source code was manipulated, it calls the use of Section 65 under the Information Technology Act.

Case Studies:

5. Bomb Hoax Mail

- In an email hoax, sent by a 15-year-old boy from Bangalore, the Cyber Crime Investigation Cell (CCIC) arrested him in 2009. The boy was accused of sending an email to a private news company saying, “I have planted 5 bombs in Mumbai, you have two hours to find them”. The concerned authorities were contacted immediately, in relation to the cyber case in India, who traced the IP address (Internet Protocol) to Bangalore.

6. Cyber Terrorism

- Since the changes were carried out in the Information Technology Act in Mumbai, this case of cyber terrorism was its first project. A threat email had been delivered to the BSE and NSE, at 10:44 am on Monday. With the MRA Marg police and the Cyber Crime Investigation Cell (CCIC) working together on the cyber crime case, the accused has been detained. The IP address had been traced to Patna, Bihar. When checked for any personal details, two contact numbers were found, which belonged to a photo frame maker in Patna.

Case Studies:

7. Sexuality

- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form
  Relevant Case U/s Sec, 67B: Janhit Manch & Ors. v. The Union of India 10.03.2010 Public Interest Litigation: The petition sought a blanket ban on pornographic websites. The NGO had argued that websites displaying sexually explicit content had an adverse influence, leading youth on a delinquent path.

8. Computer Related offenses

- Related Case u/s Sec 66: Kumar v/s Whiteley. In this case the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users. Investigations had revealed that Kumar was logging on to the BSNL broadband Internet connection as if he was the authorized genuine user and ‘made alteration in the computer database pertaining to broadband Internet user accounts’ of the subscribers. N G Arun Kumar, the techie from Bangalore to undergo a rigorous imprisonment for one year with a fine of Rs 5,000 under section 420 IPC (cheating) and Section 66 of IT Act (Computer related Offense).

Suggestion in Amending ITAct-2K:

- **(Context: Digital signature certificates, Chapter IV, Section 11)**
  Provisioning of SSL certificates compulsorily for at least all e-commerce/ transactional websites may be incorporated in the Information Technology Act, 2000 thereby conferring a degree of authenticity on these websites and eliminating fraudulent transactions to a great extent.
- **(Context: Data Protection, Chapter V section 16)**
  Data Protection in Internet Banking: Internet Banking involves not just the banks and their customers, but numerous third parties too. Information held by banks about their customers, their transactions etc. changes hand several times. It is impossible for the banks to retain information within their own computer networks. The Information Technology Act talks about unauthorised access, but it does not talk about maintaining the integrity of customer transactions. The act does not lay down any duty upon banks to protect the details of customers and clients.
- **(Context: Data Protection, Chapter V section 16)**
  Methods to deal with Proper Intellectual Property and Protection for Electronic Data.

Suggestion in Amending ITAct-2K:

- **(Context: credit card fraud, Chapter IX, Section 43)**
  Provisions to cover credit card fraud be defined appropriately and a specific provision providing for compensation to an aggrieved party for credit card frauds/thefts be incorporated under section 43.
- **(Context: Power to adjudicate, Chapter IX section 46/47)**
  The State/Central government may make provisions for providing all the necessary accoutrements to the adjudicating officer in order to help dispose duties efficiently and seamlessly under the legal framework provided by the Act.
- **(Context: Training for Cyber Appellate Tribunal, Chapter X section 48)**
  Keeping up with the latest global trends in the Information Technology, there should be frequent trainings to up skill the Cyber Appellate Tribunal. A training centre or method of dissemination of knowledge to all.
- **(Context: Restrictions, Chapter XI section 60)**
  Rules and privacy policy to be implemented by social media platforms. Restrictions on pornography, paedophilic, racial etc unlawful content/data may be strictly imposed.

Suggestion in Amending ITAct-2K:

- **(Context: Offences, Chapter XI section 66E)**
  This section may elaborate the definition of Privacy and the IT Act may lay down strict rules of punishment for not withholding private data of any person/entity.
- **(Context: Nodal agency, Chapter XI section 70A)**
  Nodal agency to be set for cross border social media terrorism. Provision for prosecution of International sources (of cybercrime) may be made.
- **(Context: Nodal officer, Chapter XI section 70A)**
  A nodal officer of Social media platforms/websites with defined number of users/hits in India (decided by the MeitY) to be appointed for any redressal of public grievances. Mechanism or protocol to be set to address the grievances of the users.
- **(Context: Offences and Violation of privacy (66E), Penalty for Breach of confidentiality and Privacy (72A), Chapter XI)**
  Provision on privacy may be more overarching and stricter penalty/punishment may be applied for violation of any privacy under the suitable Act/Law/Rules.

Suggestion in Amending ITAct-2K:

- **(Context: unlawful activities, Chapter XI section 74)**
  A proper encrypted database or record to be maintained for all future scrutiny of all unlawful activities for a minimum of 180 days. Prompt reporting of origin within 48 hours to the enforcement agency/ relevant dept/police/court and disabling access in case of any discrepancy/fraud.
- **(Context: Intermediaries not to be liable in certain cases, Chapter XII, Section 79)**
  Tracing of origin/point of start of information is very important to be verified and traced by the ISP/Social media platforms and reported by nodal officers to the investing agency.
- **(Context: Intermediaries not to be liable in certain cases, Chapter XII, Section 79)**
  All social media/content websites are responsible to remove any unlawful content from their platform within 24 hours after being notified by any entity which may lead to any unlawful activity or face legal action.

Suggestion in Amending ITAct-2K:

- **(Context: Intermediaries not to be liable in certain cases, Chapter XII, Section 79)**
  A regulatory body may be appointed to govern all OTT/ social media and online platforms to make them more accountable for the content shared on their platform.
- **(Context: Act to address online gambling, Chapter XII)**
  The Internet makes it very easy for any person to gamble using a web site which may be hosted anywhere in the world. The anonymity offered by the Internet allows operators of fraudulent web sites to dupe unsuspecting surfers of their money and escape prosecution. Keeping in the view of the seriousness of the matter, it is recommended that appropriate amendments may be made in the Gambling Prevention Act to address online gambling.

Suggestion in Amending ITAct-2K:

- **(Context: Role of network service providers, Chapter XII)**
  In an Internet based transaction, the role played by network service providers is vital as without the assistance of a network service provider, communication would not be possible over the Internet. Under such circumstances, the rights and liabilities of various classes of Network Service Providers should be clearly spelt out by virtue of provisions under the Act. Thus, it is recommended that additional provisions be included in the Act under chapter XII to clearly address the rights and liabilities of Network Service Providers so as to give impetus for investment in these areas.
- **(Context: e-commerce, Chapter XIII section 84A)**
  All e-commerce and social media platforms above a defined number of users/hits in India (decided by the MeitY) should be a registered entity in INDIA as per the Companies Act of the country and must comply with privacy policy as per the directions and guidelines by the Central government.

Suggestion in Amending ITAct-2K:

- Just like company registrations/shop act registration has been recently made permanent by tendering one-time fees, DSC may also be given for a lifetime.
- Include a member from the state in the advisory committee.
- There are no provisions in the IT Act that deals with phishing. Though the IPC talks about cheating, therefore, necessary provisions may be made in the IT Act itself to prevent phishing and suggest suitable punishments/penalties within the purview of applicable laws.
- All users must be informed through public awareness campaigns that they shall be responsible for their doings/deeds online and if found guilty or tracked down, may face charges and punishment.
- Provision of Policy/Guidelines/Training to States for dealing with relevant matters to the IT Act.
- An "Electronic Evidence Study Centre" that would be responsible for collection and processing all electronic evidence and track down any hacking attempts and establishing the identity of the suspects in other IT related cases.

Suggestion in Amending ITAct-2K:

- Due to the global pandemic WFH is preferred by government / non-government organization in this regard Privacy policy for work from home should be incorporated in IT Act 2000.
- The issue of Cyber War has also not been discussed in the Act. IT Act should have an important part of any legal regime and due provisions need to be made in congruence with the international framework of laws.
- Suitable provision may be made in the IT Act regarding usage of Crypto currency, with adequate focus on the penalties as per the extant law and rules in force.
- Dissemination of all official communication should be performed via government provided application /servers only. No applications/ servers in any case provided by private company/ individuals should be used for the purpose of official communication.

Thank You

pramod@rajasthan.gov.in