Unit 5 – Cybercrime and Cybersecurity: The legal Perspectives

- Introduction
- Cybercrime and Legal Landscape around the World
- Need Cyber Laws: The Indian Context
- The Indian IT ACT
- Challenges to Indian Law and Cybercrime Scenario in India
- Digital Signature and the Indian IT Act
- Amendments to the Indian IT Act
- Cybercrime and Punishment

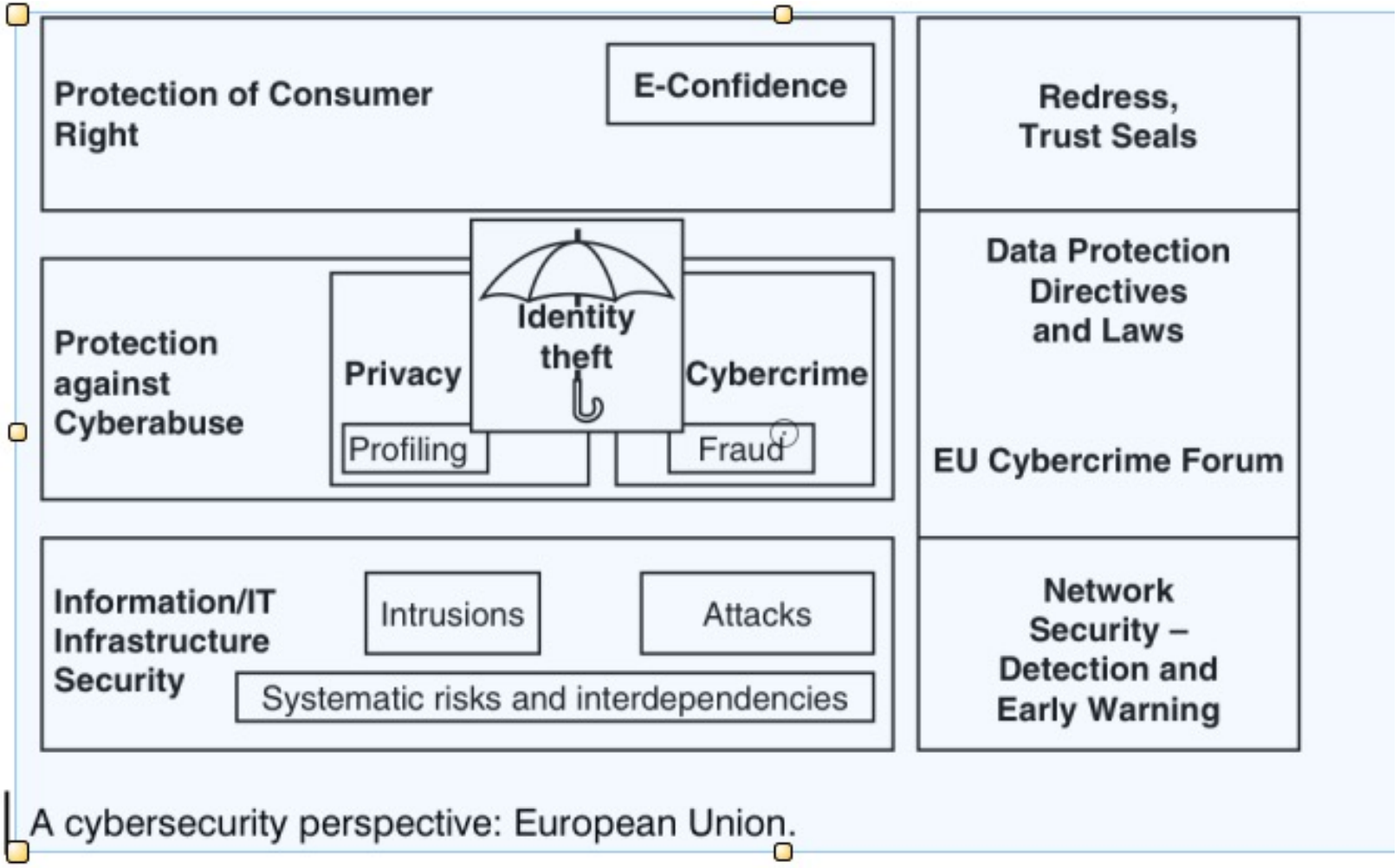
Introduction

1. cybercrime is the largest illegal industry.

2. Knowledge of Cyber laws is essential for people who may directly or indirectly involved and affected

3. In this chapter we need to understand the meaning of ***digital evidence*** given that the ITA act 2000 and its modifications ITA 2008 mention about ***evidence***

4.In the original ITA 2000.



A cybersecurity perspective: European Union.

Categories of Cyber Crime

1. **Cyber crime in the restrictive sense(computer crime):** Any illegal behavior that is carried out by means of electronic methods targeting the security of computer system.
2. **Cybercrime in general sense(computer related crime):** Any illegal behavior that is committed by means of a computer system or network ie distributing information by means of a computer system or network.
3. Examples:

- Unauthorized access to the computer
- Causing damage to the computer an act of computer sabotage
- Doing unauthorized interpretation of communications
- Carrying out computer sabotage.
- Espionage

Computer Trespassing

A person without the authorization. , intentionally gains access to a computer system or electronic database of another

1. Temporarily or permanently remove computer data, computer programs or computer software from a computer or computer network;
2. cause a computer to malfunction regardless of how long the malfunction persists;
3. alter or erase any computer data, computer programs or computer software;
4. effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
5. cause physical injury to the property of another; or make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs or computer software residing in, communicated by or produced by a computer or computer network shall be guilty of the crime of computer trespass which shall be punishable as a Class 1 misdemeanor.

Data protection is not about keeping personal information secret, rather it is about creating trusted framework for collection, exchange and use of personal data in commercial and governmental context.

The Fair information Practices:

1. Control over what to disclose
2. Awareness of how their personal data will be used
3. Right to insist that data are accurate and up to date
4. Protection when personal data is used to make decision about a person.

Table 6.2 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to Microsoft Model Privacy Bill

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
—	Australia	India*
—	Hong Kong	Indonesia*
—	Japan	Malaysia
—	New Zealand	Philippines
—	—	Singapore*
—	—	South Korea
—	—	Taiwan
—	—	Thailand
—	—	Vietnam

Table 6.3 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to anti-Spam laws (Microsoft checklist)

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
Hong Kong	Australia	India*
—	China	Indonesia*
—	New Zealand	Malaysia
—	Singapore	Philippines
—	South Korea	Taiwan*
—	—	Thailand
—	—	Vietnam

Cybercrime and Legal Landscape around the world

- Crime is a legal concept and has the sanction of the law.
- **A broad view on cybercrime in Asia Pacific Region: Challenges:**
- Lack of Awareness of information security issues
- Rapidly evolving
- Transmission networks of communications network.

Table 6.4 | Asia-Pacific region: Alignment of the countries enacted legislation with regard to European Cybercrime Convention and ICMEC's Model Child Pornography Legislation

Favorable Alignment	*Moderate Alignment*	*Weak Alignment*
Australia	Hong Kong	India*
—	Japan	Indonesia*
—	South Korea	Malaysia
—	Taiwan	New Zealand
—	—	Philippines
—	—	Singapore*
—	—	Thailand
—	—	Vietnam*

1. Anti spam law in canada

    Senate Bill S-220

    Parliamentary Bill C-27

2.cyber crime federal law in us

3.European federal law

4.cyber crime in African region

5. Australian Cybercrime Act

Need Of Cyberlaws: The Indian Context

- Cyber laws in several aspects :
  - Intellectual property
  - Data protection
  - Privacy
  - Freedom of expression
  - Crimes committed using computers

First law at ITA 2000

Reason For The Enactment:

1. Although India possesses a very well-defined legal system, covering all possible situations and cases that have occurred or might take place in future, the country lacks in many aspects when it comes to newly developed Internet technology. It is essential to address this gap through a suitable law given the increasing use of Internet and other computer technologies in India.
2. There is a need to have some legal recognition to the Internet as it is one of the most dominating sources of carrying out business in today's world.
3. With the growth of the Internet, a new concept called *cyberterrorism* came into existence. Cyberterrorism includes the use of disruptive activities with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives in the world of cyberspace. It actually is about committing an old offense but in an innovative way.

Cybercrime and Punishment

Section	Offence	Punishment
65	Tampering with Computer Source Code	Imprisonment up to 3 years or fine up to Rs 2 lakhs
66	Computer Related Offences	Imprisonment up to 3 years or fine up to Rs 5 lakhs
66-A	Sending offensive messages through Communication service, etc...	Imprisonment up to 3 years and fine
66-B	Dishonestly receiving stolen computer resource or communication device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh
66-D	Cheating by Personation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh

66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh
66-F	Cyber Terrorism	Imprisonment extend to imprisonment for Life
67	Publishing or transmitting obscene material in electronic form	On first Conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakh On Subsequent Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh
67-A	Publishing or transmitting of material containing sexually explicit act, etc... in electronic form	On first Conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh
67-B	Publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form	On first Conviction imprisonment of either description up to 5 years and/or fine up to Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh

67-C	Intermediary intentionally or knowingly contravening the directions about Preservation and retention of information	Imprisonment up to 3 years and fine	Offence is Bailable, Cognizable.
68	Failure to comply with the directions given by Controller	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh	Offence is Bailable, Non-Cognizable.
69	Failure to assist the agency referred to in sub section 3 in regard interception or monitoring or decryption of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.
69-A	Failure of the intermediary to comply with the direction issued for blocking for public access of any information through any computer resource	Imprisonment up to 7 years and fine	Offence is Non-Bailable, Cognizable.

69-B	Intermediary who intentionally or knowingly contravenes the provisions of sub-section 2 in regard monitor and collect traffic data or information through any computer resource for cybersecurity	Imprisonment up to 3 years and fine
70	Any person who secures access or attempts to secure access to the protected system in contravention of provision of Sec. 70	Imprisonment of either description up to 10 years and fine
70-B	Indian Computer Emergency Response Team to serve as national agency for incident response. Any service provider, intermediaries, data centres, etc., who fails to prove the information called for or comply with the direction issued by the ICERT.	Imprisonment up to 1 year and/or fine up to Rs. 1 lakh

71	Misrepresentation to the Controller to the Certifying Authority	Imprisonment up to 2 years and/ or fine up to Rs. 1 lakh.
72	Breach of Confidentiality and privacy	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh.
72-A	Disclosure of information in breach of lawful contract	Imprisonment up to 3 years and/or fine up to Rs. 5 lakh.
73	Publishing electronic Signature Certificate false in certain particulars	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh
74	Publication for fraudulent purpose	Imprisonment up to 2 years and/or fine up to Rs. 1 lakh

The Indian Act

- The **Information Technology Act, 2000** (also known as **ITA-2000**, or the **IT Act**)
- Act of the Indian Parliament (No 21 of 2000) notified on 17 October 2000.
- It is the primary law in India dealing with cybercrime and electronic commerce.
- The bill was passed in the budget session of 2000 and signed by President K. R. Narayanan on 9 June 2000.
- The bill was finalized by a group of officials headed by then Minister of Information Technology.

- The Information Technology Act, 2000 which consist of **94 Sections** in 13 Chapters and with Four Schedules provides for a legal framework for evidentiary value of electronic record and computer crimes which are of technological nature.

Sections 65, 66, 67, 71, 72, 73 and 74

offenses UNDER THE IT ACT, 2000

- Tampering with computer source documents
- Hacking with the computer system
- Publishing of obscene information in electronic form
- Power of Controller – investigation
- DECRYPT information
- Protection

The Indian ITA 2000

- Sections:

1. Section 65
2. Section 66
3. Section 67
4. Section 71
5. Section 72
6. Section 73
7. Section 74

Section 65: Source Code

- Most important asset of software companies
  - Knowledge, intention
  - destruction, alteration
  - computer source code required to be kept or maintained by law
- Punishment
  - imprisonment up to three years and / or
  - fine up to Rs. 2 lakh

Section 66: Hacking

- Ingredients
  - Intention or Knowledge to cause wrongful loss or damage to the public or any person data
  - Destruction, deletion, alteration, diminishing value or utility or injuriously affecting information residing in a computer resource
- Punishment
  - imprisonment up to three years, and / or
  - fine up to Rs. 2 lakh

Section 66 covers data theft aswell as data alteration

Sec. 67. Pornography

- Publishing or transmitting or causing to be published
- in the electronic form
- Obscene material

- Punishment
  - imprisonment of either description up to five years and
  - fine up to Rs. 1 lakh
  - imprisonment of either description up to ten years and
  - fine up to Rs. 2 lakh
- Section covers
  - Internet Service Providers,
  - Search engines,
  - Pornographic websites

Sec 69: Decryption of information

- Controller issues order to Government -information transmitted through any computer resource.
  - the security of the State,
  - friendly relations with foreign States,
  - public order
  - Person in charge of the computer resource fails to extend all facilities and technical assistance to decrypt the information- punishment up to 7 years.

Sec 70 Protected System

Securing unauthorised access or attempting to secure unauthorised access

- to ‘protected system’

- Acts covered by this section:
  - Switching computer - un authorized
  - Using installed software / hardware
  - Port scanning
- Punishment
  - Imprisonment up to 10 years and fine

Sections 71

- **Offence Name** - Misrepresentation - Certifying Authority
- - Making any misrepresentation to, or suppression of any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be.
- **Penalty** - Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both

section – 72

Offence Name - Penalty for breach of confidentiality and privacy

- **Description -** Any person who, in pursuance of any of the powers conferred under IT Act, has secured access to any electronic record, book, register, correspondence, information or document without the consent of the person concerned discloses such electronic record, book., register, correspondence, information, document to any other person.
- **Penalty -** Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both.

- **Section – 74**:
- **Offence Name** - Publication for fraudulent purpose
- Creation, publication or otherwise making available a Digital Signature

Penalty - Imprisonment for a term which may extend to 2 years, or with fine up to 1 lakh Rupees, or with both. .

Computer Related Crimes under IPC and Special Laws

Sending threatening messages by email	**Sec 503 IPC**
Sending defamatory messages by email	**Sec 499, 500 IPC**
Forgery of electronic records	**Sec 463, 470, 471 IPC**
Bogus websites, cyber frauds	**Sec 420 IPC**
Email spoofing	**Sec 416, 417, 463 IPC**
Online sale of Drugs	**NDPS Act**
Web - Jacking	**Sec. 383 IPC**
Online sale of Arms	**Arms Act**

Admissibility of Electronic Records : Amendments made in the India ITA 2000

The Second Schedule of the Indian ITA 2000: Amendment to the Indian Evidence Act

The Third Schedule of the Indian IT Act 2000: Amendment to the Bankers Books Evidence Act

The Fourth Schedule of the Indian IT Act 2000: Amendment to the Reserve Bank of India Act

Positive Aspects of the ITA 2000

1. Prior to the enactment of the ITA 2000 even an E-Mail was not accepted under the prevailing statutes of India as an accepted legal form of communication and as evidence in a court of law. But the ITA 2000 changed this scenario by legal recognition of the electronic format. Indeed, the ITA 2000 is a step forward.
2. From the perspective of the corporate sector, companies are able to carry out E-Commerce using the legal infrastructure provided by the ITA 2000. Till the coming into effect of the Indian cyberlaw, the growth of E-Commerce was impeded in our country basically because there was no legal infrastructure to regulate commercial transactions online.
3. Corporate will now be able to use digital signatures to carry out their transactions online. These digital signatures have been given legal validity and sanction under the ITA 2000.
4. In today's scenario, information is stored by the companies on their respective computer system, apart from maintaining a backup. Under the ITA 2000, it became possible for corporate to have a statutory remedy if anyone breaks into their computer systems or networks and causes damages or copies data. The remedy provided by the ITA 2000 is in the form of monetary damages, by the way of compensation, not exceeding ₹ 10,000,000.
5. ITA 2000 defined various cybercrimes. Prior to the coming into effect of the Indian Cyberlaw, the corporate were helpless as there was no legal redress for such issues. However, with the ITA 2000 instituted, the scenario changed altogether.

Weak Areas of ITA 2000

1. The ITA 2000 is likely to cause a conflict
2. The ITA 2000 does not even touch the issues relating to domain name.
3. Intellectual Property Rights (IPR) in the context of online environment.
4. The ITA 2000 does not cover various kinds of cybercrimes and internet related crimes namely:

- Theft of Internet hours
- Cyber theft
- Cyber harrasement
- Cyber defamation
- Cyber fraud
- Misuse of credit cards

Challenges to Indian Law and Cybercrime Scenario in India

1. Tampering with the computer source code or computer source documents;
2. un-authorized access to computer ("hacking" is one such type of act);
3. publishing, transmitting or causing to be published any information in the electronic form which is lascivious or which appeals to the prurient interest;
4. failure to decrypt information if the same is necessary in the interest of the sovereignty or integrity of India, the security of the state, friendly relations with foreign state, public order or for preventing incitement to the commission of any cognizable offense;
5. securing access or attempting to secure access to a protected system;
6. misrepresentation while obtaining, any license to act as a Certifying Authority (CA) or a digital signature certificate;
7. breach of confidentiality and privacy;
8. publication of digital signature certificates which are false in certain particulars;
9. publication of digital signature certificates for fraudulent purposes.

- Pendency of Cases
- Corruption.
- Strike by Lawyers
- Less use of technology
- Lack of Transparency
- Low judges strength and Appointment Problem
- No proper Interaction with the Society
- Lack of uniformity -devices used for internet access , tools development
- lack of national level architecture for Cyber security
- Lack of training
- Lack of awareness -IT ACT
- No hard punishment
- Not all cities have crime branch

- pendency of civil cases in Karnataka High Court witnessed a threefold increase from 78,837 cases to **2,53,613 cases**. In the same time period, in Andhra Pradesh, the number of criminal cases witnessed a threefold increase from 13,367 cases to 41,906 cases.
- https://factly.in/in-5-years-more-than-fourfold-increase-in-the-number-of-pending-cyber-crime-cases-in-courts-the-police/

Digital Signature and the Indian IT Act

- A digital signature—a type of electronic signature—is **a mathematical algorithm routinely used to validate the authenticity and integrity of a message** (e.g., an email, a credit card transaction, or a digital document).
- Digital signatures were given legal status in India, by Information Technology (**IT ACT 2000**) in the year 2000.
- E-signatures on electronic documents, the same legal status as the handwritten signatures on physical documents.
- A **digital signature** is a way to identify yourself online.
- Just like passports, driving licenses, and PAN cards allow you to prove your identity offline, **digital signatures** let you prove your identity online.
- To do this, you need a **digital signature** certificate and that lets you sign documents digitally.

- Commonly used for software distribution, financial transactions, contract management software, and in other cases where it is important to detect forgery or tampering.
- Move from the pen and paper world to an electronic era.

- Uses of Digital Signature
  - E-filling
  - E-tender
  - E-procurement
  - Income Tax
  - Sales Tax
  - Banks
  - Patent and trade marks registration
  - Oil & Natural Gas Corporation (ONGC)
  - MSTC Limited
  - Bharat Petroleum Corporation Limited (BPCL)

- Features of Digital Signature.
  - Authentication
  - Integrity
  - Non Repudiation

- How does Digital Signature Certificate work?
  - A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys
  - The certificate contains information about a user's identity.
  - The private key is stored on the user's computer hard disk ; it can only be used with the issued password.
  - The public key is disseminated with the encrypted information.
  - The authentication process fails if either one of these keys in not available or do not match.

Public key certificate

- public key certificate, also known as a digital certificate or identity certificate, is **an electronic document used to prove the ownership of a public key**. ... In email encryption, code signing, and e-signature systems, a certificate's subject is typically a person or organization.
- A **public key certificate** is a digitally signed document that serves to validate the sender's authorization and name. It uses a cryptographic structure that binds a **public**

1. X.509 version information;
2. a serial number that uniquely identifies the certificate;
3. a common name that identifies the subject;
4. the public key associated with the common name;
5. the name of the user who created the certificate, known as the subject name;
6. information about the certificate issuer;
7. signature of the issuer;
8. information about the algorithm used to sign the certificate;
9. some optional X.509 version 3 extensions. For example, an extension exists that distinguishes between CA certificates and end-entity certificates.

Advantage of digital signature

- easy to use
- speed up the pace of business
- improve document accuracy
- save time and money
- They enhance customer services
- Some have limited storage options
- Security varies depending on vendor
- Some use proprietary software

Drawback of digital signature

- A digital signature will be highly dependent on the technology used to create it.
- To use digital signatures, you have to purchase digital certificates that can be quite pricey.
- Users also have to purchase verification software.

History. . . .

- 1999 – Information Technology Bill was prepared.
- May 2000 – This bill was passed by both the houses of parliament.
- August 2000 – This was passed by President of India and was came to be known as “Information Technology Act -2000”.
- 2006 – The act was amended and presented to parliament.
- December 2008 – The act was passed by the parliament & renamed to “Information Technology (Amendment) Act – 2008”.

Reasons for ITAA 2006

- To support the growth of electronic based transaction.
- To support the extended IT enabled services such as e-governance, e-commerce, e-transactions, protection of information and security procedures.
- To prevent computer and internet related crime such as sexual publication, leakage of data etc.
- To harmonize the IT act with the UNCITRAL (United Nations Commission on International TRAde Law.
- To authorise, service providers to setup, maintain and upgrade computerised facilities to provide services to public.

ITAA 2008 composition

- 4 Schedules
- 13 Chapters
- 90 Sections and
- Sub-sections

Section 65: Tampering with source document

Imprisonment up to 3 years OR fine up to 2 lakhs OR both.

Section 66: Computer related Offences

If any person does act referred in section 43, imprisonment upto 2 years OR fine upto 5 lakhs OR both.

Section 66A: Sending offensive messages

- Any person who sends –
- Any information of offensive or menacing character.
- Any information known as false but sent for the purpose of insult, annoyance, enmity, ill will etc.

- Any e-mail for the purpose of causing annoyance, to deceive, mislead etc.
- Imprisonment up to 3yrs AND fine.

Section 66B: Receiving stolen resources

Whoever dishonestly retains any stolen computer resource… imprisonment up to 3yrs OR fine up to 1 lakh OR both.

Section 66C: Identity theft

Whoever fraudulently make use of the E.Sign, password, UID etc….

Imprisonment up to 3yrs AND fine up to 1 lakh.

Section 66D: Cheating by personating

Imprisonment up to 3yrs AND fine up to 1 lakh.

Section 66E: Violation of Privacy

Whoever knowingly captures, publishes or transmits the images of private area of any person without his/her consent…Imprison. upto 3yrs or fine upto 2lakh or both.

Section 66F: Cyber terrorism

Whoever, with the intent to threaten the integrity, security or sovereignty of India or strike terror in public by –

- Denying or cause denial of access to any person authorised to access a computer resources.

- Attempting to penetrate a computer resource without authorization.
- Introducing any computer contaminant causing death or injury to person.
- Damage or destruct property causing disruption of services essential to the life of community.
- Adversely affect Critical Information Infrastructure.
- Whoever, knowingly penetrates a computer resource, database that is restricted for reason of sovereignty, integrity of india, friendly relations with foreign states … … commits cyber terrorism.

- Imprisonment for LIFE.

Section 67 : publishing obscene material in E-form

- Whoever publishes or transmits in e-form any material which is lascivious shall be punished –
- First conviction – 3 yrs AND 5 lakh
- Subsequent conviction – 5 yrs AND 10 lakh

Section 67A : publishing sexually explicit material

- First conviction – 5 yrs AND 10 lakh
- Subsequent conviction – 7 yrs AND 10 lakh
- Exception –
- Published in the interest of science, literature, art, learning or which is used for religious purpose.

Section 67B : publishing material depicting children in sexually explicit act in E-form

- First conviction – 5 yrs AND 10 lakh
- Subsequent conviction – 7 yrs AND 10 lakh
- Exception –
- Published in related to science, literature, art, learning or which is used for religious purpose.

Section 67A : Retention of infor. by intermediaries

- Intermediaries shall retain such info., for such duration, in such format as prescribed by CG.
- If fail –
- Up to 3 yrs ANDup to 2 lakh.

Section 68 : Power of controller

- The controller may direct CA or his Emp. to take such measure or cease carrying out any activity, to ensure compliance with the provisions of Act.
- If any fails – 2 yrs OR 1 lakh OR Both

Section 69 :Power to intercept/monitor/decrypt

- Where CG, SG or any of its officer, is of opinion that it is necessary for the integrity, sovereignty, security of India, may intercept or monitor or decrypt any information transmitted through any computer resources.
- Procedure/safeguard for I/M/D shall be prescribed.

- Any person in-charge of the computer resource shall extend all facilities and technical assistance.
- If fail – 7 yrs AND fine.

Section 69B :Power to authorize to monitor/collect

- To enhance cyber security, prevent intrusion or spread computer contaminant, CG may autho. any agency of Govt. to monitor and collect traffic data from any computer resource.
- Procedure/safeguard for blocking shall be prescribed.
- The person in-charge shall provide technical assistance and extend all facilities.
- If fails to comply with the direction– 3 yrs AND fine.

Section 70 : Protected System

- The appropriate Govt. by official gazette may declare any computer resource which affects C.I.I., as protected system.
- CII means the computer resource, destruction of which may weaken the national security, economy, public health etc.
- Appropriate Govt. may authorize the persons to access protected system.
- Any other person who secure access or attempt to access protected system – 10 yrs AND fine.
- CG shall prescribe the information Security practice and procedure for such protected system.

Section 70 A: National Nodal Agency

- CG, by official gazette, may designate any govt. org. as the national nodal agency in respect to CII.
- The agency shall be responsible for all measures including R&D in protection of CII.

Section 70 B: I. C. E. R. T. for incident response

- CG, by official gazette, may appoint an govt. agency to be called Indian Computer Emergency Response Team.
- ICERT is headed by Director General and have such other officers and employee as prescribed.
-

.....

- **Functions of ICERT –**

- Collection, analysis and dissemination of information on cyber incident.
- Forecast and alerts of cyber security incidents.
- Emergency measures for handling C.S. incidents.
- Coordination of C.S. incident response activities.
- Issue guidelines, advisories relating to information security practice, procedure, prevention, reporting and response of cyber incidents.
- Such other functions relating to cyber security as may be prescribed.

....

- For carrying out the functions agency may call for info. and give directions to service provider, intermediaries, body corporate and any person.
- Any of these party fail to provide information and comply with the directions – up to 1 yr OR up to 1 lakh OR both.

Section 71 : Penalty for Misrepresentation

Whoever make any misrepresentation or hide any fact to Controller or CA, to obtain License or DSC shall be punished – upto 2 yrs OR upto 1 lakh OR both.

Section 72 : Breach of confidentiality and privacy

- Any person who has secured access to electronic record without the consent of person concerned, discloses such information to other person –
    - Upto 2 yrs OR upto 1 lakh OR both

Section 72 A : Breach of lawful contract

- Any person including intermediary, under the term of contract, has secured access to personal info. of other person and with the intent of cause wrongful loss or gain, without consent of the person concerned, provide such info. to other person –
    - Upto 3yrs OR 5 lakh OR both

Section 73 : publishing false DSC

- Person who publishes a DSC with the knowledge –
  - The CA listed in the certificate has not issued it.
  - The subscriber listed in the certificate has not accepted it.
  - The certificate has been suspended or revoked.
- Upto 2 yrs OR 1 lakh OR both.

Section 74 : publishing for fraudulent purpose

- Whoever knowingly creates, publishes or otherwise makes available ESC for any fraudulent purpose ---
  - Upto 2 yrs OR upto 1 lakh OR both

Section 75 : Act to apply for offence outside India

- The Act is applied to any offence where –
  - Perpetrator is Indian(or)
  - Victim is Indian (or)
  - Server is Indian

Section 76 : Confiscation

- Any computer, system, floppy, CD, tape or any other accessories has been or is being involved in contravention of provision of the act shall be liable to confiscate.

- If the court is satisfied that the person in-charge of these computer resources are, is not guilty, the court may, instead of order of confiscation, make such other order against the person contravening the provision of the act, as it may think fit.

Section 77 : penalties not to interfere with other punishment.

No compensation awarded, penalties imposed or confiscation made under this act shall prevent the punishment awarded under any other law for the time being in force.

Section 77 A : Compounding of offense

- A court may compound offences other then offences –
  - Where punishment for life or term exceeding 3 yrs has been provided.
  - Where the accused is, by reason of his previous conviction, liable to enhanced punishment.
  - Where such offences affects the socio-economic condition of India.
  - Where offence is committed against a child below the age of 18yrs or women.

Section 77B : Cognizable offense

The offence punishable with imprisonment of 3 yrs or more shall be cognizable and shall be bailable.

Section 78 : Power to investigate

Not with standing any thing contained in the Code of Criminal Procedure 1973, a police officer not below the rank of Inspector shall investigate the offence.

Section 79 : Exemption from liability

An intermediary shall not be liable for any third party communication if –

- Their function is limited to provide access to a communication system
- The intermediary does not –
  - Initiated the communication
  - Select the receiver
  - Select or modify the information contained in the communication
- The intermediary observe de diligence and observes such guidelines in discharging duties.

- An intermediary shall not be exempted from liability if–
- It conspired, aided or induced the unlawful act by the threats or otherwise.
- Upon receiving actual knowledge that the information connected to the computer resources controlled by intermediary is being used to commit unlawful act, fail to expeditiously remove or disable access to the material.

Section 79 A: CG to notify Examiner of E. Evidence

- The CG, for the purpose of providing expert opinion on evidence in electronic form before any court, may specify any department, agency, body of the Govt. as examiner of E. E.

Section 80 : Power of police officer or other officer

- Any police officer not below the rank of Inspector or other officer of the govt. may enter any public place and search and arrest any person who is reasonably suspect of having committed contravention under this act.
- Where any person is arrested by the other then police officer, such officer shall immediately send the arrested person to the magistrate or the officer-in-charge of the police station.

Section 81 : Act not to have overriding effect

- The provisions of this act shall not have inconsistent effect with any other law for the time being in force.

Section 81-A : E-cheque and truncated cheque

- Act shall apply to, E-cheques and truncated cheques subject to such modification as may be necessary for carrying out purposes of negotiable instrument act, in consultation with RBI.
- Every notification shall be laid before each house of the parliament for a total period of 30 days, in one or multiple sessions.

Section 82 : officers to be public servants

Chairman, Members, Controller, AC/DC and other officers deemed to be public servant within the meaning of IPC section 21.

Section 83 : CG's power to give direction

The CG may give directions to any SG, on the provisions of the Act.

Section 84 : Protection of action taken in good faith

No suit, prosecution or other legal proceeding lie against CG/SG/C/AC/DC or any other person acting on behalf, for anything done in good faith or done in pursuance of this act.

Section 84-A : Mode or method of encryprion

- CG may, for the promotion of e-commerce or e-governance, prescribe the mode or method of encryption.

Section 84-B : Punishment for Abetment

Whoever provoke any offence shall be punished with the punishment provided for the offence under the Act.

Section 84-C : Punishment for attempt to commit

One half of the longest term of imprisonment provided for that offence or such fine as is provided for the offence or both.

Section 85 : Offences by Companies

- Where a person committing a contravention is a company, every person who was in charge of or was responsible of conduct of business shall be guilty and liable to be punished.
- However, if he proves that such contravention took place without his knowledge and he exercised all due diligence then he shall not be liable for punishment.

Section 86 : Removal of Difficulties

- If any difficulty arises in giving effect to the provision of the Act, CG make such provision not inconsistent with the provision of the act, for removing the difficulty.

- However, no order shall be made after the expiry of 2 years from the commencement of the act.
- Order shall be laid before each house of parliament.

Section 87 : Power of CG to make rules

Section 88 : Constitution of Advisory Committee

- The CG shall constitute a committee called Cyber Regulation Advisory Committee.
- CRAC shall have Chairperson and official and non-official members representing the interest affectd or having special knowledge of the subject matter.
- The CRAC shall advise CG and Controller in framing regulation of the act.

Section 89 : Power of Controller

The controller, after consultation with CRAC and previous approval of CG, by notification in official gazette make regulation in the following matters –

- Particulars relating to maintenance of database.
- Conditions & restriction of recognizing foreign CA
- T&C of granting license
- Standard to be observed by CA.
- Manner in which CA shall disclose the matter.
- Statement which shall accompany an application.
- The manner in which subscriber communicates the compromise of private key.

Section 90 : Power of state Govt.

- The SG may, by notification in official gazette, make rules on the following matters –
  - The electronic form in which filing, issue/grant of receipt, payment shall be effected.
  - For matters specified in section 6.
- Every rule made by SG shall be laid before the house(s) of state legislature.