LAWXPERTSMV. #UNDERSTANDING NOTES

Information Technology Law including Cyber Laws - Concept, purpose/prospects

INTRODUCTION : To deal with the problems of cybercrimes and recognition of e-commerce in cyber space i.e. Cyber Law or Cyber Space Law or Information Technology Law came into picture.

1996- Model Law on E-commerce was adopted by United Nations Commission on International Trade and Law (UNCITRAL). India was a signatory and ratified it with the passing of the Information Technology Act, 2000.

WHY DO WE NEED INFORMATION TECHNOLOGY ACT> IMPORTANT.

1. Legal recognition to
   - all electronic records and other activities carried out by electronic means/ e-commerce.
   - Electronic Data Interchange (EDI)
   - Digital signatures + its regulation by a regulatory body.
2. Creation of civil and criminal liabilities for contravention of the provisions of the Act and to prevent misuse of the e-business transactions + Consequential amendments to Indian Penal Code, 1860 and the Indian Evidence Act, 1872 for equating paper-based offences carried by electronic means.
3. Facilitating e-governance in government offices and agencies so that citizen-government interaction becomes more hassle free.
4. Facilitating electronic transfer of Funds + books of accounts maintained in electronic form.

STRUCTURE OF IT ACT : It has 13 Chapters and 90 sections. It starts with definitions, thereafter it recognizes the concepts of authentication and certification of digital signatures, electronic records, electronic signatures etc. Later on, it deals with cyber crimes and authorities to tackle with.

SALIENT FEATURES OF INFORMATION TECHNOLOGY ACT 2000

PREAMBLE :

- to provide legal recognition for transactions carried out by means of *electronic data interchange*[1] and other means of electronic communication, commonly referred to as "electronic commerce"[2], which involve the use of *alternatives to paper-based methods of communication and*
- storage of information, to facilitate electronic filing of documents with the Government agencies

EXTRA-TERRITORIAL EFFECT : Section 1(2) The Act extends to the whole of India and also to any offence or contravention committed outside India by any person.

1. ***Chapter 1*** consists of preliminary provisions such as short title, extent, commencement, application and various definitions of terms used in the statute.

Section 1(4) of the Act excludes from the scope of the Act the documents or transactions listed in the First Schedule. *The First Schedule consists of negotiable instruments, powers-of-attorney, trusts, wills and any contract for the sale or conveyance of immovable property or any interest in the property.*

2. ***Chapter 2*** explains the concept of authentication of electronic records and electronic signature. It describes the working of digital signature in Section 3 of the Act.

3. ***Chapter 3*** deals with electronic governance. Under this chapter, legal recognition is granted to electronic records and electronic signature. The chapter recognises the offline functions of government that takes place in online medium such as publication of gazette(Sec.8). Section 10-A recognises legal and binding nature of online contracts.

4. ***Chapter 4*** deals with attribution, acknowledgment and dispatch of electronic records.

[1] EDI - Electronic Data Interchange. It is a standard format to exchange business information between two organizations electronically instead of using paper documents.
[2] E-Commerce- buying or selling of goods or services including digital products over digital or electronic network.[Consumer Protection Act, 2019]

5. ***Chapter 5*** deals with secure electronic records and secure electronic signatures. A record shall be deemed to be a secure electronic record from such point of time to the time of verification where any security procedure has been applied to an electronic record at a specific point of time. Also, an electronic signature shall be deemed to be a secure electronic signature if

(i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

(ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

6. ***Chapter 6*** deals with regulation of certifying authorities. It has provisions for appointment and functions of Controller, recognition of foreign certifying authorities and the process for granting licence to issue electronic signature certificates. It contains procedures to be followed by certifying authorities and provisions for its suspension, revocation and surrender of licence.

7. ***Chapter 7*** deals with provisions for issuance, suspension and revocation of electronic signature certificates.

8. ***Chapter 8*** lays down the duties of subscribers to the digital and electronic signature certificate. The subscriber has to exercise reasonable care to retain control of his private key.

9. ***Chapter 9*** prescribes various penalties for the offences laid down in the Act. Provisions related to adjudication such as appointment of an adjudicating officer and the factors to be taken into account for by him in adjudging compensation have been laid down.

10. ***Chapter 10*** dealt with Cyber Appellate Tribunal. It is now merged with Telecom Disputes Settlement and Appellate Tribunal [TDSAT] established under section 14 of the Telecom Regulatory Authority of India Act, 1997. *[Refer Finance Act,2017]*

11. Chapter 11 lays down various information technology related offences. Section 70-A deals with notification of National Nodal Agency by Central Government responsible for all measures 73 including research and development relating to protection of Critical

Information Infrastructure. Section 70-B deals with appointment of Computer Emergency Response Team responsible for maintenance of cyber security.

12. ***Chapter 12*** deals with exemption of liability for intermediaries in certain cases.

13. ***Chapter 12-A*** provides for the power of Central Government to notify an Examiner of Electronic Evidence for providing expert opinion on electronic form of evidence before any court or other authority specified.

14. ***Chapter 13*** deals with various miscellaneous provisions. Section 81 of the IT Act states that the provisions of the Act have an overriding effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. However, the proviso to the section states that the Act shall not restrict any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970.

15. The Act originally consisted of four schedules. Third and Fourth Schedule was omitted in 2009. The First Schedule lists the various documents or transactions to which the Act does not apply, and the Second Schedule deals with electronic signature or electronic authentication technique or procedure.

SALIENT FEATURES OF IT AMENDMENT ACT,2008

- The term *'digital signature'* has been replaced with *'electronic signature'* to make the Act more technology neutral.
- A new section has been inserted to define 'communication device' to mean cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text video, audio or image.
- A new section has been added to define cyber cafe as any facility from where the access to the internet is offered by any person in the ordinary course of business to the members of the public.
- A new definition has been inserted for intermediary.
- A new section 10A has been inserted to the effect that contracts concluded electronically shall not be deemed to be unenforceable solely on the ground that electronic form or means was used.
- The damages of Rs. One Crore prescribed under section 43 of the earlier Act of 2000 for damage to computer, computer system etc. has been deleted and the relevant

parts of the section have been substituted by the words, 'he shall be liable to pay damages by way of compensation to the person so affected'.

- A new section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected.
- Sections 66A to 66F have been added to Section 66 prescribing punishment for offences such as obscene electronic message transmissions, identity theft, cheating by impersonation using computer resource, violation of privacy and cyber terrorism.
- Section 67 of the IT Act, 2000 has been amended to reduce the term of imprisonment for publishing or transmitting obscene material in electronic form to three years from five years and increase the fine thereof from Rs.100, 000 to Rs. 500,000.
- Sections 67A to 67C have also been inserted. While Sections 67A and B deals with penal provisions in respect of offences of publishing or transmitting of material containing sexually explicit act and child pornography in electronic form, Section 67C deals with the obligation of an intermediary to preserve and retain such information as may be specified for such duration and in such manner and format as the central government may prescribe.

In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving power to the state to issue directions for interception or monitoring of decryption of any information through any computer resource. Further, sections 69A and B, two new sections, grant power to the state to issue directions for blocking for public access of any information through any computer resource and to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

LAWXPERTSMV. #COMPREHENSIVE NOTES

Information Technology Law including Cyber Laws - Concept, purpose/prospects

CHAPTER – I – PRELIMINARY

Section 1 : IT act extends to the whole of India.

CHAPTER – II : DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE :

Authentication of electronic records (Section 3) : Digital signatures enable the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones. The purpose of a digital signature is the same as that of a **handwritten signature**.

Digital signature means 'authentication of any electronic record by a subscriber by means of an electronic method or procedure'.[3]

Section 3 : specifically stipulates that **any subscriber may authenticate an electronic record by affixing his digital signature.** It further states that any person can verify an electronic record by the use of a public key of the subscriber.

3 Features of Digital Signature :

1. Authentication : It is used to authenticate the source of messages.
2. Integrity : Section 3 mandates *Asymmetric crypto system and hash function* so that a digital signature could not be altered during transmission and ensures the integrity of the message to the sender and receiver.
3. Non-Repudiation :Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

Electronic signature means authentication of any electronic record by a subscriber by means of an electronic technique.[4] A subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which is considered reliable.[5]

[3] Section 2 (1) (p).
[4] Section 2 (1) (ta)
[5] Section 3A (1).

"E-governance represents a new form of governance which needs dynamic laws, keeping pace with the technological advancement. " Comment on the adequacy of the Information Technology Act, 2000 in ensuring effective EGovernance in India.
UPSC 2018.

CHAPTER – III ELECTRONIC GOVERNANCE :

WHAT IS E-GOVERNANCE? The World Bank *defines e-governance* as the use of information and communication technologies by government agencies to transform relations with citizens, business and other arms of the government. It involves information technology enabled initiatives that are used for improving (i) the interaction between government and citizens or government and businesses-e-services (ii) the internal government operations – e-administration and (iii) external interactions – e-society.

WHY IS IT REQUIRED? The Information Technology Act, 2000 has adopted a "functional equivalent approach" in order to extend *offline governmental functions and practices to the online environment.* The idea is to facilitate efficient government-citizen interface by giving due legal recognition to digital signatures and electronic records. E-governance or Electronic Governance is dealt with under Sections 4 to 10A of the IT Act, 2000.

- Legal recognition of electronic records (Section 4) : Where any law require any document to be in printed / handwritten form, notwithstanding that law, this document can be submitted in e-form.
- Legal recognition of digital signatures (Section 5) : Where any law require affixing of signature of the person in a document, notwithstanding that law, it can be made as digital sign.
- E-Governance in Government Transactions (Section 6-10) : Filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form.

- Section 6-A allows Appropriate Government for efficient delivery of services to the public through electronic means authorize any service provider to set up, maintain and upgrade the computerized facilities and perform such other services.
- ELECTRONIC CONTRACTS (Section 10-A) : Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, are expressed in *electronic form or by means of an electronic record*, then such record shall **not** be deemed to be **unenforceable** solely on the ground that such electronic form or means was used for that purpose.

Under the IT Act, 2000 earlier there was no provision relating to e-contract, but the IT (Amendment) Act, 2008 has inserted section 10A which confers the validity on contracts formed in e-form.

CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

- ATTRIBUTION : Section 11 provides that An electronic record will be attributed to the originator - if it was sent by the originator himself / by his/her agent/ or by an information system programmed by or on behalf of the originator to operate automatically.
- ACKNOWLEDGE MENT : Section 12 – acknowledgement of receipt of electronic record by addressee by can done in electronic mode or other modes, which would sufficiently constitute acknowledgement.
- DISPATCH : Section 13 - The dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.

CHAPTER V : Security procedure for electronic records and digital signature (Sections 14, 15, 16)

CHAPTER – VI - CERTIFYING AUTHORITY (CA) AND CONTROLLER OF CA

CERTIFYING AUTHORITY : Certifying Authority" means a person who has been granted a license to issue Digital Signature Certificates. (Sec.24)

- ROLE OF CA : to issue, renew and provide directories of Digital Certificates.

- Provisions with regard to Certifying Authorities are covered under **Chapter VI i.e. Sec.17 to Sec.34** of the IT Act, 2000. It contains detailed provisions relating to the appointment and powers of the Controller and Certifying Authorities.
- Accordingly a prospective CA has to establish the required infrastructure, get it audited by the auditors appointed by the office of Controller of Certifying Authorities, and only based on complete compliance of the requirements, a license to operate as a Certifying Authority can be obtained.

CONTROLLER OF CERTIFYING AUTHORITIES :

- Controller of Certifying Authorities (CCA) is appointed by central government under section 17, to license and regulate the working of Certifying Authorities.
- FUNCTION : Section 18 : To exercise supervision over the activities of the **Certifying Authorities** such as, laying down their **qualifications, standards, duties,** and resolve any conflicts between CA and subscribers.
- Controller to act as repository of all digital signature certificates (Section 20);
- The Controller will also specify the various forms and content of digital signature certificates.
- The Act accepts the need for recognizing foreign certifying authorities and it further details the various provisions for the issuance of license to issue digital signature certificates.

CHAPTER – VII – DIGITAL SIGNATURE CERTIFICATES

DIGITAL SIGNATURE CERTIFICATES : Chapter VII of the Act details the scheme of things relating to digital signature certificates

- Digital certificates are the digital equivalent (i.e. electronic format) of **physical or paper certificates.** *Examples* of physical certificates are driver's licenses, passports or membership cards.
- A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth.
- The certificate can be used to verify that a public key belongs to the individual.

CYBER CRIME – HOLISTIC APPROACH

1. Definition as per United Nations :

- Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.
- Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession [and] offering or distributing information by means of a computer system or network.

2. Information Technology Act : "Cyber Security" is defined under Section (2) (nb) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Chapter IX talks about penalties and adjudication for various offences.

- Appointment of adjudicating officer for holding inquiries under the Act (Sections 46 & 47)
- The Act talks of appointment of an officer not below the rank of a Director to the Government of India or an equivalent officer of a state government as an Adjudicating Officer to judge whether any person has made a contravention of any of the provisions of the Act.
- Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)
- The officer has been given the powers of a civil court

SECTION	OFFENCE	PENALTY
Section 43	Act of destroying, altering or stealing computer system/network or deleting information with act of damaging data or information without authorization	

	of owner of that computer	
Section 43-A	Compensation for negligence in implementing and maintaining reasonable security practices and procedures in relation to sensitive personal data or information ("SPDI").	
Section 65	Tampering with Computer source Documents	3years Imprisonment or Fine of 2 Lakhs or Both.
Section 66	**Hacking** of computer system by individual with dishonesty or fraudulently COMMENT : Hacking means unauthorized attempts to bypass the security mechanisms of an information system or network.	3 yrs imprisonment or fine of Rs. 5,00,000 or both
Section 66A	Sending offensive information with *demean character* or *information* known as false but sent for purpose of causing annoyance, inconvenience, danger, enmity, hatred or criminal intimidation to mislead the recipient	Imprisonment upto 3 years with (or) without fine
Section 66 B	Retains any stolen computer resource or communication device	Same
Section 66 C	Fraudulent use of electronic signature	Same
Section 66D	Cheats by personating by using computer resource (**Identity theft**) COMMENT : Identity theft is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name.	Same

Section 66 E	Violation of privacy by **transmitting image of private area**	Same
Section 66 F	**Cyber Terrorism** affecting unity, integrity security, sovereignity of India through digital medium	Life Imprisonment
Section 67	Publishing obscene information or pornography or transmitting obscene information in public	Imprisonment 5 years or penalty of Rs. 10,00,000 or both
Section 67-A	Publishes or transmits sexually explicit material	5 years imprisonment / 10 lakh fine or both
Section 67-B	Abusing children online	Same as above.
Section 70	Un-authorised access to protected system	10 years imprisonment /fine or both
Section 72	Breach of Confidentiality and Privacy	2 years imprisonment / 1 lakh fine or both
Section 72-A	Disclosure of information in breach of lawful contract or without the information provider's consent.	3 years imprisonment / 5 lakh fine or both
Sec.73 & 74	Publishing false digital signature certificates	2 years imprisonment / 1 lakh fine or both
Section 85	Offences by the Companies	

Chapter XI of the Act talks about various offences, which could 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 that is obscene in electronic form and hacking.

SECTION 66-A AND SHREYA SINGHAL CASE : (VERY IMPORTANT)

Two years ago, on 24 March 2015, online speech or communication got a boost as the Supreme Court declared a draconian provision—Section 66A of the Information Technology Act, 2000—unconstitutional.

FACTS : Shaheen Dhada and Rinu Srinivasan were arrested under Section 66A for criticizing the shut down of Mumbai after the death of Shiv Sena leader Bal Thackeray on social networking website Facebook

- The case came to be known as *Shreya Singhal versus Union of India*, now in the annals of history as a landmark decision in the free speech regime.
- The court struck down Section 66A of the IT Act for being "**open ended, undefined, and vague**" and the words used in the text of the provision being "nebulous in meaning".
- The provision was titled "punishment for sending offensive messages through communication service" and included information shared via a "computer resource or a communication device" known to be "false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will".
- The wide net cast by the section did not go unnoticed by the apex court which said, "Section 66A is cast so **widely that virtually any opinion on any subject would be covered by it, as any serious opinion dissenting** with the mores of the day would be caught within its net."

Cyber-terrorism is a well organized trans-border criminal act, hence a combined domestic law supported by a Global Law may help to address the problem. Discuss. UPSC 2014.

Section 66-F | Cyber Terrorism is punishable with Imprisonment for Life.

ESSENTIAL ELEMENTS : Intention to threaten the unity, integrity, security or sovereignty of India or to strike terror - (A) by denying access or penetrating into computer resource or introduce computer contaminant. (B) obtains access to information, data or computer database relating to security of state/foreign relations.

As per the facts available regarding 26/11 attacks, the perpetrators did access the computers/computer resources available at Trident Hotel and Taj Hotel. Perpetrators by able to access hotels' computer databases came to know the details of the foreign guests, which they otherwise would not have been able to do so. After obtaining the identity of the guests, they selectively chose their targets and caused death or injuries to

large many of guests. Thus, the acts of perpetrators of 26/11 may fall under the category of cyber terrorism.

Information Technology-brought about by Computers, Internet and Cyberspace- has posed new problems in jurisprudence. ' In the context of this statement, critically examine how far our existing laws are deficient in meeting these challenges. **UPSC 2009.**

Ascertainment of Jurisdiction is a big challenge under the cyber law. Elaborate the relevant legal provisions of the Information Technology Act along with various tests applied by the Indian Courts. **UPSC 2019.**

- Write Section 1(2) & Section 75 of the Information Technology Act.[6] + 6 Theories.

Essential Elements of Section 1(2) & Section 75 of IT Ac

1) Offence or Contravention committed.

2) By Any person outside India [Of any nationality]

3) In a computer, computer system or computer network located in India.

There are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity.

SUBJECTIVE TERRITORIALITY - Wherever an activity happens that particular country will have jurisdiction over that activity. Section 2 IPC & Section 177 CrPC.

OBJECTIVE TERRITORIALITY - Where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. It is also known as "EFFECTS DOCTRINE".

[6] **Section 1(2) of IT ACT** | This Act extends to the whole of India and also to any offence or contravention committed outside India by any person.
Section 75. Act to apply for offence or contravention committed outside India.—(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-section (1), 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.

Section 4(3) of Indian Penal Code, 1860. : Any person in any place without and beyond India committing offence targeting a computer resource located in India

Example : A person from Pakistan shoots across the border and an Indian is injured in the process.

SECTION 179 CRPC | When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued.

Section 179 giving statutory recognition to the 'effects' doctrine is squarely applicable in computer crime cases. There would be many situations where we would find that though the initiator of an illegal action is somewhere outside the territory of India, the effect of his digital wrong-doing has caused damage to persons within India

3. NATIONALITY | where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. section 4 of the Indian Penal Code stipulates that the provisions of the Code would also apply to any offence committed by any citizen of India in any place without and beyond India.

4. PASSIVE NATIONALITY | Theory of jurisdiction based on the nationality of the victim.

5. PROTECTIVE PRINCIPLE | Desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. Government is "victim"

6. UNIVERSAL JURISDICTION | A State has jurisdiction to define and prescribe punishment for certain offenses recognized by the community of nations as of universal concern. It includes acts of terrorism, attacks on or hijacking of aircraft, genocide, war crimes etc.

AUTHORITIES UNDER THE IT ACT AND ADJUDICATION

OFFICER → CYBER APPELLATE TRIBUNAL = TDSAT → HIGH COURT → SUPREME COURT : The Act in **Chapter X** talks of the establishment of Cyber Regulations Appellate Tribunal, an appellate body where appeals against the orders passed by the Adjudicating Officers shall be preferred.

Telecom Disputes Settlement and Appellate Tribunal[TDSAT] established under section 14 of the Telecom Regulatory Authority of India Act, 1997.

Section 48-64 of IT Act, 2000 deals with Appellate Tribunal.

- **Sections 49-52-C,53-54 are now Omitted by Finance Act 2017.**
- **Section 48, 52, 55-64 are still in place.**

1. Appeal from order of Adjudicating Officer to **Cyber Appellate Tribunal** [TDSAT] and not to any Civil Court (Section 57)
2. Appeal from order of Cyber Appellate Tribunal to **High Court** (Section 62);
3. Act to apply for offences or contraventions committed outside India (Section 75);
4. Constitution of **Cyber Regulations Advisory Committee** who will advice the Central Government and Controller (Section 88).
5. Section 70-A : The **Indian Computer Emergency Team (CERT – In)** shall serve as the national nodal agency in respect of Critical Information Infrastructure for coordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report.

USE OF SECTION 69-A |
69A. Power to issue directions for blocking for public access of any information through any computer resource. (1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource. (2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed. (3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.
On 29 June 2020, the Modi government banned 59 Chinese mobile apps, most notably TikTok, supported by Section 69A and citing national security interests.
On 24 November 2020, another 43 Chinese mobile apps were banned supported by the same reasoning, most notably AliExpress.

CURRENT AFFAIRS [UPTO AUGUST 2022]

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 framed under section 87 (2) of the Information Technology Act, 2000 to regulate digital content, featuring a code of ethics and a three-tier grievance redressal framework, have come into force (May 26)

Overview of the new rules:

1. It mandates **a grievance redressal system** for over the top (OTT) and digital portals in the country. This is necessary for the users of social media to raise their grievance against the misuse of social media.
2. **Significant social media firms** have to appoint **a chief compliance officer** and have **a nodal contact person** who can be in touch with law enforcement agencies 24/7.
3. **A grievance officer:** Social media platforms will also have to name **a grievance officer** who shall register the grievance within 24 hours and dispose of it in 15 days.
4. **Removal of content:** If there are complaints against the dignity of users, particularly women – about exposed private parts of individuals or nudity or sexual act or impersonation etc – social media platforms will be required to remove that within 24 hours after a complaint is made.
5. **A monthly report:** They also will have to publish a monthly report about the number of complaints received and the status of redressal.

There will be **three levels of regulation for news publishers —** self-regulation, a self-regulatory body, headed by a retired judge or an eminent person, and oversight from the Information and Broadcasting Ministry, including codes of practices and a grievance committee.

LAWXPERTSMV. #REVISION NOTES

Information Technology Law including Cyber Laws - Concept, purpose/prospects

INTRODUCTION :

Why Cyber Law ? To deal with the problems of cybercrimes and recognition of e-commerce in cyber space

1996 - United Nations Commission on International Trade and Law (UNCITRAL)

2000- Information Technology Act, 2000 : gave legal recognition to e-commerce + e-governance.

STRUCTURE OF IT ACT : It has 13 Chapters and 90 sections

CHAPTER – I – PRELIMINARY

Section 1 : IT act extends to the whole of India.

CHAPTER – II : DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE :

Handwritten signature is equated with Digital signature, ensuring authentication based on *Asymmetric crypto system and hash function, which ensures* Non-Repudiation of the signature. (Section3)

CHAPTER – III ELECTRONIC GOVERNANCE :

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

- Document in printed / handwritten form – can be submitted in e-form (Sec.4)
- Hand written signature can be replaced with digital signature (Sec.5)
- E-Governance in Government Transactions (Section 6-10)
- E-contracts can be equated with paper-based contract. (Sec.10-A)

CHAPTER IV - ATTRIBUTION, ACKNOWLEDGEMENT AND DESPATCH OF ELECTRONIC RECORDS

Attribution of electronic record to originator (Section 11) ; acknowledgement of receipt of electronic record by addressee by can done in electronic mode or other modes (Sec.12) ; dispatch means – when e-record goes outside the control of the originator. (Sec 13)

CHAPTER V : Security procedure for electronic records and digital signature (Sections 14, 15, 16)

CHAPTER – VI - CERTIFYING AUTHORITY (CA) AND CONTROLLER OF CA

CERTIFYING AUTHORITY : Certifying authority role is to issue, renew and provide directories of Digital Certificates.(**Chapter VI i.e. Sec.17 to Sec.34)**

CONTROLLER OF CERTIFYING AUTHORITIES : Controller of Certifying Authorities (CCA) is appointed by central government under section 17, to license and regulate the working of Certifying Authorities.

CHAPTER – VII – DIGITAL SIGNATURE CERTIFICATES

DIGITAL SIGNATURE CERTIFICATES : Chapter VII of the Act details the scheme of things relating to digital signature certificates

A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth.

CYBER CRIME – HOLISTIC APPROACH

U.N Definition – Illegal behavior – in relation to, a computer system or network or targets the security of computer systems and the data processed by them.

"Cyber Security" is defined under Section (2) (b) means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction.

Chapter IX talks about penalties and adjudication for various offences.

- Appointment of adjudicating officer for holding inquiries under the Act (Sections 46 & 47)
- The Act talks of appointment of an officer not below the rank of a Director to the Government of India or an equivalent officer of a state government as an Adjudicating Officer to judge whether any person has made a contravention of any of the provisions of the Act.
- Power of police officers and other officers to enter into any public place and search and arrest without warrant (Section 80)
- The officer has been given the powers of a civil court

Refer penalties table in comprehensive notes itself.

Chapter XI of the Act talks about various offences, which could 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 that is obscene in electronic form and hacking.

SECTION 66-A AND SHREYA SINGHAL CASE : (VERY IMPORTANT)

FACTS : Shaheen Dhada and Rinu Srinivasan were arrested under Section 66A for criticizing the shut down of Mumbai after the death of Shiv Sena leader Bal Thackeray on social networking website Facebook

- The case came to be known as *Shreya Singhal versus Union of India*, now in the annals of history as a landmark decision in the free speech regime.
- The court struck down Section 66A of the IT Act for being "**open ended, undefined, and vague**" and the words used in the text of the provision being "nebulous in meaning".

AUTHORITIES UNDER THE IT ACT AND ADJUDICATION

OFFICER → CYBER APPELLATE TRIBUNAL[TDSAT] → HIGH COURT → SUPREME COURT.

Telecom Disputes Settlement and Appellate Tribunal[TDSAT] established under section 14 of the Telecom Regulatory Authority of India Act, 1997.

Section 48-64 of IT Act, 2000 deals with Appellate Tribunal.

- **Sections 49-52-C,53-54 are now Omitted by Finance Act 2017.**
- **Section 48, 52, 55-64 are still in place.**
- Act to apply for offences or contraventions committed outside India (Section 75);
- Constitution of **Cyber Regulations Advisory Committee** who will advice the Central Government and Controller (Section 88)
- Section 70-A : The **Indian Computer Emergency Team (CERT – In)** shall serve as the national nodal agency in respect of Critical Information Infrastructure for coordinating all actions relating to information security practices, procedures, guidelines, incident prevention, response and report.