REMEDIES FOR CONSUMERS UNDER CYBER LAW

ADV. KUNAL TANDON

CYBER LAW – MEANING AND SIGNIFICANCE

Meaning:

Cyber Law is the law governing cyber space. Cyber space is a very wide term and includes computers, networks, software, data storage devices (such as hard disks, USB disks etc), the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

Significance:

With the gradual growth of technology, the ambit of cyber space has expanded many fold. The growth is so significant that the Hon'ble Supreme Court has recognised "informational privacy" as an intrinsic facet of Right to life guaranteed under Article 21 of our Constitution.

Need:

- Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.
- Cyberspace has complete disrespect for jurisdictional boundaries.
- Cyberspace is absolutely open to participation by all.
- Theft of corporeal information (e.g. books, papers, CD ROMs, floppy disks). Electronic records are copied quickly, inconspicuously and often via telecommunication facilities.
- The rapid growth of digital technology and electronic communication had called for legal reforms in India.
- As technology had advanced, the cyber crimes have increased, it was important to create laws to regulate and prevent crimes related to and incidental to technology.

CYBER LEGISLATIONS / FRAMEWORK IN INDIA

- Information Technology Act, 2000
- Indian Penal Code, 1860/Bhartiya Nyaya Sanhita, 2023
- Companies Act, 2013
- Digital Personal Data Protection Act, 2023

HISTORY OF REGULATION OF INFORMATION TECHNOLOGY

- In **1984**, the **United Nations Commission on International Trade Law** at its 17th Session considered a report of the Secretary-General which talked about the legal aspects of automated data processing. This started the flow of work on the legal implications of automated data processing.
- In **1985**, a report by the Secretariat noted that the legal obstacles to the use of computers in international trade arose out of the requirement that the documents had to be signed in paper form.
- Following the report, the commission adopted a recommendation to review the legal requirements of written forms of documents.
- In **1988**, the commission proposed to examine the need to provide legal principles applicable for the formation of international commercial contracts by electronic means.
- With a view to validate the increasing number of transactions in international trade law, the United Nations Commission on International Trade Law adopted the Model Law in Electronic Commerce in 1996.
- As an aftermath, the United Nations General Assembly by its **Resolution No. 51/62 dated 30.01.1997** recommended all the states to adopt the **Model Law in Electronic Commerce** adopted by the **UNCITRAL**.

NATURE OF ADJUDICATION UNDER IT ACT, 2000

- IT Act recognises two kinds of infractions viz. **Cyber Contraventions** and **Cyber Offences**.
- Cyber Contravention is a violation of law or rule dealt appropriately in Chapter IX of the IT Act, 2000, which stipulate penalties and adjudication.
- Cyber Offence is a specific criminal violation, and dealt appropriately under Indian Penal Code and Chapter XI of the IT Act, 2000.

CIVIL JURISDICTION

Section 43 of the IT Act, 2000 prescribes scenarios whereby a computer is accessed without the permission of the owner or any other person who is in charge of a computer (or “computer network” or “computer system”).

Scenarios identified under Section 43:

- If a person downloads or copies any information stored in the system.
- Introduces any virus to the computer system.
- Disrupts the system.
- Denies access to the owner or person authorized to use the computer.
- Tampers or manipulates the computer system.
- Destroys, deletes or makes any alteration to the information stored in the system.
- Steals the information stored therein.
- Assists a third person to facilitate access to a computer, computer system or network in contravention of the IT Act.

CIVIL JURISDICTION

- **Section 43** of the IT Act prescribes damages by way of compensation to be paid to the person affected.
- Such claim for compensation can be filed before the Adjudication Officer appointed under **Section 46** of the Act.
- Remedy under Section 43 is in addition to any criminal liability qua the said offending action.
- **Recent Example**- Reliance Jio registered an FIR against a computer course dropout from Rajasthan for data theft under Sections 43(2) and 66 of the IT Act, 2000 and Section 379 of the Indian Penal Code.

CIVIL JURISDICTION

Section 43A: Compensation in the case of failure to protect data

If any corporation or company has stored the data of its employees or other citizens or any sensitive data in its computer system but fails to protect it from hackers and other such activities, it shall be liable to pay compensation.

Section 44: Failure to furnish the required information

- Failure to furnish any document, return or report to the Controller, the Certifying Authority would invite penalty ranging from Rupees 1.50 Lacs for each failure;
- Failure to file any return or furnish any information, books or other documents within specified time, would invite the penalty Rupees 5000 for every day during such failure.

Section 45: Residuary Penalty

If any person contravenes any provision of this Act and no penalty or compensation is specified, he shall be liable to pay compensation or a penalty of Rupees 25000.

ADJUDICATING OFFICER

- **Section 46** prescribes the appointment of an Adjudicating Officer by the Central Government exercising jurisdiction to adjudicate matters of compensation for the injury/damages suffered by cyber contraventions.
- The pecuniary jurisdiction of the adjudicating authority does not exceed Rs. 5 Crore.
- Above Rs. 5 Crores, jurisdiction has been vested with competent Court.
- The Adjudicating Officer shall exercise the power of the civil court as conferred to the Appellate Tribunal under **sub-section (2) of Section 58**.
- The adjudicating Authority shall be a civil court for the purposes of execution of decrees and orders.

POWERS OF ADJUDICATING AUTHORITY

- **Rule 4** of Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003 prescribes scope and manner of enquiry by the Adjudicating Officer
- The **Adjudicating Officer** shall exercise jurisdiction in respect of the contraventions in relation to Chapter IX of the IT Act.
- Similar to a Civil Court, the Adjudicating officer also has the power to summon parties and witnesses, to sift and weigh the evidence.
- To hear and decide on every application, as far as possible, in **4 months** and the whole matter in **6 months**.
- In a case, the Adjudicating Officer is convinced that the scope of the case extends to the offences under Chapter XI of the IT Act instead of contravention, needing appropriate punishment instead of mere financial penalty, should transfer the case to the magistrate having jurisdiction to try the case, through the Presiding Officer.

POWERS OF ADJUDICATING AUTHORITY

Duplicity Avoided

- Rule 9 provides that any matter of contravention pending before the Adjudicating Officer, same matter may not be pursued before any court or Tribunal or Authority.
- If there is a report filed already, proceedings before any other court or tribunal or Authority shall be deemed to be withdrawn.

COMPOUNDING OF CONTRAVENTIONS

- **Rule 11** of the Rules prescribe powers of the Adjudicating officer to compound contravention, an application for compounding the contravention may be made by person against whom a report of contravention has been filed.
- An anticipatory application for compounding can also be made before the filing of any report of contravention.
- The person making the Application for compounding must deposit the sum determined by the Adjudicating officer as a compounding fee. The Compounding fee cannot exceed the maximum penalty amount.

APPEAL FROM THE ADJUDICATING AUTHORITY

- The IT Act established the Cyber Appellate Tribunal having Appellate jurisdiction against the orders of the Adjudicating Authority.
- Part XIV of Chapter IV of the **Finance Act, 2017** vested the appellate jurisdiction under IT Act, in the Telecom Disputes Settlement and Appellate Tribunal [“**TDSAT**”].
- Statistics show that since the jurisdiction has been vested with the Hon’ble TDSAT a total of **196** cyber appeals have been instituted out of which **75** have been duly disposed off, despite the fact that COVID-19 impacted the functioning of the Court.
- **Section 57** of the Act allows the person aggrieved by Order passed by the controller/adjudicating authority to file an appeal before the Appellate Tribunal.
- The limitation to file an appeal against the order passed by the Adjudicating Authority is 45 days from receiving the copy of the order.

APPEAL FROM APPELLATE TRIBUNAL

- **Section 62** provides that any person aggrieved by any decision or order of the Appellate Tribunal may file an appeal before the High Court within 60 days of such decision or Order passed on any question of fact or law arising out of such Order.

OFFENCES UNDER CHAPTER XI OF IT ACT, 2000

- Section 65: Tampering with computer source documents.
- Section 66-C: Punishment for identity theft.
- Section 66-D: Punishment for cheating by personation by using computer resource.
- Section 66-E: Punishment for violation of privacy.
- Section 66-F: Punishment for cyber terrorism.
- Section 67: Punishment for publishing or transmitting obscene material in electronic form.
- Section 67-A: Punishment for publishing or transmitting of material containing sexuality.
- Section 67-A: Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
- Section 67-B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

COMPANIES ACT, 2013:

- The Serious Frauds Investigation Office (SFIO) established under Section 211 of Companies Act**,** can now prosecute Indian companies and their directors for cyber frauds under the Companies Act of 2013.
- With the Companies Inspection, Investment, and Inquiry Rules, 2014, the SFIO has become stricter in handling cyber fraud cases.
- The law covers various areas of regulatory compliance, including cyber forensics, e-discovery, and cybersecurity diligence.
- The Companies (Management and Administration) Rules, 2014 set strict cybersecurity standards and hold company directors and executives responsible for ensuring compliance.

INDIAN PENAL CODE (IPC), 1860
BHARTIYA NYAYA SANHITA, 2023

IPC	BNS
➢ Section 464: Making a false documents ➢ Section 465: Forgery ➢ Section 468: Forgery intended to cheat ➢ Section 469: Harming someone's reputation ➢ Section 471: Using a fake document as real	➢ 335. Making a false document. ➢ 336(2): Whoever commits forgery shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both. ➢ 336(3): Whoever commits forgery, intending that the document or electronic record forged shall be used for the purpose of cheating, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine ➢ 336(4): Whoever commits forgery, intending that the document or electronic record forged shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine. ➢ 340. Forged document or electronic record and using it as genuine.

DIGITAL PERSONAL DATA PROTECTION ACT 2023

- The Data Protection Legislation can be traced back to 2017 when an expert Committee was Constituted by the Ministry of Electronics and Information Technology (Meity).
- In the matter of "*Justice K.S. Puttaswamy (Retd.) & Another vs. Union of India & Ors.*" the Hon'ble Supreme Court of India has recognized a fundamental right to privacy in India, including informational privacy, within the "right to life" provision of India's Constitution. In this judgment, a nine-judge bench of the Hon'ble Supreme Court urged the Indian Government to put in place "a carefully structured regime" for the protection of personal data.
- The Hon'ble Supreme Court in K.S. Puttaswamy (supra) affirmed that privacy (including informational privacy) was protected under the Constitution of India. More practically, the decision played a role in forcing the hand of the executive to create legislation on privacy and data protection.
- Finally, on 3rd August 2023, The Lok Sabha introduced the Digital Personal Data Protection Bill, 2023 on 3rd August 2023 to provide for the processing of digital personal data which not only recognizes the right of individuals in protecting their personal data but the need to process such personal data for any lawful purposes.
- Until the President of India gave her assent on **Digital Personal Data Protection Act 2023 (DPDA Act)** on 11th August 2023, **The Information Technology Act, 2000 (IT Act)** was the data protection legislation in India because there was no special legislation.

KEY HIGHLIGHTS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Intent

An Act to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

Applicability of the Digital Personal Data Protection Act 2023

The Act applies to the processing of digital personal data within India's territory, whether collected in digital or non-digital form and digitized subsequently.

Act also applies to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India.

The Act is not applicable to personal data processed by an individual for any personal or domestic purpose and personal data which is made publicly available by Data Principal.

KEY HIGHLIGHTS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Section 2 (a) : Appellate Tribunal

Appellate Tribunal means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997;

Section 2 (c) : Board

“Board” means the Data Protection Board of India established by the Central Government under section 18.

Section 2 (h): Data

“Data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means.

Section 2 (i): Data Fiduciary

“Data Fiduciary” means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.

KEY HIGHLIGHTS OF THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

Section 2 (j): Data Principle

"Data Principal" means the individual to whom the personal data relates and where such individual is—

(i) a child, includes the parents or lawful guardian of such a child.

(ii) a person with disability, includes her lawful guardian, acting on her behalf.

Section 2 (t): Personal Data

"personal data" means any data about an individual who is identifiable by or in relation to such data.

Section 2 (u) : Personal Data Breach

"personal data breach" means any unauthorized processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data.

OBLIGATIONS OF DATA FIDUCIARY

A data fiduciary plays a vital role in the processing of personal data and the onus of protection of those data lies with data fiduciary.

> Example: Data fiduciary may be your telephone operator, Myntra, Amazon, Matrimony website, or any other person or organization with whom you have shared your personal data.

A data fiduciary may process the personal data of an individual in accordance with the provisions of the Act and for a lawful purpose for which the consent is given or for certain legitimate use.

While asking for consent from a data principal, a data fiduciary shall also give notice beforehand or at the moment informing the purpose of data processing, rights of data principal and manner in which the data principal may make a complaint to the Board.

A data Fiduciary is a duty bound to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent a personal data breach.

In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.

SIGNIFICANCE OF DATA FIDUCIARY

Section 2(z): Significant Data Fiduciary

"Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10.

The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.

The Significant Data Fiduciary shall —

- appoint a Data Protection Officer who shall be the point of contact for the grievance redressal mechanism under the provisions of this Act;
- appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary.
- carry a periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals.
- carry out a periodic audit.

RIGHTS AND DUTIES OF DATA PRINCIPAL

Rights of Data Principal

- to access information about personal data .
- Right to correct, complete, update and erasure of the personal data provided.
- Right to nominate any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data.
- Right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager Duties.

Duties of Data Principal

- Comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act.
- to ensure not to register a false or frivolous grievance or complaint.
- to ensure not to suppress any material information while providing personal data for any document.
- to ensure not to impersonate another person while providing personal data for a specified purpose.

DATA PROTECTION BOARD AND IT'S FUNCTIONS

- **Data Protection Board**
  The Data Protection Board of India is established by the Central Government.
  The Board is a body corporate with perpetual succession, a common seal, and powers to acquire, hold, dispose of property, contract, sue, and be sued.
  The headquarters of the Board is determined by the Central Government.
  Central Government is in consultation with stakeholders and is likely to form the board within a month.

- **Key functions of the Board include**
  Monitoring compliances and imposing penalties.
  Directing data fiduciaries to take necessary measures in the event of data breach.
  Hearing grievances made by affected persons.

- **Authority of Data Protection Board**
  Inspect documents of Companies handling personal data.
  Summon and examine individuals under oath.
  Recommend blocking access to intermediaries that repeatedly breach the provisions of the bill.

APPEAL & DISPUTE RESOLUTION UNDER DPDP ACT

- Any person aggrieved by an order or direction made by the Board under this Act may prefer an appeal before the Appellate Tribunal i.e. Telecom Dispute Settlement and Appellate Tribunal.
- Every appeal shall be filed within a period of sixty days from the date of receipt of the order or direction appealed against.
- An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.
- The Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.
- If the Board is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

PENALTIES AND ADJUDICATION

If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the person an opportunity of being heard, impose such monetary penalty specified in the Schedule.

All sums realised by way of penalties imposed by the Board under this Act, shall be credited to the Consolidated Fund of India.

As per Schedule, the penalty imposed upon Breach of provisions of this Act or rules made thereunder are as follows:

- **Extend to Rupees 250 Crore** - Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach.
- **Extend to Rupees 200 Crore** - Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach.
- **Extend to Rupees 200 Crore** - Breach in observance of additional obligations in relation to children.
- **Extend to Rupees 150 Crore** - Breach in observance of additional obligations of Significant Data Fiduciary.
- **Extend to Rupees 10,000/-** Breach in observance of the duties.
- **Extend to rupees 50 Crore** - Breach of any other provision of this Act or the rules made thereunder.

THE PROTECTION OF CHILDREN FROM SEXUUAL OFFENCES ACT, 2012

- Cyber Crime is not define in any statute/legislation.
- POCSO Act, 2012 was passed to defend children from sexual offences while additionally also keeping in mind to secure the interest of child at each and every stage of judicial process.
- The act defines a child as any person below the age of 18 years, and regards the best interests and welfare of the child as being of paramount importance at every stage, to ensure the healthy, physical, emotional, intellectual and social development of the child.
- It defines different forms of sexual abuse, penetrative and non-penetrative assault, as well as sexual harassment and pornography, and deems such sexual assault to be aggravated under certain circumstances, such as when the abuse child is mentally ill or when the abuse is committed by a person in a position of trust or authority vis-à-vis a child, like a family member, police officer, etc.

POCSO vis-à-vis IT ACT

The Hon’ble Supreme Court in its recent judgment dated 23rd September 2024 in the matter of *Just Rights for Children Alliance & Anr. Vs. Union of India* [Crl. Appeal Nos. 2161-2162 of 2024] has explained in detail the relation between IT Act and POCSO Act.

The Hon’ble Supreme Court has held that viewing, possessing and not reporting possession of any child pornographic material will constitute offences under POCSO Act and IT Act

The Hon’ble Supreme Court has issued number of suggestions to the Union of India as well as courts, inter alia, refraining all concerned stakeholders from using the term “child pornography” and use “child sexual exploitation and abuse material [**CESAM**]”

ARTIFICIAL INTELLIGENCE VIS-À-VIS IT ACT

On 15th March 15, 2024, the Ministry of Electronics and Information Technology (hereinafter “MeitY”), has issued new advisory titled “Due diligence by Intermediaries/Platforms under the Information Technology Act, 2000” for the regulation of Artificial Intelligence (“AI”) models, software, or algorithms used by intermediaries or platforms vide issuance of Advisory and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,2021 (“IT Rules”)” .

The 15th March Advisory supersedes the earlier advisory of 1st March 2024 which mandated intermediaries and platforms to get explicit permission of government of India before use or deploying “under-tested” or “unreliable” AI models and tools in the country.

Significantly, Rule 3(1)(b) of the IT Rules dealing with the due diligence section mandates intermediaries to communicate their rules, regulations, privacy policy, and user agreement in the user’s preferred language. They are also obliged to ensure reasonable efforts to prevent users from hosting, displaying, uploading, modifying, publishing, transmitting, storing, updating, or sharing any information related to eleven (11) listed user harms or content prohibited on digital intermediaries.

ARTIFICIAL INTELLIGENCE VIS-À-VIS IT ACT

Features of 15th March Advisory:

All Intermediaries and Platforms are advised to ensure compliance with the following:

To ensure that use of AI model/LLM/Generative AI, software or algorithm on or through its computer resource does not permit its users to host, display, upload, modify, publish, transmit, store, update or share any unlawful content.

To ensure that their computer resources in itself or through the use of AI model/LLM/Generative AI, software or algorithm do not permit any bias or discrimination or threaten the integrity of the electoral process.

The use of under-testing / unreliable Artificial Intelligence model /LLM/Generative AI, software or algorithm and its availability to the users on Indian Internet should be made only after appropriately labeling the possible inherent fallibility or unreliability of the output generated.

The ‘consent popup’ or equivalent mechanisms may be used to explicitly inform the users about the possible inherent fallibility or unreliability of the output generated.

All users must be clearly informed including through the terms of services and user agreements of the intermediary or platforms about the consequence of dealing with the unlawful information, including disabling of access to or removal of non-compliant information, suspension or termination of access or usage rights of the user to their user account, as the case may be, and punishment under applicable law

THANK YOU