CHAPTER 9

CYBER CONTRAVENTIONS, ADJUDICATION, APPELLATE TRIBUNAL AND OFFENCES

CHAPTER OUTLINE

9.1 INTRODUCTION

The Act has provided legal protection to the owner of computer resources against cyber crimes. Any illegal act or unauthorized use of the computer system constitutes cyber crime. It may be in the form of contravention or offence. Secs. 43 to 47 of the Act deal with contraventions, penalties and their adjudication. Chapter X of the IT Act, 2000 provides for the establishment of Cyber Appellate Tribunal to exercise jurisdiction, powers and authority as conferred under the Act.

9.2 PENALTIES AND COMPENSATION

Chapter IX of the Act provides for the following penalties :

1. **Penalty and compensation for damage to computer, computer system (CS) or computer network (CNW) (Sec. 43).** This section states that if a person commits any of the following prohibited acts, he shall be liable to pay damages by way of compensation not exceeding ₹ 1 crore to the affected party :

   (*i*) **Access without authority.** If he accesses or secures access to such computer, computer system or computer network.

   (*ii*) **Downloading, copying or extracting any data without authority.** If he downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network.

   (*iii*) **Introduction of computer contaminant/virus.** If he introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network including information or data held or stored in any removable storage medium.

   (*iv*) **Damage to computer database.** If he damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network.

   (*v*) **Disruption of computer, computer system or computer network.** If he disrupts or causes disruption to the stated computer resources.

   (*vi*) **Denial of access.** If he denies or causes to denial of access to any person authorized to access any computer, computer system or computer network by any means.

   (*vii*) **Providing assistance to facilitate access.** If he provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder.

   (*viii*) **Charging the services to the account of another.** If he charges the services availed of by a person to the account of another person by tempering with or manipulating any computer CS or CNW.

   (*ix*) **Destruction, deletion or alteration or information.** If he destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means.

(*x*) **Stealing, concealing or destroying computer source code.** If he steals, conceals, destroys or alters or causes any person to steal, conceal, destroy, or alter any computer source code used for a computer resource with an intention to cause damage. [Inserted vide ITAA, 2008].

Explanation of terms used under section 43

(*i*) "**Computer Contaminant**" means any set of computer instructions that are designed (*a*) to modify, destroy, record, transmit data or programme residing within a computer, CS or CNW ; or (*b*) to seize illegally by any means the normal operations of the computer, or CNW.

(*ii*) "**Computer Database**" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized manner or have been produced by a computer, CS or CNW and are intended for use in a computer, CS or CNW.

(*iii*) "**Computer Virus**" means any computer instruction, information, data or programme that destroys, damages and degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource.

(*iv*) "**Damage**" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(*v*) "**Computer Source Code**" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

2. Compensation for failure to protect data [43A, Inserted vide ITAA, 2008]. This section provides that if a body corporate, processing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages by way of compensation **not exceeding ₹ 5 crore to the affected party**.

Explanation of terms used under section 43A

(*i*) "**Body Corporate**" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

(*ii*) "**Reasonable Security Practices and Procedures**" means security practices and procedures designed to protect such information from

unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies, or associations as it may deem fit.

(*iii*) "**Sensitive Personal Data or Information**" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

3. Penalty for failure to furnish information, return or report (Sec. 44). This section provides for the following penalties for a person who has to fulfil some legal requirements under this Act, rules or regulations made thereunder :

(*i*) **Penalty for failure in furnishing any document, return or report to CCA or CA.** He shall be liable to a penalty **not exceeding ₹ 1,50,000 for each such failure.**

(*ii*) **Penalty for failure in filing return or furnishing information, books or other documents within the specified time.** He shall be liable to a penalty **not exceeding ₹ 5,000 for every day during which such failure continues.**

(*iii*) **Penalty for failure in maintenance of books of account or records.** He shall be liable to a penalty **not exceeding ₹ 10,000 for every day during which the failure continues**.

4. Penalty for contravention of rules or regulations (Sec. 45). This section provides that if any person contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been prescribed, he shall be liable to pay compensation **not exceeding ₹ 25,000** to the person affected by such contravention.

9.3 JUSTICE DISPENSATION SYSTEM FOR CYBER CRIMES UNDER IT ACT, 2000

The IT Act, 2000 provides the following authorities for justice dispensation system for cyber crimes.

- Controller of Certifying Authorities (CCA)
- Adjudicating Officer (AO)
- Appellate Tribunal (AT)
- High Court

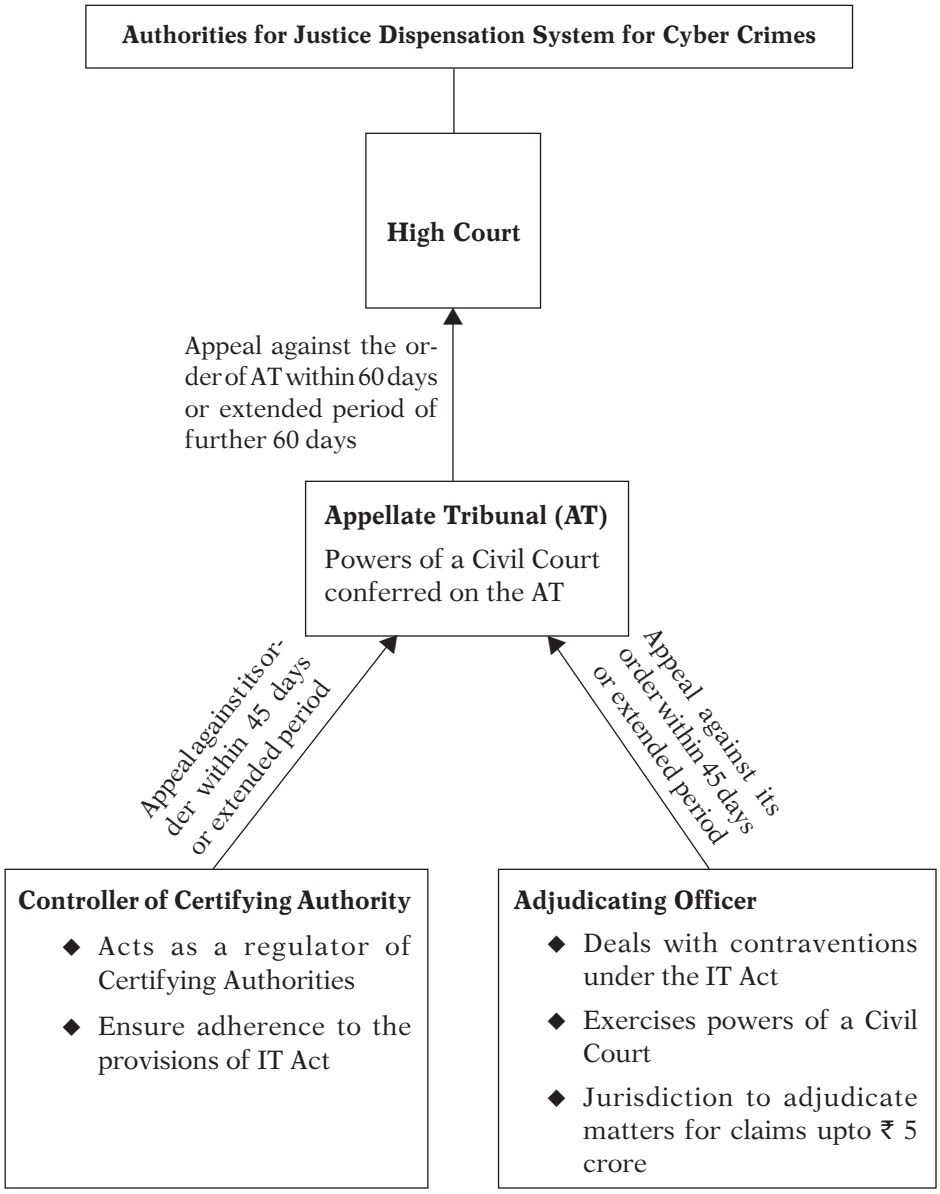

FIG. 9 : JUSTICE DISPENSATION SYSTEM FOR CYBER CRIMES UNDER IT ACT, 2000

Note : various provisions relating to CCA have been explained in Chapter 8