

CYBER CRIMES AND AVAILABLE REMEDIES

AT GANGTOK ON 17.02.2024

**BY HIMANSHU DHAWAN,
ADVOCATE**

FOUNDER | PARTNER



Utkrishtha Law Offices

Advocates & Solicitors

CYBER CRIME AND ITS CATEGORIES

“Any unlawful act where computer or communication device or computer network is used to commit or facilitate the commission of a crime”.

Categories of Cyber Crimes

Financial Cyber
Crimes

Non-Financial
Cyber Crimes



Utkrishtha Law Offices
Advocates & Solicitors

EXAMPLES OF CYBER CRIMES:

FINANCIAL CYBER CRIMES

- Data Theft/Damage to Computer Computer Systems Etc.
- UPI and OTP related frauds
- Malware or Ransomware Attacks
- Tampering with Computer Source Documents.

NON-FINANCIAL CYBER CRIMES

- Identity Theft
- Cyber Stalking
- Cyber Bullying
- Cyber Terrorism



Utkrishtha Law Offices
Advocates & Solicitors

“DATA” AND “DATA THEFT”

- Under Section 2 (o) of the IT Act, 2000, ‘**Data**’ means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and maybe in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.
- **Data theft** is the unauthorized acquisition of valuable or personal information from an organization, compromising privacy and obtaining confidential data. This includes hacking passwords, accessing banking and personal customer information, and exploiting sensitive data such as trade secrets or government databases.
- Section 43 of the IT Act, 2000 specifically defines, what constitutes the unauthorized access of the Computer Systems by a person without the permission of the owner of the computer systems.

SECTION 43 OF THE IT ACT, 2000

If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network accesses or secures access to such computer, computer system or computer network (b)downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) 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; (e) disrupts or causes disruption of any computer, computer system or computer network;(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) 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; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network; (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) steal, conceal, 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; he shall be liable to pay damages by way of compensation to the person so affected.

RECOVERY OF DAMAGES UNDER THE IT ACT, 2000

- For the purpose of determining that whether “any person” has committed a contravention of any of the provisions of this Act or of any rule, regulation, the Central Government shall appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer for holding an inquiry in the manner prescribed by the Central Government.
- The adjudicating officer appointed under shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore, Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court.
- The adjudicating officer shall, after giving the person referred hereinabove a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

FIRST APPELLATE JURISDICTION OF “TDSAT”

Any person aggrieved by an order made by an adjudicating officer under this Act may prefer an appeal before The TDSAT, within 45 Days of the receipt of the copy of the Order. The Telecom Disputes Settlement and Appellate Tribunal established under Section 14 of the TRAI Act, 1997 shall, be the Appellate Tribunal for the purposes of this Act and the said Appellate Tribunal shall exercise the jurisdiction, powers and authority conferred on it by or under IT Act with a Chairperson and any additional members appointed by the Central Government. Sub-clause (1) Section 58 of the IT Act, 2000 states that the TDSAT is not bound by the Code of Civil Procedure, 1908, but rather by the principles of natural justice, and the Tribunal has the authority to regulate its own procedure, including the location of its hearings. *Second Appeal Lies before High Court within 60 days of the order passed by the TDSAT, New Delhi.*



Utkrishtha Law Offices
Advocates & Solicitors

INITIATIVES TAKEN BY THE GOVERNMENT OF INDIA TO CURB CYBER CRIMES

- The Central Government has taken steps for spreading awareness about cybercrimes, issuance of alerts/ advisories, improving cyber forensic facilities etc. The Government has established Indian Cyber Crime Coordination Centre (I4C) to provide a framework and eco-system for its officials to deal with the cyber crimes in a comprehensive and coordinated manner. The Government has launched the National Cyber Crime Reporting Portal, to enable public to report incidents pertaining to all types of cyber crimes, with a special focus on cyber crimes against women and children.
- A toll-free number “155260” has been operationalized to get assistance in lodging online cyber complaints. Citizen Financial Cyber Fraud Reporting and Management System module has been launched for immediate reporting of financial frauds and to stop siphoning off fund by the fraudsters.
- The Indian Computer Emergency Response Team (CERT-In) is serving as national agency for responding to cyber security incidents as per provisions of Section 70B of Information Technology Act, 2000. CERT-In receives inputs from its situational awareness systems and threat intelligence sources about malware infections in networks of entities across sectors. Whenever any incident comes to the notice of CERT-In, it issues alerts and advisories to the entities concerned and sectoral Computer Emergency Response Teams (CERTs) for remedial measures.

THANK YOU!



Utkrishtha Law Offices
Advocates & Solicitors