VOLUME 29 | APRIL, 2022 ISSN 2456-9704

CYBERCRIMES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

By Aksharaa Saxena and Sirla Harshitha das
From IFHE – ICFAI LAW SCHOOL, Hyderabad

IT Act, 2000 is a primary law in India that deals with cybercrime and electronic commerce. It is based on the United Nations Model on Electronic Commerce based on Cybercrime, 1996. In India, the bill was finalised by the group of ministers headed by the Minister of Technology Mr.Promod Mahajan and the bill was passed by the President of India at that time Mr K.R. Narayanan on 9th May 2000. The laws are applicable across India.

Other acts were also changed/updated after the commencement of IT ACT, 2000. It also established the cyber Appellate Tribunal to resolve disputes arising from the new law. it also defines Cybercrimes and prescribed penalties for them. The uniqueness of this Act is that any person who is in or out of India has access to the Indian networks and tampers with it intending to cause harm will be liable under this law.

As our country progresses towards the digital age, where people are dependent on technology more than usual, there must be strict and advanced laws to protect the sensitive information of the people. It is an irony that the data can be stolen and used for malicious purposes from the most trusted sources as well. In a technologically advanced country, cybercrimes are most common and menacing at the same time. In the IT Act of 2000, there are all types of cybercrimes covered including hacking.
Hacking is the gaining of unauthorized data from others without their consent. There are two types of hackers —- hackers and crackers. Crackers are the ones who do the work illegally and cause damage to sensitive information and use it for themselves or other malafide purposes. A hacker is a person who is a somewhat good person or a group who does hacking for a good reason and to get additional information from it. They for the most part observe loopholes in the framework and assist them with covering the provisos. They are for the most part developers who acquire advanced information about working frameworks and programming dialects. These individuals never harm or mischief any sort of information. In the year 2008, the IT Act was amended and the word hacker was removed which was mentioned in Section 43 of the act as there are a lot of professionals who teach ethical hacking and anything taught at the place of education is not illegal.

There have been many cases logged in India regarding cybercrimes. As there are many social media users where people need to create their accounts by providing their pieces of information like phone numbers, emails, allowing access to track locations, etc. which has become a cakewalk to the crackers to steal the information and threaten the public. There are money scams and frauds, online mode of transactions are the easiest and most convenient way of money transfers and it has become really easy for an unethical hacker to take down the bank servers, steal money from one account, scam with fake and fraudulent messages and so on. If a person knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal destroy

or alter any computer source code used for a computer, computer program from a computer system or computer network when the computer source code is required to be kept or maintained by the law for time being in force. [1]

Academicians have a perspective that it is challenging to demonstrate goal to cause unjust misfortune or harm in the electronic climate and Internet. The words "wrongful loss" isn't characterized under the IT Act, 2000. Notwithstanding, Section 23 of the Indian Penal Code characterizes "wrongful loss" to imply "misfortune by unlawful method for property to which the individual "loss by unlawful means of property to which the person losing it is legally entitled".

Section 43A of the IT Act manages the common responsibility of digital wrongdoers. The segment manages the remuneration that ought to be made for disappointment of security of the data. His was presented under the alteration of the demonstration in 2008. The corporate obligation regarding information insurance is enormously underlined by embedding Section 43A by which corporate are under a commitment to guarantee reception of sensible security rehearses. Further, what is touchy individual information has since been explained by the focal government vide its Notification dated 11 April 2011 giving the rundown of all such information which incorporates secret phrase, subtleties of ledgers or card subtleties, clinical records, and so forth.[2]
Punitive responsibility of breaking emerges when the goal or the obligation of the saltine to hurt the framework or take any significant data gets laid out. Assuming the saltine just sins the framework with practically no aim to hurt, it just remaining parts a type of common responsibility under area 43A. The lawbreaker trespass can likewise bring about other reformatory exercises culpable under the Indian Penal Code like digital burglary that can be culpable under segment 378 of Indian Penal Code.[3]

If a person denies access to the computer sources or hinder or threatens the unity, integrity, sovereignty or security of India then he commits cyber terrorism and extends his punishment to life imprisonment.[4] Some punishments extend to 2 years for publishing or promoting obscene material in the electronic form and the punishment may also extend to paying a fine of Rs.25,000.[5]

The other provisions to be safeguarded under this Act are :

1. Digital Signatures
2. Fradulental Digital Certificates
3. Electronic Records[6]

FILING A COMPLAINT –

A complaint about digital wrongdoing can be recorded at any cyber cell universally. There are different digital cyber cells in India; a protest can be filled at any of these

Right off the bat compose an application to the top of the digital cell division and the details shall contain the name, address, email and phone number.

[1] SECTION 65, IT ACT
[2] Civil liability
[3] Criminal liability
[4] Sec 66F
[5] Sec 67
[6] Sec 73-75

Also, present the accompanying reports with the cell;

1. **Server logs**- Log documents that get consequently with the server when records are opened. It saves a rundown of exercises performed on an everyday basis.
2. **The printed version and a delicate duplicate of the absconded material**- Every material that has been tampered with by the programmer should be submitted with the digital cell as proof.
3. **A printed copy of the first website pages and the defaced ones**- Duplicates of both the first and ruined material ought to be submitted with the goal that it makes the work simple to find the damaged or altered material.
4. Details of the control mechanism where the complainant needs to tell the details of those who had the access to the password and the computer.
5. Assuming there is any doubt on an individual, a rundown of the suspects ought to likewise be given for additional reference that could help the digital cell in the examination.

CASE LAWS

Shreya Singhal v. UOI (2013) 12 SCC 73

In the above case, the validity of Section 66A of the IT Act was challenged before the Supreme Court. (Punishment for sending offensive messages through communication service, etc. -Any person who sends, by means of a computer resource or a communication device,-

(a) any information that is grossly offensive or has menacing character)

Facts: Two ladies were arrested under Section 66A of the IT Act after they posted purportedly hostile and offensive remarks on Facebook concerning the total closure of Mumbai after the demise of a political pioneer. Section 66A of the IT Act gives discipline in the event that any individual utilizing a computer asset or correspondence, such data which is hostile, misleading, or causes irritation, burden, risk, affront, scorn, injury, or malevolence.

The ladies, because of the capture, recorded a request testing the defendability of Section 66A of the IT Act on the ground that it is violative of the right to speak freely and with articulation.

Judgment: The Supreme Court put together its decision with respect to three ideas specifically: conversation, backing, and affectation. It saw that simple conversation or even backing of a reason, regardless of how disagreeable, is at the core of the right to speak freely and articulation. It was observed that Section 66A was equipped for limiting all types of correspondence and it contained no qualification between simple promotion or conversation on a specific reason which is hostile to some and prompting by such words prompting a causal association with public turmoil, security, wellbeing, etc.

Shamsher Singh Verma v. State of Haryana 2015 SCC OnLine SC 1242

In this case, the accused filed an appeal to the Supreme Court after the High Court rejected the accused's application to have the forensic laboratory display and verify the compact disc submitted for defence.

The Supreme Court held that a Compact Disc is also a document. It further observed that it is not necessary to obtain admission or denial concerning a document under Section 294

(1)[7] of CrPC personally from the accused, the complainant, or the witness.

Shankar v. State Rep Crl. O.P. No. 6628 of 2010

Facts: The candidate moved toward the Court under Section 482, CrPC to subdue the charge sheet recorded against him. The applicant tied down unapproved admittance to the safeguarded arrangement of the Legal Advisor of Directorate of Vigilance and Anti-Corruption (DVAC) and was charged under Sections 66, 70, and 72 of the IT Act.

Judgement: The Court observed that the charge sheet filed against the petitioner cannot be quashed with respect to the law concerning non-granting of sanction of prosecution under Section 72 of the IT Act.

Avnish Bajaj v. State (NCT) of Delhi (2008) 150 DLT 769

Facts: Avnish Bajaj, the CEO of Bazee.com was arrested under Section 67 of the IT Act for the telecom of digital erotic entertainment. Another person had sold duplicates of a CD containing obscene material through the bazee.com site.

Judgement: The court found that Mr Bajaj was not involved in the broadcast of pornographic material. In addition, pornographic material could not be viewed on the Bazee.com website. However, Bazee.com receives commissions from sales and profits from the ads served through its website. The
court further stated that the evidence collected indicates that cyberporn crimes are not attributed to Bazee.com, but someone else. The court granted Mr Bajaj's bail on bail, provided that the two bail bondsman each provided 10,000 rupees. However, the defendant is liable that he was merely a service provider and did not provide the content.

CBI v. Arif Azim (Sony Sambandh case)

A website called www.sony-sambandh.com enabled NRIs to send Sony products to their Indian friends and relatives after online payment for the same. In May 2002, someone logged into the website under the name of Barbara Campa and ordered a Sony Colour TV set along with a cordless telephone for one Arif Azim in Noida. She paid through her credit card and the said order was delivered to Arif Azim. However, the credit card agency informed the company that it was an unauthorized payment as the real owner denied any such purchase.

A complaint was therefore lodged with CBI and further, a case under Sections 418, 419, and 420 of the Indian Penal Code, 1860 was registered. The investigations concluded that Arif Azim while working at a call centre in Noida, got access to the credit card details of Barbara Campa which he misused.

The Court convicted Arif Azim but being a young boy and a first-time convict, the Court's approach was lenient towards him. The Court released the convicted person on probation for 1 year. This was one of the landmark cases of Cyber Law because it displayed that the Indian Penal Code, 1860 can be effective legislation to rely on when the IT Act is not exhaustive.[8]

[7] Obscene acts and songs.

[8]REFERENCES

Enhelion.com
Indiankanoon.org

The ward of the case in digital regulations is for the most part questioned. Cybercrime doesn't occur in a specific domain. It is geology less and borderless. So it gets truly challenging to decide the locale under which the case must be recorded. Assume an individual work from numerous spots and his information gets taken from a city while he dwells in another city, there will be a debate with respect to where the objection ought to be recorded.

*****

ipleaders.in