INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 4

2020

Cybercrime: A Legislative Overview

GAURI ANIL TOTE[1]

ABSTRACT

Computer technology has provided a pathway to human life and adds precision, speed and efficiency. There is a potential for all of us to become victims of the rising pool of offenders who skillfully navigate the Internet. Cyberspace, also referred to as the Internet, is an intangible and complex environment. Cyber-crime is a major growing problem in the current legal scenario for the nation. The exponential rise in cyber-crime makes information security an essential part of our lives.

The paper focuses on the legal implications of cyber-crime under acts of Information Technology Act 2000 and 2008, Indian Penal Code 1860, The Bankers' Books Evidence Act 1891, Indian Evidence Act 1872 and the latest draft of Personal Data Protection Bill 2019 and focuses on the significance of cyber-security law to achieve a cyber-safe environment.

I. INTRODUCTION

Cyber-terrorists commonly use technology as a tool, or a goal, or both for their illegal activity, either to obtain data that could outcome being a serious harm/injury to the owner of the critical sensitive information. The Internet is a new way by which criminals may acquire such price-sensitive information from businesses, corporations, people, banks, intellectual property offenses (such as theft of future product, summary of them, business systematics, list of clienteles, etc.), selling illegitimate products, pornography, etc., using a range of approaches such as tampering, pharming, internet phishing, etc.

II. CYBER-CRIME

Cyber-crimes can be described as unlawful activity where software are used either as a device or as a target or both. Several banks, financial institutions, investment offices, brokerage firms, etc. have been targeted over time and pressured by cyber-criminals to extort money to keep their private information unaffected in order to escape major damages. And it has been reported that certain institutions in the United States, Europe and Britain had already covertly paid to prevent massive meltdowns or breakdown of consumer trust. Such instances have led to countries forming elaborate laws to avoid Cyber-Crime and penalize

[1] Author is a student at MMCC Law College, Pune, India.

 [ISSN 2581-5369]

organizations or individuals which indulge in such activities.

For corporations, there are two primary fields in cyber-crime. The first takes the form of software and hardware attacks from threats such as viruses, malware, spyware, and network intrusions. The second is financial, and may include fraud, theft of financial records, and phishing.

1. **Phishing**

With the use of electronic mail messages that are *entirely identical* to the customer's original e-mail messages, cyber-criminals may request clarification of some details, such as account details which might include passwords, etc., ignorant/unaware customer may not realize that the e-mail messages are false and unintentionally provide sensitive information, which may result in huge financial losses when cyber-criminals use that details for personal gain. Phishing is also carried out by mobile devices where using in-voice messages cyber-criminals ask people reveal their account identity, and passwords to lodge grievances or any issues related to their bank accounts, etc.

2. **Spoofing**

This is accomplished by deluding sites or messages. Such outlets impersonate the first sites very well by utilizing the logos, names, illustrations and even the genuine bank code of the space. Such sites focus to get touchy individual subtleties of clients, for example, card subtleties to trick individuals.

3. **Viruses**

Viruses, for example, malwares and others are utilized by Hackers to hack a client's Computer and to crush information put away on a Computer by utilizing a payload of infections that conveys an unsafe message. Individual are only be liable under the Information Technology Act (hereby I.T. Act) if the owner's permission was not obtained before the virus was introduced into his device. The incongruity here is that while certain infections, for example, adware cause impermanent disturbance by indicating messages on the client's Computer, they are as yet not culpable under the Information Technology Act 2000 as they don't cause physical mischief. In any case, it must be rebuffed in light of the fact that it will fall into the extent of unapproved get to, in spite of the fact that it doesn't do any damage. Innocuous infections should likewise go under the term utilized in the arrangement as they intrude on the customary working of the gadget, program or system. This vulnerability should be rethought.

 [ISSN 2581-5369]

4. Internet Pharming

Cyber Hackers use web pharming to divert a site utilized by the client to another phony site by capturing the casualty's DNS server (the machines answerable for changing over web names into real locations Internet signs) and adjusting its I.P address to a phony site by controlling the DNS server. This sidetracks clients of the first site to a bogus deluding site so as to get unapproved data.

5. Credit Card Fraud

Huge damages can be caused by this form of fraud to the victim. It is achieved by the production of fake digital signatures. Many people lose credit cards on the way they are shipped to the receiver or are damaged or faulty, misinterpreted, etc.

6. Deep Fake Videos

"Deepfake is an AI-based technology used to produce or alter video content so that it presents something that didn't, in fact, occur"[2]

Deepfake technology works by using deep learning neural networks to mimic video (face) and audio (voice). In certain ways, neural networks are close to just how our brain processes information. Large amounts of data, in the form of millions of pictures or vocal samples, are used to develop the neural networks.

With the creation of such videos there is a high risk of it being misused and since the concept brought in with this technology is completely new, there might be need for ramifications in the existing laws to fit with the current legal scenario. If the presented point is not soon addressed in the indian legislation it might lead to various illegal and explicit activities.

III. GOVERNING LAWS IN INDIA

There was no enactment in India administering digital enactment on issues of protection, ward, licensed innovation rights and a huge number of other administrative concerns. Because of the penchant to abuse innovation, there is a requirement for rigid enactment to control criminal operations in the digital world and to safeguard the genuine feeling of the innovation *Information Technology Act, 2000'* embraced by the Parliament of India to save internet business, e-administration, e-banking just as authorizations and disciplines in the field of digital violations. The previously mentioned Act was additionally changed as the

[2] Margaret Rouse, WHAT IS DEEPFAKE (DEEP FAKE AI)? - DEFINITION FROM WHATIS.COM (2018), https://whatis.techtarget.com/definition/deepfake (last visited Jul 14, 2020)

Information Technology Amendment Act, 2008 (hereby alluded as ITAA)

INFORMATION TECHNOLOGY ACT

The Information Technology Act, 2000 which was implemented by the Parliament of India to ensure web based business, e-government, e-banking and to accommodate fines and disciplines in the field of digital violations.

The I.T. Act 2000 characterizes 'Machine' as any electronic attractive , optical or other fast information transmission gadget or framework that performs numerical, math and memory works by controlling electrical , attractive or optical driving forces and incorporates any information , yield, handling , stockpiling, Computer programming or correspondence hardware that is connected or connected to a Computer in a system. The term 'Computer'[3] and 'Computer framework' are extensively characterized and deciphered as any electronic gadget containing information handling abilities, executing Computer capacities, for example, consistent, math and preparing capacities with information, memory and yield abilities, and along these lines any very good quality programmable gadgets, for example, a switches and switches utilized in a system would all be able to be utilized.

The Act was further amended by the Legislation on Information Technology (Amendment) 2008. Terms such as 'communication devices' was added in the concept to include mobile devices, personal digital support or other devices used in the definition. ITAct-2000 described 'digital' Signature, however this concept was insufficient to meet the needs of the hour and hence the term 'Electronic Signature' was familiarized and specified in the ITAA 2008 as a legitimate way to execute signatures.

Some of the essential provisions of the IT Act on the protection against cyber-crime are under chapters IX, X and XI.

Chapter IX under IT Act sets out the punishments and rewards for numerous offences, such as consequences for damages to equipment, computer systems, damages for inability to protect data, penalties for failure to provide information, returns, residual penalties, and so on. In addition, this chapter offers for the authority to litigate an officer selected by the central government not less than the Minister of the Government of India or an alike officer of the Government of India.

Chapter X calls for the creation of the Cyber Appellate Tribunal (CAT)[4]. Any aggrieved individual may make an appeal towards the guidelines of the adjudicating officer referred to

[3] Section 2 (a) Information Technology Act (Amendment), 2008

[4] Section 2(n) of The Information Technology Act (Amendement), 2008

 [ISSN 2581-5369]

above to the Petition. In addition, any person distressed by some judgment or order of that tribunal might bring an appeal to the High Court on any query of fact or law rising out from such an order.

Chapter XI of the Act provides for penalties for various offenses, such as computer data files tampering, computer-related crimes, identity theft, cyber terrorism, and others. These offenses are examined distinctly by a cop who isn't underneath the position of Deputy Superintendent of Police.

In *Shreya Singhal v Union of India*[5] , the Supreme Court held that the legitimacy of the particular laws of the IT Act had been thought of, specifically the sacred legitimacy of Section 66A of the IT Act. Area 66A of the IT Act accommodates punishments for sending hostile messages by interchanges organizes and is referred to as follows:

Whoever , by the means of a computer resource or a communication tool sends;

(a) any aspect that is clearly offensive or of a dangerous nature, or

(b) any data that recognized to be incorrect, but with the intent of initiating distress, inconvenience, risk, interference, insult, damage, criminal coercion, hostility, or hate, by constant use of such a computer tool or device;

(c) any electronic mail with the intent of instigating irritation or embarrassment, or for deluding or misleading the recipient or receiver as to the source of such messages, will be punishable with incarceration for a period of which may extend to a time frame of 3 years with a fine.

INDIAN PENAL CODE

The Indian Penal Code was modified by embedding the word 'electronic' so as to treat computerized records and reports on level footing with physical records and archives. Areas identifying with bogus passage in a record or bogus documentation, and so on go under segments, for example, §192, §204, §464, §464, §468 to §470, §471, §474, §476 have been corrected as 'electronic record and electronic report' in this way falling inside the extent of the IPC. Paper records and electronic archives have additionally been taken care of similarly as physical records and reports during the execution of demonstrations of phony or adulterating of physical records in a wrongdoing.

Segment 67 of I.T. Act , 2000 related to Section 292 of the Indian Penal Code , 1860, distributes and transmits any substance in electronic arrangement that is lecherous or claims

[5] WRIT PETITION (CRIMINAL) NO.167 OF 2012

 [ISSN 2581-5369]

to the obscene enthusiasm as a wrongdoing and is deserving of detainment of as long as 5 years and a fine of 1 lakh rupee and a resulting offense with a time of detainment that may reach out to 10 years and a fine of 2 lacs. On account of *Ranjeet D. Udeshi v. Province of Maharashtra*[6], the Supreme Court recognized that the Indian Criminal Code doesn't characterize foulness, despite the fact that it accommodates discipline for distribution of profanity. There is a meager qualification between a substance that may be viewed as revolting and an aesthetic one.

INDIAN EVIDENCE ACT

Until ITA was upheld, all declaration in court was in a physical structure in particular. Electronic records and archives have been perceived after the presence of ITA. The extent of the Indian Evidence Act was revised to include "all documents, especially electronic records." Other terms, for example 'digital signature,' 'electronic type,' 'secure electronic record ‘data’ as utilized in the ITA, have likewise been added to make them part of the realities under the Act. The vital correction was seen by the affirmation as proof of the suitability of electronic records as set down in Section 65B of the Act.

THE BANKERS' BOOKS EVIDENCE ACT

Upon the section of IT Act, the bank needed to deliver the first journal or other unmistakable record or archive in proof under the watchful eye of the court. After IT Act has been received, the term some portion of the Bankers' Books Evidence Act was revised as follows: ‘bankers’ books will incorporate booklets, money books, account books and every single other book utilized in the typical business of a bank, regardless of whether in composed structure or as printouts of information put away in a plate, tape or some other type of electromagnetic information stockpiling gadget.' When books comprise of printouts of information contained in a floppy, circle, tape, and so on., the printout of that passage will be confirmed in consistence with the arrangements of Section 2A to the degree that it is a printout of that passage or a duplicate of that printout by the primary bookkeeper or branch chief; a testament gave by the individual dependable of the Computer framework bearing a concise synopsis of the Computer framework and portrayals of the shields actualized by the framework to guarantee that the information or some other movement completed by endorsed people is entered; the protections executed to evade and follow undesirable information changes and the assurances accessible for information recovery that are lost because of methodical disappointment or other information recovery. The previously mentioned

[6] 1965 AIR 881, 1965 SCR (1) 65

 [ISSN 2581-5369]

correction to the provisions of the Bankers' Books Evidence Act perceived printing from a Computer framework and other electronic reports as a genuine record with regards to the verification accommodated in such a printout or electronic record will be joined by a testament as expressed previously.

PERSONAL DATA PROTECTION BILL

Individual Information put away on the Computer will be his property of its proprietor and must be made sure about. There are a few manners by which such information can be misused, for example, unapproved divulgence, Computer viruses, code duplicating, eradications, and so on.

With the emergence of the problem of data privacy and the emergence of privacy as a fundamental right with Supreme Court judgment by Justice *K.S. Puttaswamy (Retd.) & Anr v Union of India*[7] there was a clear need of a Data Protection Act, this was presented by the B.N. Sri Krishna Committee of tackling the problems of personal/sensitive information, data brokers, right to erasure/forgotten etc. while the bill has still not passed it has faced issues related to data localization and liabilities of third parties on continuous disclosure, it has brought in measures and compensations for victims under cyber law, which was the need of the hour.

IV. SHORTCOMINGS OF INFORMATION TECHNOLOGY ACT

- It is argued that ITAct and ITA Act are, indeed, a groundbreaking first step and have become a milestone in the nation's technological growth; indeed, current legislation is not adequate. Numerous issues in digital wrongdoing and numerous violations stay revealed. Regional locale is a significant developing worry that isn't even sufficiently tended to in the ITA Act or the ITAA Act.

- The purview alluded to in Sections 46, 48, 57 and 61 with regards to the settling procedure and the intrigue method related thereto. Area 80 arrangements with the forces of cops to enter, look an open spot for digital wrongdoing, and so forth. Since digital wrongdoings are basically Computer based violations and, accordingly, if somebody's mail is hacked in one area by the blamed sitting far in another State, it is hard to find the police headquarters concerned who might know about them.

- It is indicated that the agents are normally trying to stop this tolerating these complaints based on purview. Since digital wrongdoing is topographically rationalist,

[7] Writ Petition (Civil) No. 494 of 2012)

 [ISSN 2581-5369]

borderless, regionally free and normally conveyed across domains of an assortment of wards, satisfactory preparing ought to be given to those concerned. By and by, most cybe-wrongdoings in the country stay inside the particular pieces of the IPC, read with the equivalent segments of the ITAct or the ITAAct, which permit the analytical offices that, regardless of whether the ITAct some portion of the case is lost, the guilty party can't escape from the IPC part.

- Usually teens engage in cyber-crime unknowingly or which they think is enjoyable. So, that's it. The Home Ministry and the IT Department have recommended that the first time offenders be treated with leniency and solutions such as warning, counselling and parental guidance. It is argued that the Government might find it necessary to enact an appropriate law on such offenders

V. CONLUSION

Society becomes increasingly dependent on technology, and crimes based on online crimes are expected to increase. Cyber-crime is rife and is growing exponentially as a side effect of the overuse and abuse of computers and the Internet. Crime is a significant barrier to the prosperity of a nation which adversely affects the citizens of society which inhibits the country's economic growth. The Information Technology Act is a coupled with above mentioned acts in the fight against cyber-crime. Cyber-crime occurs almost every day, but only some of it is published. Cases of computer crime before the court of law, therefore, very few. Difficulties occur in gathering, preserving and appreciating digital content. The Act has a long way to go and promises to drive victims of cyber-crimes safe. In the light of the severity of the crimes committed by the scammers, the enactment of the law making the mechanism of the nation should be made to hold the offenses at the lowest possible point. Steady endeavors by rulers and administrators will likewise be made to guarantee that innovation enactment covers all aspects and issues of digital wrongdoing and keeps on advancing in a nonstop and safe manner to keep a consistent attentive gaze on and track significant violations.

*****

 [ISSN 2581-5369]