Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

Cite this article as:

MRS. DEOYANI VASANTRAO NIKAM, "*A Conceptual Analysis with reference to Information Technology Act, 2000",* Vol.4 & Issue 3, Law Audience Journal (e-ISSN: 2581-6705), Pages 16 to 28 (19th September 2022), available at ***https://www.lawaudience.com/a-conceptual-analysis-with-reference-to-information-technology-act-2000/.***

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

Publisher Details Are Available At:

https://www.lawaudience.com/publisher-details/

Editorial Board Members Details Are Available At:

https://www.lawaudience.com/editorial-board-members/

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

ABSTRACT:

"The world is experiencing the fastest revolution after the industrial, green and digital revolution. India is emerging as an Information Technology hub and at the same time cyber-crimes are increasing day by day. Cyber-crimes are defined as an, ***"illegal act in which a computer is a tool or a goal or both."*** *Cyber-crimes are also known as computer crimes. Cybercrime can be committed against an individual or a group. It can also be committed against government and private organizations. It may be intended to harm someone's reputation, physical harm, or even mental harm. The internet technology has been using by the few people for criminal activities like hacking, phishing, cyber terrorism, bombardment of e-mails, pornography etc.*

This is mainly because around more than half of the online users are not fully aware of the functioning of online platforms. India is one of the countries which has enacted Information Technology Act 2000 on par with the model law framed by the United Nations Commission on Trade Law and made an attempt to define use and misuse of digital media in a country. The IT Act was amended in 2008 in which various cyber offences are punishable with imprisonment and fine. During Covid-19 lockdown situation, Cyber-crimes have increased at a large scale in several states as the people are confined in their respective homes. The present paper highlights the meaning of cyber-crime, kinds of cyber-crimes, classification of cyber-crimes, various cyber laws in India with judicial pronouncements. The study also suggests various measures and recommendations to curtail cyber-crime incidents and tries to ensure cyber security".

Keywords: Cyber-Crimes, Cyber Security, Cyber Laws, Internet.

I. INTRODUCTION:

The industrial revolution in 16th Century has made drastic changes in the human beings. The world is experiencing the fastest revolution after Industrial, Green and Digital Revolution. It

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

is to be noted that with the advent of this revolution today, we have access to more Information than ever but at the same time poses some new challenges to the legal world. The internet has become a part of life of every individual. Internet data is available at affordable prices in India. So, millions of human being are using websites and e mails as a means of communication also. The rapid use of Internet has increased the rate of crime. Internet is actually very much usable for us but some criminal minded people use it for crimes.

It is essential to note that the first cyber-crime took place in the year 1820. In the recent past in India the cyber-crimes have gain momentum. The word ***'Cybercrime'*** is neither defined in Indian Penal Code 1860 nor the Information Technology Act. In simple way we can say that Cybercrime is unlawful act wherein there is either a tool or target or both. It is also defined as an illegal activity which used a computer for fraud, forgery, unauthorized access to or interference with data.

II. CAUSES OF CYBER CRIMES:

II.I Easy To Access:

The difficulty to guard a computer system from hackers due to complex technology. The skilled hackers can get unauthorized access by breaching access codes, retina images, voice recognition, etc. They can easily fool the biometric system and pass through the firewall of the system.

II.II Capacity To Store Data In Small Space:

A computer has feature of storing data in very small space. Storing data in a small space makes it easier for hackers to steal data in no time and utilize it for their own profit.

II.III Complex Coding:

The computers work on operating systems. These operating systems are composed of millions of codes. Operating systems are programmed by developers are human beings, thereby, making the codes vulnerable to make errors. Cyber-criminals can slip in through these loopholes and make the operating system malicious for the users. That's why the complex coding can often become the common cause of cyber-crime

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

II.IV Negligence:

Negligence is related with human conduct. So it is possible the while protecting the computer system there might be negligence which provides cyber criminals to get access and control over the computer system. Anything that we neglect and consider easy to ignore can turn into a grave concern. Cybercrime works the same way. Negligence in ensuring the security of your system can bring you big troubles. A little negligence at your end can provide a welcoming aisle for cybercriminals. Hence, it is necessary to remain vigilant to the happenings in your system.

II.V Loss of Evidence:

Hackers generally attack on computer system in sections, and the evidence regarding their first breach can be easily destroyed. This makes their crime even stronger that cannot be detected during the investigation of cybercrime. Loss of evidence can become an important cause of cybercrime that can possibly paralyze this system and make it more vulnerable to the cyber-attacks.

III. CLASSIFICATION OF CYBER CRIMES:

Cyber-crime has been classified on the basis of nature and purpose of the offence and have been broadly grouped into three categories depending upon the target of crime. It may be against person such as crimes like stalking, defamation, hate messages and transmissions of pornographic material. The Cyber-crime involving property include unauthorized computer trespass, vandalism and transmission of harmful programmes and unauthorized possession of computerized information. The third category of Cyber-crime targets the Government .This kind of Cyber-crime is known as Cyber terrorism.

Another classification of computer crimes has been given by David L. Carter who classifies computer-related crimes into three categories.

- *Where computer is the target go the crimes;*
- *Where computer facilitates the commission of crime;*
- *Where, computer is incidental to the crime.*

III.I Computer As The Target of Crimes:

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

In this process the attackers use a computer to attack other computers. Crimes in which the computer is target includes such offences as;

i. *Theft of intellectual property, theft of marketing information e.g., customer list, pricing data or marketing plans.*
ii. *Blackmail based on information gained from computerized files e.g., medical information, personal history or sexual preference.*
iii. *Unlawful access to criminal justice and the Government record e.g., changing a criminal history, modifying want and warrant information, changing tax records, creating driver's license, passport etc.*
iv. *Sabotage of computer and computer system and programs with the intent to impede a business or create chaos in business's operations.*

III.II Computer As A Tool of Crime:

In this process computers are used to commit traditional crimes.in this category of computer crimes, the computer is not essential for crime to occur. This means that the crime could occur without technology but computerization helps the crime to occur faster. ***Crimes in which the computer is a tool includes such offences as;***

i. *Fraudulent use of credit cards*
ii. *Fraudulent use of Automated Teller Machine (ATM) and accounts*
iii. *Fraud involving electronic fund transfers*
iv. *Fraudulently conversion to transfer accounts*
v. *Telecommunication frauds*

III.III Computer As Incidental To Crime:

In this process computer is not essential. Crime could occur without Computer but use of computer help the crime to occur faster. Computers also permits processing of greater amount of information and makes the crime more difficult to identify and trace. ***Computer as incidental to the crime may be classified into two broad categories;***

- *Internet Crimes;*
- *Web based Crimes;*

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

III.III.I Internet Crimes:

- ***a)*** *Hacking*
- ***b)*** *Espionage*
- ***c)*** *Spamming*
- ***d)*** *Launching malicious Programmes*

III.III.II Web Based Crimes:

III.III.II.I Website Related Crime:

- ***a)*** *Sale of pirated software*
- ***b)*** *Gambling*
- ***c)*** *Insurance frauds*
- ***d)*** *Distribution of Pornography*

III.III.II.II Crimes Through E-Mails:

- ***a)*** *Threats*
- ***b)*** *Extortion*
- ***c)*** *E-mail bombarding*
- **d)** Defamation

IV. CATEGORIES OF CYBERCRIME:

- *Hacking*
- *Identity Theft*
- *Cyber Stalking*
- *Hate Speech Online*
- *Intellectual Property Crimes*
- *Phishing*
- *Electronic Mail and IRC related Crimes*
- *Cyber Terrorism*

IV.I Hacking:

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

Means trying to get into computer systems in order to steal, corrupt or illegitimately view data. ***Examples of Hacking***, Using password cracking to gain access to a system. Hacking also means using computers to commit fraudulent acts such as fraud, privacy, invasion, stealing corporate/personal data etc.

IV.II Identify Theft:

When personal information of a person is stolen with a purpose of using their financial resources or to take a loan or credit card in their name then such crime is known as identify theft.

IV.III Cyber Stalking:

The word Cyber Stalking has not been defined in Information and Technology Act But the cyber stalking means follow a person through internet by posting message on the social sites or continuously sending emails to victim etc. The cyber stalkers collect all personal information about the victim such as name, family background, telephone numbers of residence and work place, daily routine of the victim and may post this information on any website related to sex-services or dating services and invite the people to call the victim on her telephone numbers to have sexual services.

IV.IV Hate Speech Online:

In ***Pravasi Bhalai Sangathan vs. Union of India***, the Supreme Court requested the commission to define 'hate speech'. According to law commission report in the age of technology, internet is means of spreading false incite violence but also perpetuate the discriminatory attitude in the society.

IV.V Intellectual Property Crimes:

The intellectual property becomes suspected to misuse and theft in cyberspace. In ***Kabushiki Kaisha Trading vs. Mrs. S.K Sile & Others***, the Court held that on account of advancement of technology, fast access to information, international travel and advertising, publicity on internet, television, magazines which are available throughout the world of goods and services during fairs/exhibition, more and more persons are coming to know of the trademarks. Therefore, trademarks need to be protected.

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

IV.VI Phishing:

This is a financial crime on the cyberspaces. It refers to a form of online identity theft such as online banking passwords and credit card information from users. The earliest form of phishing attacks was email based and they date back to 90's.

IV.VII Electronic Mail & IRC Related Crimes:

This is another kind of crimes where some unrelated person stole our emails.

IV.VII.I Defamatory Emails:

In this process the email receives contains defamatory mails but as per true meaning of the defamation to be attacked the defamatory matter must be known to some other person in addition to receiver.

IV.VII.II Email Frauds:

In this process some unknown abuse request for help of the use to clear some legal or accounting problems.

IV.VIII Cyber Terrorism:

Cyber terrorism is the act of internet terrorism in terrorist activities number of cyber terrorists hacks government and private computer system.

V. CYBER LAW IN INDIA:

Hart in his work ***"The Concept of Law"*** has said ***'Human beings are vulnerable so rule of law is required to protect them'***. If this principle is applied to cyberspace then computers are supposed to be vulnerable and rule of law is essential to protect and safeguard them against cyber-crimes. Till 2000, there was no a legislation which deals with Cyber-crimes. Parliament of India enacted ***'Information Technology Act 2000'*** on par with the law framed by the ***United Nation Commission on Trade Law***. The Act provides legal recognition for transactions carried out by means of electronic data interchanged and other means of electronic communications referred to as electronic commerce which involves the use of alternatives to paper-based methods of communication and storage of information to facilitate

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

electronic filing of documents with the government agencies. The original Act contained 94 Sections divided into 13 chapters and 4 schedules. The law apply to whole of India. Persons from other nations can also liable under the law. If the crime involves a computer or network located in India. This act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures. The act also amended various sections of Indian Penal Code 1860, Indian Evidence Act 1872, Bankers Book evidence act 1891 and Reserve Bank of India Act 1934 to make them comply with new technologies.

Objective Of Information Technology Law In India:

1) *To give Protection to the legal recognition to E-transaction*
2) *Legal Recognition to Digital Signature is considered as valid signature to accept agreements online*
3) *To stop Cyber-crimes and provide protection to online privacy*
4) *To protect Legal Recognition to keep accounting books in electronic form by bankers*

The Offences And Punishment Under Information Technology Act, 2000:

1 *Sec.43: Penalty for damage to Computer, Computer system etc.*
Punishment: Compensation to tune of Rs. 1 crore to the affected person.

2. *Sec.44 (a): Penalty for failing to furnish any document, return on report to the Controller the Certifying Authority.*
Punishment: Penalty not exceeding one lakh and fifty thousand rupees for each such failure

3. *Sec.44 (b): Penalty for failing to file any return or furnish any information or other document within the prescribed time.*
Punishment: Penalty not exceeding five thousand rupees for every day during which such failure continues.

4. *Sec 44(c): Penalty for not maintaining books of account or records.*
Punishment: Penalty not exceeding ten thousand rupees for every day during which the failure continues.

5. *Sec.45: Offences for which no penalty is separately provided.*

   Punishment: Compensation not exceeding twenty five thousand rupees to the affected person or a penalty not exceeding twenty five thousand rupees.
6. *Sec. 65: Penalty for tampering with computer source documents.*

   Punishment: Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
7. *Sec 66: Hacking with computer system with the intent or knowledge to cause wrongful loss.*

   Punishment: Imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
8. *Sec. 67: Publication of obscene material in an electronic form.*

   Punishment: Imprisonment up to 5 years and with fine which may extend up to two lakh rupees on forst conviction and its double punishment for second and subsequent convictions.
9. *Sec 68: Penalty for failing to comply with the directions of the Controller.*

   Punishment: Imprisonment up to three years and fine up to two lakh or both.
10. *Sec.69: Penalty for failing facilities to decrypt information which is against of sovereignty or integrity of India.*

    Punishment: Imprisonment which may extend to seven years.
11. *Sec.70: Securing or attempting to secure access to a protected system.*

    Punishment: Imprisonment which may extend to ten years and fine.
12. *Sec.71: Penalty for misrepresentation or suppression of any material fact from the Controller or the Certifying Authority.*

    Punishment: Imprisonment up to 2 years or fine up to rupees one lakh or with both.
13. *Sec.72: For break of confidentiality and privacy.*

    Punishment: Imprisonment up to 2 years, or fine up to one lakh rupees, or with both
14. *Sec. 73: For publishing digital signature certificate false in certain particulars*

    Punishment: Imprisonment up to two years, or with fine which may extend up to one lakh rupees or with both.

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

15. *Sec.74: Penalty for publication of Digital Signature Certificate for any fraudulent or unlawful purpose.*

    Punishment: Imprisonment up to 2 years, or fine up to one lakh rupees.

The Offences and Punishment under Information Technology Act 2008:

A major amendment was made in 2008. It introduced Section 66A which penalized sending of ***'Offensive Messages'***. Section 67 and 67A prohibits circulating obscene and sexually explicit material through internet respectively. Section 69A allows government to block content which creates threat to security to the state; the sovereignty, integrity or defense of India; friendly relations with foreign States; public order etc. It also introduced Sections which gave authorities the powers of interception or monitoring or decryption of any information through any computer resource, it also introduced for child porn, cyber terrorism and voyeurism.

VI. LANDMARK CASES OF CYBER-CRIMES:

VI.I Shreya Singhal vs. UOI AIR 2015 SC 1523:

Facts: The two women were arrested under Section 66A of the IT Act, alleged to have posted objectionable comments on Facebook regarding the complete shutdown of Mumbai after the demise of a political leader. Section 66A of IT Act states that whoever by using a computer resource or communication provides information that is offensive, false, or causes inconvenience, danger, annoyance, insult, hatred, injury, or ill will, be punished with imprisonment. The women challenged constitutionality validity of Section 66A of the IT Act before the Supreme Court.

The Court held that section 66A is ambiguous, and is violative of the right to freedom of speech and it takes within its range the speech that is innocent as well. It removed an arbitrary provision from IT Act, 2000 and upheld citizens' fundamental right to free speech in India. It was of the view that even though section 66A is struck down, provisions in the Indian Penal Code, 1860 will continue to be applicable prohibiting racist speech, any speech that outrages

the modesty of a woman or speech aimed at promoting enmity, abusive language, criminal intimidation, racism, etc.

VI.II CBI vs. Arif Azim (Sony Sambandh case):

Facts:

The website ***www.sony-sambandh.com*** allowed NRIs to send Sony products to their Indian friends and relatives after paying online for the same. Someone logged in May 2002 into the website under the name of Barbara Campa and a Sony Colour TV set along with a cordless telephone was ordered for Arif Azim in Noida. The payment was made by her through a credit card and the said order was delivered to Arif Azim. Though the credit card agency informed the company that it was an unauthorized payment, the purchase was denied by the actual owner. The complaint was lodged with CBI and a case under Section 419, 418, and 420 of IPC, 1860 was registered. An investigation was held, and it was concluded that Arif Azim while working at the Noida Call Centre, got access to the credit card details of Barbara Campa which he misappropriated. The court found Arif Azim guilty. He was given a one-year probationary period. The Indian Penal Code, 1860, was cited by the court as an effective piece of legislation to depend on when the IT Act was not sufficient.

VI.III State of Tamil Nadu vs. SuhasKatti CC No. 4680 of 2004:

Facts:

The accused was the victim's family friend and wanted to marry her but she married another man which resulted in a divorce. After her divorce, the accused influenced her again and but she was unwillingness to marry him. He opened a false e-mail account in the victim's name and posted obscene, defamatory, and annoying information about the victim. Charge sheet was filed under Section 67 of the IT Act and Section 469 and 509 of the Indian Penal Code, 1860 against the accused. The accused was held liable under Section 469 and 509 of the Indian Penal Code, 1860 and Section 67 of the IT Act. He was punished with a Rigorous Imprisonment of 2 years along with a fine of Rs. 500 under Section 469 of the IPC, Simple Imprisonment of 1 year along with a fine of Rs. 500 under Section 509 of the IPC, and

Law Audience Journal, Volume 4 & Issue 3, 19th September 2022, e-ISSN: 2581-6705, Indexed Journal, IF 5.381, Published at https://www.lawaudience.com/volume-4-issue-3/, Pages: 16 to 28,

Title: "A Conceptual Analysis with reference to Information Technology Act, 2000", Authored By: Mrs. Deoyani Vasantrao Nikam, Assistant Professor, Shri Omkarnath Malpani Law College, Sangamner (MS), affiliated to Savitribai Phule Pune University, Pune, Maharashtra, Email Id: deoyaneedeshmukh@gmail.com.

Rigorous Imprisonment of 2 years along with a fine of Rs. 4,000 under Section 67 of the IT Act.

VI.IV Pune Citibank Mphasis Call Center Fraud:

Some ex-employees of BPO arm of MPhasiS Ltd MsourcE defrauded US Customers of Citibank to the tune of Rs 1.5 crores. It was one of those cyber-crime cases that raised concerns of many kinds including the role of ***"Data Protection"***. The crime was obviously committed using ***"Unauthorized Access"*** to the ***"Electronic Account Space"*** of the customers. It is therefore firmly within the domain of ***"Cyber Crimes".*** The accused held liable under Sec.66 and Sec.43 of Information Technology Act 2000. Accordingly, the persons involved are liable for imprisonment and fine as well as a liability to pay damages to the victims to the maximum extent of Rs 1 crore per victim.

VII. CONCLUSION AND SUGGESTIONS:

The Information Technology Act of 2000 provides all safeguards for prevention of cyber-crimes but it is insufficient to cope with the current offence as India is moving closer to being a digital nation. Crimes are on the rise and new forms of Cyber Crime are emerging every day. There is need to improve and advance legislation to deal with Cyber Crime as India's Cyber Law has been found to be inadequate in comparison to other states. The Information Technology Act of 2000 provides safeguard for prevention of cybercrime but it cannot stop each and every crime as every passing minute thousands of publics are using internet.

There is also big lacuna for proper implementation of the Act because lack of skilled technical staff in the law enforcement department and many police officer have not aware the provisions of the Act and their enforcement. For effective control and checking of illegal activities in the cyber system, the police official should be trained and separate cell may be created in every district. The Public Prosecutor must be given training in cyber-crime must be added in the curricular of law course in India so that awareness can be created among the public to effectively fight cyber-crime and its exploitation.

References:

- *Chaubey, R. K. (2008) Cybercrime and Cyber law, Kamala House Publication, Kolkata*
- *Shelkar, A (2008) Cyber Law, Nashik Law House, Nashik*
- *Jaishankar, K. K. and Jhonson, Philip (2011) Cyber Law, Pacific Publication, Delhi*
- *Amar Meena (2015) Lectures on Cyber Law, Asia Law House, Hyderabad*
- *Thakur, Kalpana and Kaur, Parminder , Cyber Crimes against Women and Children with Reference ti IT Act*
- *Manikyam, Sita (2009) Cyber Crimes Law & Policy Perspective, Hind Law House Publciation, Pune.*
- *Ahmad, Farooq (2006) Book Cyber Laws in India, New Era Publication, Delhi.*
- *www.cyberlawsindia.net*
- *www.myadvo.in>blog*
- *newindiaexpress.com*
- *https://blog.ipleaders.in*
- *oneindia.com*
- *https://www.lawyersclubindia.com/articles/landmark-judgments-on-cyber-law-14025.asp*
- *https://www.cyberralegalservices.com/detail-casestudies.php*