ISSN: 2582-6433

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed6th Edition

VOLUME 2 ISSUE 7

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

 ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

 ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

CYBER LAW: A DETAILED ANALYSIS OF CYBER CRIMES AND THEIR IMPACT ON CONTEMPORARY INDIA

Submitted by: Shivam Pandey
Batch IPL02
INTEGRATED PROGRAMME IN LAW
INDIAN INSTITUTE OF MANAGEMENT, ROHTAK

TABLE OF CONTENTS:

 ISSN: 2582-6433

CERTIFICATE OF ORIGINALITY

This is to certify that Shivam Pandey, IPL02047, a student enrolled in the Integrated Programme in Law at the Indian Institute of Management, Rohtak has completed the research project titled, "CYBER LAW: A DETAILED ANALYSIS OF CYBER CRIME AND THEIR

IMPACT ON CONTEMPORARY INDIA", and is free from any plagiarism and has not been submitted elsewhere for publication.

INTRODUCTION

The world has made rapid progress ever since the introduction of the Internet and its deep integration into domestic households, allowing for better means of communication and information exchange, becoming an integral part of civilised societies all across the globe. The virtual space provided by the internet is a space relatively free from control by a central authority and thus has given the criminal class an upper hand into taking up different unmonitored areas for carrying out its unlawful activities and causing harm to the general public through the means of such information exchange technologies. Crimes thus committed over the internet or through any such electronic means are known as cybercrimes. Also referred to as e-crimes (electronic crimes), cybercrimes are a threat to all countries, businesses and individuals worldwide. Rising number of cybercrimes occurrences are being recorded on a daily basis across numerous regions throughout the world, with millions of people having fallen prey to it, it is no surprise that a shared awareness and knowledge of illegal behaviour is necessary for effective e-crime prevention and control.

The term itself, however, remains to be well-defined by any statute or act passed by the Indian legislature. It could be, as per certain judicial interpretations and judgements, partially defined as: *Any illegal act committed on the cyber space by and through any electronic means as recognised by the Information Act, 2000 (hereinafter referred to as ITA 2000) can be called a "Cybercrime".* There are all sorts of criminal activity that take place in such cyber spaces and that which are defined by the provisions of ITA, 2000, including, but not limited to, acts of spamming, spoofing, financial scams, phishing/data theft, cyberterrorism, child pornography/ uncensored gore, critical data leaks, and even government data system leaks that may lead to

 ISSN: 2582-6433

the compromise of the security and safety of a massive chunk of civilians in a country.

However, owing to several legal loopholes and intricacies that arise out of the constantly evolving world of digital communication, criminal syndicates are always a step ahead when it comes to the various kinds of crimes and wrongs done. *What are the most common variations of crimes committed digitally? What are the possible preventive measures against cybercrimes? What are the legal provisions and remedies available in India? Are the traditional laws under the ITA 2000 keeping up with the dynamic world of cyber crimes or is there a need for amendments? What are some of the landmark judgements passed against cybercrime in the recent years?* A detailed discussion into these topics are done throughout the study by looking at the different cybercrime cases under different categories, Indian acts and statutes and doctrinal research carried out so far by established academicians.

This study is aimed towards understanding the nature and different types of cybercrimes, and how criminal activity unfolds in digital virtual spaces or by the means of different virtual communication medias, by taking a look at pre-existing provisions, articles and some of the landmark cybercrime cases in India under the Information Technology Act, 2000 (and/or Indian Penal Code). A look into the various acts implemented in monitoring and providing remedies to cybercrime is discussed afterwards.

We will now delve into more definitions of "Cybercrime" as covered and defined by different research articles, journals, books, etc.

LITERATURE REVIEW

1. Tej Naraian Prasad Verma and Dr. DA Khan (National Institute of Technology, Jamshedpur) in their article titled, **"Curbing Cyber Crimes by Indian Law"** spoke aboutthe relations between cybercrime and Indian law through the detailed means of studying various types of cybercrimes and the means of curbing them through the provisions, statutes and regulations as enlisted in the IT Act of 2000 and its amendment of 2008. Their study explores the cybercrime risks and the distinct repercussions brought about by each of them.

They went on to describe the possible instances of cybercrime that occur most frequently in Indian cyber space with detailed descriptions of them, which we shall be mentioning in this study in a very brief and abbreviated manner, as enlisted below:

 ISSN: 2582-6433

- *That Cyber-crime is, according to the author, a new type of crime in the world. Any illegal behavior that takes place on or via the medium of computers, the internet on anyother devices recognized by the IT Act 2000 is called cybercrime.*
- *The author believes that cybercrime is an uncontrollable evil which springs from the misappropriation of modern society's ever growing reliance on technology.*
- *The different forms of Cyber-crime include malicious acts of stalking, spam, scam, catfishing, impersonation, blackmail, child pornography, email bombing etc.*
- *The author then went on to describe specific sections under IT Act 2000 and focuses on "Section 43, Section 66, Section 66B, Section 66C, Section 66D" and then further wenton to look into the Indian Penal Code (IPC 1980), Companies Act (2013), NIST Compliance, so on and so forth.*
- *The author then studies the statistical data of cybercrime and concludes withhypothetical ways to prevent them.*

2. Author Sanjay Goel in his article **"National Cyber Security Strategy and the Emergence of Strong Digital Borders"** talks about the weaponization of digital technologies and the threats to national security. An unfettered environment, without the scope of any intervention by the government in its initial days, the Internet has evolved into a potent weapon for influencing geopolitical disputes, including meddling in the internal affairs of other nations, compromising national security, undermining the financial system, and assaulting critical infrastructure. This is a result of society's close dependency on the internet. Despite the social and economic benefits that the internet offers, many nations are worried about the threats it presents to their national security. The author goes on to talk about issues pertaining to national security on the cyber space and the effective ways and methods that could be adopted to combat it.

3. Author Devashish Bharuka in his article **"Indian Information Technology Act, 2000 Criminal Prosecution Made Easy For Cyber Psychos"** aimed at bridging the gap between cyber and traditional Indian criminal laws by analysing some on going cybercrime cases, and studying provisions related to criminal liability. It is a high-level overview of India's first cyber legislation and a recommendation for how it can be implemented to minimise cybercrimes and encourage further IT (information technology) growth in India.

 ISSN: 2582-6433

4. In **"A brief study on Cyber Crime and Cyber Law's of India"** by **Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah,** the authors have provided a bird-eye's view into cybercrime, prevention and its respective legislation in India. The authors have defined the various types of crimes that occur through the means of the net and went on to observe India's cybercrime scenario through lens of a few cases such as the Parliament attack case, the Sony-Sambandh.com (also referred to as the "Sony-Sambandh.com" case, ***CBI v. Arif Azim)*** [1] cases etc. They went on to look into the existing cyber laws and correlated the different sections of ITA applicable for different offences committed in the cyber space.

RATIONALE

To achieve answers to the previously introduced questions, to figure the scope and prospect of the Indian legislative rules governing the cyber domain, the study aims to examine cybercrime, the various different types of cybercrimes that exist in the modern world, the most common forms of cybercrimes that have plagued India over the past decade and the various provisions that exist under Information Technology Act, 2000, to deal with such cases.

The project is divided into three parts. In the first part, the study tries to define "cybercrime" and explore the various types of cybercrime that exist. The second part particularly focuses on the legal provisions as under Indian Information Technology Act, 2000 and takes a look at the various landmark cases of cybercrime that have happened in the past decade, and the various judgements arising out of it. And lastly, after having analyzed the various cases and their respective pre-existing legal remedies, it will take a look into the various methods of prevention that (may) exist and will try and identify the shortcomings of the Information Technology Act.

STATEMENT OF PROBLEM

Through the means of this research, the study tries to find a conclusive inference towards each of the following propositions:

1. **What are the various types of cybercrimes that occur throughout the world?**
2. **What are the preventions and legal remedies against cybercrime as under Information Technology Act, 2000 and Indian Penal Code, 1860?**
3. **What are the limitations of the cyber laws of India?**

---

[1] ***[(2008) 105 DRJ 721: (2008) 150 DLT 769]***

 ISSN: 2582-6433

OBJECTIVES OF THE REPORT

1. To study the definition and scope of cyber crime in the Indian context.
2. To study and analyze the Information Technology Act, 2000.
3. To study various cybercrime cases and landmark judgements passed in the recent years.
4. To comment on the existing legislation for cybercrime in India and loop holes in the system, if any.

SOURCES AND NATURE OF THE STUDY

This study relies heavily on the *doctrinal research* method and therefore, relies, on utilizing published academic references, newspaper/digital articles, and books as the primary source of data. As for the empirical data that may be utilized further into this research, it is mostly secondary, with the surveys being conducted by academics before and the study only benefitting from the interpretation of their inferential data; thereby making the empirical studies derivative from secondary sources.

CONTRIBUTION OF THE STUDY

The report is aimed at studying the cyber laws existing in India by studying various cybercrime cases and landmark judgements, thereby drawing inferences as to the grip of the Indian legislative in combatting injustices committed in the digital space. It also provides for the areas of improvement by analysing the inconsistencies that exist, if any.

LIMITATIONS OF THE STUDY

The study is limited owing to lack of verified and genuine sources with published articles, journals, and previously conducted studies, specifically done in the Indian context. Further, the lack of some important terms in the cyber-law context, that remain yet to be defined by the Information Technology Act, 2000, has added to its limitations. The study is thus bounded to the scope as covered by the different literary works previously listed alongside some other journals, articles, and judicial interpretations and decisions from the different cases that have been picked up for analysis in this study.

 ISSN: 2582-6433

CHAPTER I:

An overview of Cybercrime

Definitions for Cybercrime:

Cybercrime, as previously stated, is not yet defined by an act or statute passed by the Indian legislature. Many academicians have tried to define cybercrime, besides some existing judicial interpretations of the term. Some such definitions of cybercrime according to different authors are briefly discussed below:

"…Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conducts. These acts are based on the material offence object that affects the computer data or systems. These are the illegal acts where a digital device or information system is a tool or a target or it can be the combination of both. The cybercrime is also known as electronic crimes, computer-related crimes, e-crime, high technology crime, information age crime etc…"

"'Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems.' The aforementioned definitions are proposed by the authors Animesh Sarmah, Roshmi Sarmah, and Amlan Jyoti Baruah from ***A brief study of Cyber Crime and Cyber Laws of India***.

Dr. Debabrati Halder and Dr. K. Jaishankar, define the Cyber-crime to be:

"Offenses committed against individuals or groups of individuals with a criminal motive to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, via modern telecommunication networks such as the Internet (Chat rooms, emails, notice boards, and groups) and mobile phones (SMS/MMS)"

It could be thus summarised as:

"Cybercrime is an illegal activity, that is an offence against individuals/groups of individuals and/or the society at large with a criminal motive to harm the victim, committed in the cyber space by and through any electronic communication means as mentioned and recognised under Information Technology Act, 2000."

 ISSN: 2582-6433

Types of Cybercrimes:

Cybercrimes are usually classified into the following four categories:

1. Cybercrime against Person
2. Cybercrime against the Government
3. Cybercrime against Property
4. Cybercrime against the Society

We will now take a brief look into the various types of crimes committed in digital cyber space:

I. Hacking/Cracking: Hacking or cracking refers to unauthorized and illegal access into a computer system or a system of networks for the purpose of stealing, copying,or modifying the data for misappropriate intentions and/or for causing harm to the victim.

II. DoS Attack: It can be defined as the prevention of authorized access to a system orthe delaying of system operations and functions.

III. Email Bombing: An email bomb utilizes various available software to drop in hugevolumes of email to a specifically targeted recipient. It is usually an attempt to overflow a server network or to overwhelm the mailbox in an attempt of Denial ofService (DoS) attack.

IV. Cyber-stalking: Repeated acts of harassment or threats directed towards targeted individuals in digital cyber spaces can be defined as acts of cyber-stalking. It is a punishable offence with a wide range of implications and repercussions.

V. Child Pornography: Pornographic content are audio-visual material available on the internet that displays and/or is indicative of performing sexual acts directly or indirectly. Section 67B of ITA (amendment of 2008) addresses the issue of possession of child pornography as a punishable offence with possible imprisonment provisions of 5 years and fines which may extent up to 10 lakhs firstoffence and then increased imprisonment sentence and monetary sanctions if caughtwith the illicit possessions again in the future.

VI. Fraud (Banking/E-Commerce): Any theft of data that results in monetary loss fromthe targeted victim either directly or indirectly fall under the category of fraud (alsoreferred to as scam) and is punishable by ITA, 2000. Consumers in this domain, are therefore, highly dependent on cyber laws for protection from such frauds and scams.

 ISSN: 2582-6433

VII. Cyber-warfare: Hacking done for the purposes of sabotaging and espionage for political reasons across States or different political bodies is reffered to as cyberwarfare.

VIII. Cyber-terrorism: Terrorists make use of digital virtual and physical storage media for the purposes of keeping record of their illicit businesses in a hidden manner. Such individuals and organisations use mails and chatrooms to establish contact with their members around the world. In order to avoid snooping and tracking by the government, these individuals/organisations purchase expensive encryption softwares that encrypt their stored and transmitted data.

We will now take a look into the various as to why such crimes happen in the first place.

Causes of Cybercrimes:

The different motivations for commiting acts relating to cybercrime can broadly be classified in three categories, mainly, as:

1. Personally motivated cybercrime:

Cybercriminals may commit crimes motivated by personal feelings and emotions. In the end, cybercriminals are humans and are prone to feelings of hurt and grudge which might motivate individuals or certain groups to send a message to a targeted victims digitally by the means of sabotage, theft and/or vandalism etc. Many of these crimes can have a serious impact on personal property and possessions and lead to financial and/or social consequences that could seriously affect the life of an individual.

2. Financially motivated cybercrime:

Many cybercrimes are primarily committed with the intention of financial theft for monetary benefits. Given the complexity and anonymity of cyberspace, the perception of relatively low risks with high financial rewards encourages people with digital expertise to engage in electronic malpractices of malware, identity theft, fraudulent money request attacks and phishing. According to Businessweek, an estimation suggests that cyber crimes that target digital bank accounts alone are able to steal almost
$700 million every year, globally.

 ISSN: 2582-6433

3. Ideologically motivated crimes:

Cyber attacks (attempts of hacking with the intent of data theft or sabotage) to send a message to the government, general public masses and/or individual affiliated/unaffliated with ogranizations, on the grounds of ethical, moral and/or ideological reasons are perceived to be ideologically motivated attacks. A prominent case of such an attack was demonstrated when the "hacktivist" group *Anonymous* attacked financial service providers, the likes of Paypal and MasterCard for their refusal to make charitable contributions to the whistle blowing controversial non-profit website by the name of WikiLeaks, rendering the servers of these fintech giants unreachable tothe Internet banking users.

CHAPTER II:

Cybercrimes in the Indian Context

The term 'cybercrime' has not been defined in the ITA 2000 or in any other legislation in India. The ITA was passed to facilitate e-commerce transactions and give legal recognition to those carried out by the means of electronic communication which involve othe use of other alternatives to paper-based forms of communication and information storage. The ITA 2000 plays a key role in combatting and providing legal provisions and remedies in India and is often used in coordination with the Indian Penal Code, 1860 (hereinafter referred to as IPC) in prosecuting and addressing crimes of such nature.

Information Technology Act, 2000:

The most important act governing the wrongs committed under cybercrimes are monitored through the **Information Technology Act (ITA)** of 2000. ITA secures transactions done online on e-Commerce websites by making them safe and secure through the process of electronic documentation, thereby making it easier to trace and integrate with Government records, reducing the scope of frauds and scams conducted through the means of electronic media. Numerous changes and amendments were made to the act throughout the years in order to keep up with clever decisive means of cheating that cyber criminals and terrorists come up with while exploiting pre-existing technological loop holes or legal fallacies. ITA highly stresses on imposing fines and sanctions on the rulebreakers, thereby serving as a precautionary warning to the potential cyber criminals who turn to the profession of deceiving and exploiting people online having had technical expertise but being unable to find jobs.

 ISSN: 2582-6433

The primary objectives[2] of the ITA 2000 were:

1. To give legal recognition to any transaction carried thorugh digital/electronic means
2. To legally recognise digital signatures used in accepting any agreements over the computer.
3. To facilitate digital agreements for the purposes of record keeping and registration
4. To facilitate digital storage of data for companies and corporations.
5. To prevent digital crimes and for individual privacy protection.
6. To enable legal recognition of book keeping and other transaction by banking institutions and other companies. [3]

Indian Penal Code, 1860:

The Indian Penal Code, 1860 and the ITA of 2000 are primarily used in coordination with each other in prosecuting identity theft and related cyber offences. The following sections and the areas broadly covered under them are discussed below:

i. Section 463: Forgery

ii. Section 464: Making a false document

iii. Section 468: Forgery for the purpose of cheating

iv. Section 469: Forgery for the purpose of harming reputation

v. Section 471: Using as genuine a forged document or electronic record

According to **Chapter XVIII** of the **IPC**;

vi. Section 463: Forgery

1. "Whoever makes any false document or false electronic record or part of a document or electronic record, with intent to cause damage or injury], to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery."

[2] *"Cyber Crime Law and Practice"*

[3] India: Cyber Crimes Under The IPC And IT Act - Mondaq. https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence

 ISSN: 2582-6433

2. Section 464: Making a false document

"A person is said to make a false document or false electronic record—

First.—Who dishonestly or fraudulently—

(a) makes, signs, seals or executes a document or part of a document;

(b) makes or transmits any electronic record or part of any electronic record;

(c) affixes any 4 [electronic signature] on any electronic record;

makes any mark denoting the execution of a document or the authenticity of the 4 [electronic signature], with the intention of causing it to be believed that such document or partof document, electronic record or 4 [electronic signature] was made, signed, sealed, executed, transmitted or affixed by or by the authority of a person by whom or by whose authority he knows that it was not made, singed, sealed, executed or affixed; or

Secondly.—Who without lawful authority, dishonestly or fraudulently, by cancellation or otherwise, alters a document or an electronic record in any material part thereof, after it has been made, executed or affixed with [electronic signature] either by himself or by any other person, whether such person be living or dead at the time of such alteration; or Thirdly.—Who dishonestly or fraudulently causes any person to sign, seal, execute or alter adocument or an electronic record or to affix his [electronic signature] on any electronic record knowing that such person by reason of unsoundness of mind or intoxication cannot, or that by reason of deception practised upon him, he does not know the contents of the document orelectronic record or the nature of the alteration."

3. Section 468: Forgery for the purpose of cheating

"Whoever commits forgery, intending that the [document or electronic record forged] shall be used for the purpose of cheating, shall be punished with imprisonment of either description fora term which may extend to seven years, and shall also be liable to fine."

4. Section 469: Forgery for the purpose of harming reputation

"Whoever commits forgery, [intending that the document or electronic record forged] shall harm the reputation of any party, or knowing that it is likely to be used for that purpose, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine."

5. Section 471: Using as genuine a forged document or electronic record

"Whoever fraudulently or dishonestly uses as genuine any [document or electronic record]

 ISSN: 2582-6433

which he knows or has reason to believe to be a forged [document or electronic record], shall be punished in the same manner as if he had forged such [document or electronic record]."

Cybercrime Cases in India:

We will now take a look into a few landmark cybercrime cases that shaped the cyber laws in Indian landmark.

a. CBI v. Arif Azim[4] (Sony-Sambandh.com Case):

The very first cybercrime conviction in India came along with the "Sony-Sambandh" case. Sony India Private Limited (hereinafter referred to as "SONY") ran a website; www.sony-sambandh.com, that allowed NRIs to send products by SONY to their relatives and friends in India for a prepaid transaction. The company would do the necessary undertaking involved in delivering the products to the involved recipients. SONY, in the year 2002, would then go on to file a complaint after a fraudulent purchase made through their website that would involve assisted investigations from the CBI. In May 2002, an individual anonymously logged onto the website disguising themselves under a false identity of an individual named "Barbara Campa" and ordered a coloured television set along with a pair of cordless headphones. The individual had allegedly requested to deliver the product to a Noida resident by the name of Arif Azim and seemingly had used their credit card for processing the payment. The payment was cleared, thereby allowed for the completion of the transaction, and the products were delivered to the involved individual. On completion of the delivery, the company encaptured digital pictures so as to indicate that the delivery was accepted by Arif Azim. A month and a half afterwards, the credit card agency tagged the previously transacted amount to be an unauthorised one, owing to a dispute raised by the real owner who had denied of having made the purchase. SONY then filed a complaint for online cheating at the CBI and a case was registered under Section 418[5], Section 419[6] and Section 420[7] of the IPC. The matter was investigated and the arrest of Arif Azim was made. Investigations revealed that Arif Azim, being an employee of a call centre in

[4] ***[(2008) 105 DRJ 721: (2008) 150 DLT 769]***

[5] Section 418: "Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect."

[6] Section 419: "Punishment for cheating by personation"

[7] Section 420: "Cheating and dishonestly inducing delivery of property."

ISSN: 2582-6433

Noida had misappropriated his position to get the credit card number of the victim which he wouldgo on to misuse for his personal gains. The CBI recovered the the cordless headphones along with the coloured television set. With enough admissible proof, the accused finally admitted his wrongdoings. The court then convicted Arif Azim under the Section420, Section 419 and Section 418 of the IPC, making it the first cybercrime case to be conducted in the Indian landscape. The defendant, Arif Azim, being a young person ofonly 24 years of age at that time, was given a compassionate sentence owing to his age and him being a first time convict. The court would discharge him eventually, with a probation for one year.

Official Maharashtra Government Website hacked:

The official website of Maharashtra government was hacked in September, 2007. Immediate action was taken by Cyber Crime branch police in investigating and trackingdown the parties involved. The state government website[8], containing important details and information regarding government departments, reports, circulars, was down for anentire day, restricting access to the general public. Some IT experts had speculated thatthe breaching party might have had destroyed all of the website's information and content. Sources suggested that the hacking group might be operating from Saudi Arabia and identified themselves under the name "Hackers Cool Al-Jazeera". The government website was previously attacked by several virus attacks in the past but never had been the target of a hacking attempt. Investigating IT officials said the website was unprotected and without a firewall.

ICICI Pune fraud case:

Three people were held guilty in online credit card scam who had misappropriated a customer's credit card details online to book airline-tickets. The Cyber Crime Investigation Cell in Pune arrested Dharmendra B. Kale, Ahmed Sikandar Sheikh and Mahavir Singh, the three alleged individuals involved in the crime. Further investigations revealed that details belonging to almost 100 people were misused. Ahmed was employed in a branch of State Bank of India(hereinafter referred to as SBI) while the other two were colleagues workig together at some private instituition. The authorities at SBI claim thay Sheikh had misused the banking systems for the purposes of financial theft and phishing. One of ICICI's customers,had received a suspicious message one day, alerting for the purchase of the air tickets.

ISSN: 2582-6433

The official website of the Maharashtra Government: http://www.maharashtragovernment.in

The customer being aware immediately contacted his bank and inquired about the purchase and got to know about the misuse. A complaint was filed by Mr Parvesh Chauhan on the customer's behalf. Police had to check for tansaction log details on the net to pin point the bank involved in processing the transaction and finally narrowed it to SBI where it was discovered that Sheikh was the one working with handling credit cards and had thus been able to misappropriate some accounts for his own self benefit, working in coordination with Kale and Singh. Cyber cell, after 8 days of investigative involvement, had finally caught the culprits

b. Parliament Attack Case:

A laptop, confiscated from the two terrorists, who were shot dead on December 13, 2001, during the Parliament siege, was transported to the Computer Forensics Division of Bureau of Police Research and Development, Hyderabad, which had previously handled some of the top cyber cases. The laptop physically had several evidences that would confirm the two terrorists' motives, including the stickers of the Ministry of Home Affairs that they had deceitfully used to get into Parliament house. It also contained the fake identity card being carried by one of the two terrorists which had a carefully forged Government of India seal and emblem, with the residential address locating them to the state of Jammu and Kashmir. Foreinsic cyber investigations carried on their laptop later revealed every detail was forged very minutely, with extreme care to include the realistic details.

c. First ATM Card Fraud Case in India:

The Chennai City police had uncovered and busted an international gang that was suspected to be constantly involved in a multitude of cyber crimes across the world, with the arrest of Deepak Prem Manwani (aged 22) who was caught red-handed in the act of breaking into an ATM in the city. The arrested individual was on the FBI watch list of the United States and had cash amounting Rs 7.5 lakhs were recovered from him during the time of his detention, cash that was allegedly knocked off from two different ATMs in the city. The investigation of Mawani's case led to the discovery of an elaborate scam that was assisted by Mawani's contacts in Europe. It was discovered that Mawani was involved in the selling of credit cards of American Banks by these contacts at a price of $5 per card. They operated a site

ISSN: 2582-6433

who had found a way to phish Personal Identification Numbers (PIN) of card users by floating a site, exactly similar to that of a reputed telecom company with millions of subscribers and customers. Owing to the stark similarity of the websites, genuine subscribers and users had logged into the site which promised to return them $11.75, an amount they seemingly claimedto have charged by "mistake". The login would thus allow the hackers to access their PIN. Soon thousands of users were defrauded and thus the FBI was alerted on the reception of numerous large-scale complaints from the previously billed credit card users and banks in the United States and consequently lodged an investigation into thematter while also alerting the CBI in New Delhi that the international group might have had developed some connections in India too. Mawani was eventually granted bail after the completion of interrogations and investigations by the CBI.

A brief overview of Information Technology Amendment Act, (2008):

The ITA 2000 was subject to extensive debates, reviews, and criticisms, being the very first legislation on technology, digital communication and computers. Some sections of the act were called out to be extremely harsh towards the growth, progress and functioning of the IT industry while others were considered to be too laxed and lenient. The reliance of the ITA 2000 on IPC in prosecuting the criminals was also questioned and challeneged with many legal and technological academics, researchers, scholars and lawyering individuals believing that it allowed investigators to rely too much to one-time tested"one and half century" old IPC. Thus there arose a need for a more detailed amendment of the Information Technology Act of 2000. In the drafting of the amendment, many major IT industry players and bodies were consulted and advisory groups and committees were formed to come up with better and more comprehensive legal acts to cover the scope of loopholes and inconsistencies previously left uncovered by ITA, 2000. This Amendment Act was made effective from 27th October 2009 after receiving the Presidential assent on 5th Feb 2009.

Some of the prominent features of the ITA(Amendent) are as follows:

- Focussing on data privacy
- Focussing on Information Security
- Defining cyber cafe
- Making digital signature technology neutral

ISSN: 2582-6433

- Defining reasonable security practices to be followed by corporate
- Redefining the role of intermediaries
- Inclusion of some additional cyber crimes like child pornography and cyber terrorism
- Authorizing an Inspector to investigate cyber offences

Limitations of the ITA 2000:

The law continues to suffer from following weaknesses:

1. Copyright infringement has not been mentioned in the act
2. No domain name protection
3. Act does not relate to taxation

CONCLUSION

Technological progress has had aided the Indian as well as different societies across the globe in making remarkable progress owing to the advanced means of communications. It however,tends to play the role of a double edged sword. With the increasing reliability of the society ontechnology, there will be increasing instances of defiance of law and order in the cyberspace, especially given the challenging problem of jurisdiction over the Internet. The ITA 2000 was the first step towards securing digital transactions and communications in India and served an important milestone in modern Indian history. The ITA(A) provides scope for criminal prosecution and was not covered under the scope of this project as it would further introduce effective sanctions that act as deterrents in keeping away criminals from the cyberspace. The project details the Information Technology Act, 2000, and covers some landmark cybercrime cases that were instrumental in shaping the prospective areas of the ITA Amendment of 2008. The prosecution of criminals committing acts on the cyber space was taken up in different casescenarios and gave us an insight into the functioning of how policing and administrative authorities are empowered to fight cybercrime. Some topics were left out to be covered in the scope of this project owing to time and resource constraints, but the overall objective of taking a look into the functioning of India's cyberlaws was achieved.

ISSN: 2582-6433

SOURCES:

Journals and Articles:

1. ANIMESH SARMAH, ROSHMI SARMAH, AMLAN JYOTI BARUAH, A brief study on Cyber Crime and Cyber Laws of India, International Research Journal of Engineering and Technology (IRJET), Volume 04 Issue 06, June-2017
2. Cyber Crime Law and Practice, The Institute of Company Secretaries of India, November 2016
3. DEVASHISH BHARUKA, Indian Information Technology Act, 2000, Criminal Prosecution Made Easy for Cyber Psychos, Journal of the Indian Law Institute, July- September 2002, Volume 44, No.3, pp. 354-379
4. SANJAY GOEL, National Cyber Security Strategy and the Emergence of Strong Digital Borders, Connections, Winter 2020, Volume 19, No. , pp 73-86, Partnership for Peace Consortium of Defence Academies and Security Studies Institutes
5. GLENN ALEXANDER CROWTHER, The Cyber Defense Review, Volume 2, No. 3, pp. 63-78, Army Cyber Institute
6. TALAT FATIMA, Cyber Crimes, EBC Publishing, Third Edition, 2021

Internet Websites:

1. JSTOR Home (https://www.jstor.org)
2. LexisNexis India Bookstore: Law Books, Legal Books, Law Journals, Student Books, Bareacts, eBooks (https://www.lexisnexis.in/)
3. EBC Reader (ebcreader.com)
4. www.academia.org