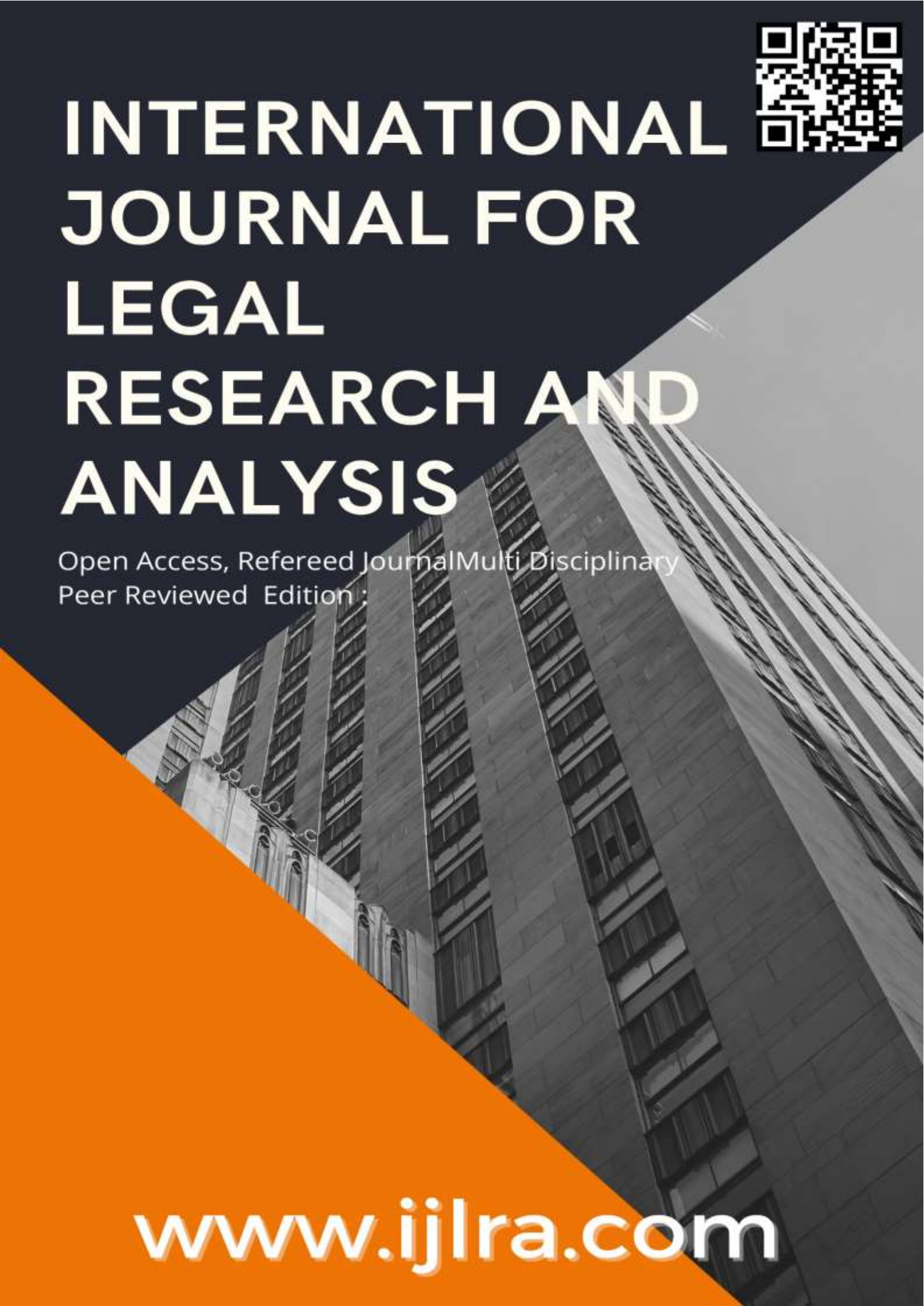
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :



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

TERRORISM VIS-À-VIS CYBER LAWS IN INDIA: ISSUES AND REDRESSAL

AUTHORED BY - UMAKANT TIWARI
ENROLMENT NO- A8101823083
AMITY LAW SCHOOL,
AMITY UNIVERSITY, UTTAR PRADESH, LUCKNOW

CERTIFICATE

I hereby certify that-

Umakant Tiwari, A8101823083 student of **LLM (2023-2024)** at Amity Law School, Amity University, Uttar Pradesh has completed the project report on "**Terrorism vis-à-vis cyber laws in India: Issues and Redressal**", during **2nd** semester under my supervision.

(a) The presented work embodies original research work carried out by the student as per the guidelines given in university regulations.
(b) The research and writing embody in the thesis are those of the candidate except where due reference is made in the text.
(c) I am satisfied that the above candidate's prima facie, is worthy of examination both in term of its content and its technical presentations relative to the standards recognized by the university as appropriate for examination.
(d) I certify that in accordance with NTCC guidelines, the report does not exceed the pre-scribed maximum word limit; or prior approval has been sought to go beyond the word limit.
(e) Wherever work from other source has been used, all debts (for words, data, arguments

 ISSN: 2582-6433

and ideas) have been appropriately acknowledged and referenced in accordance with the requirements of the NTCC regulations and guidelines.

Signature Of the Faculty

JUHI SAXENA

Amity Law School

 ISSN: 2582-6433

DECLARATION

Title of project report "**Terrorism vis-à-vis cyber laws in India: Issues and Redressal**".

I understand what plagiarism is and am aware of the university's policy in this regard.

…….

I declare that

(a) The work submitted by me in partial fulfillment of the requirement for the award of degree **LLM** assessment in this dissertation is my own; it has not previously been presented for another assessment.

(b) I declare that this dissertation is my original work. Wherever work from other source has been used, all debts (for words, data, arguments and ideas) have been appropriately acknowledged and referenced in accordance with the requirements of NTCC regulations and guidelines.

(c) I have not used work previously produced by another student or any other person to submit it as my own.

(d) I have not permitted and will not permit anybody to copy my work with the purpose of passing it off as his or her own work.

(e) The work conforms to the guidelines for layout, content and style as set out in regulations and guidelines.

Date: 21/04/2024

UMAKANT TIWARI

A8101823083

LLM

 ISSN: 2582-6433

ACKNOWLEDGEMENT

The ability to complete my dissertation had its origins before the commencement of my formal studies at amity law school, amity university. Without the benefit of so many great interactions with people throughout my life, this path might not have opened for me to pursue. As such, it is necessary to reach back and thank a great number of people. To acknowledge everyone, is a formidable undertaking and I make no apology for the length of these acknowledgement. It is loosely presented in chronological order, with overlap in names reflective of multiple influences certain people have had on my journey. First, I thank to my god who gave me that much capacity and made me able by giving adequate intellect so that I got succeed in making my dissertation. Now i would like to thank my mentor and guide **Ms. Juhi Saxena,** faculty of law, for selecting me to work on this research and guiding me throughout. I thank her for his intellectual guidance throughout my dissertation more as an academician. Thanks to my mother, **Mrs. Nema Tiwari**, for teaching me to love learning and letting me know that how to present myself in the various chapters of life. Thanks to my father **Mr. Jagdish P Tiwari** , for teaching me activeness, presence and confidence. I would undoubtedly like to thank my friends who helped me in the completion of the work and all my well-wishers who had helped in the completion of this work.

Mr. UMAKANT TIWARI
A8101823083

 ISSN: 2582-6433

Table Of Contents

 ISSN: 2582-6433

2.2 PREVENTION OF CYBERCRIME

2.3 ANALYZING RISK EXPOSURE

2.4 PREVENTIVE MEASURES FOR CYBERCRIME

2.5 CYBERCRIME LAWS

 ISSN: 2582-6433

Chapter -3

INFORMATION TECHNOLOGY ACT, 2000 OVERVIEW OF THE ACT

 ISSN: 2582-6433

CHAPTER-4

EVOLUTION OF CYBER CRIME

4.1 INTRODUCTION

4.2INDIAN PENAL CODE,1860

[1] http://www.infoplease.com/ipa/A0872842.htm

 ISSN: 2582-6433

4.3INFORMATION TECHNOLOGY RULES

CHAPTER-5

INTERNATIONAL PERSPECTIVE OF CYBER LAW

5.1 INTRODUCTION

5.2CYBER LAW IN PEOPLE'S REPUBLIC OF CHINA

5.3 CYBER LAW IN UNITED STATES OF AMERICA

5.4 APPLICATION OF CYBER LAW IN PRESENT DAY SOCIETY

CHAPTER-6

CONCLUSIONS, SUGGESSTIONS AND FINDINGS

 ISSN: 2582-6433

6.1 FINDING

6.2 CONCLUSIONS

6.2.1 HESITATION TO APPROACH COURT OF LAW IN CASE OF CYBER CRIMES

6.2.2 TIME OF DISPOSAL FOR CYBER CRIME

6.2.3 REASONS FOR NOT USING E-COMMERCE WIDELY INSTEAD OF ENACTMENT OF IT

 ISSN: 2582-6433

6.2.4 COMPARISON OF GENERAL MATTER WITH MATTER REGISTERED UNDER IT ACT

6.2.5 PARAMETERS FOR SPEEDY DISPOSAL FOR THE MATTER REGISTERED UNDER THE ACT

6.3 SUGGESTIONS

6.3.1 HESITATION TO APPROACH COURT OF LAW IN CASE OF CYBER CRIMES

6.3.2 TIME OF DISPOSAL FOR CYBER CRIME

6.3.3 REASONS FOR NOT USING E-COMMERCE WIDELY INSTEAD OF ENACTMENT OF IT

6.3.4 PARAMETERS FOR SPEEDY DISPOSAL FOR THE MATTER REGISTERED UNDER IT ACT.

6.3.5 GENERAL SUGGESTIONS

6.4 FOR CYBER LAW INSTEAD OF CRIMINAL PROCEDURE COURT (CR. P. C).

 ISSN: 2582-6433

CHAPTER -1
INTRODUC
TION

A general definition of cyber law is a legal system that deals with the internet, computer systems, cyberspace, and any issues pertaining to cyberspace or information technology. Contract law, privacy regulations, and intellectual property laws are only a few of the many topics covered by cyberspace law. It regulates electronic commerce, information and data security, and the dissem- ination of software electronically. E-documents are accepted as legal documents under cyberlaw. Additionally, the system offers a framework for electronic form filling and transactions related to electronic commerce. To put it simply, it's a statute that addresses cybercrime. With the rise in popularity of e-commerce, it is now essential to ensure that appropriate standards are in place to prevent fraud. The rules governing cybersecurity are numerous and widely differ depending on the country's geographical location.

Depending on the offense committed, different punishments apply, which can include fines and or jail time adopted as the first cyber law in history was the Computer Fraud and Abuse Act of 1986. The illicit use of digital information and unapproved computer access are prohibited. As the use of the Internet has increased, so too has cybercrime. Cybercrime has grown in tandem with growing Internet usage. There are numerous tales in the media nowadays about cybercrimes such as identity theft, crypto jacking, child pornography, cyber terrorism, and so on. In cybercrime, the computer utilized as either a tool or a target, or both, to accomplish illegal be- havior. Electronic

 ISSN: 2582-6433

commerce (e-commerce) and online stock trading have skyrocketed in our fast-paced digital age, fueling an increase in cybercrime.[2]

[2] https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users (Accessed on 3 rd February, 2022)

 ISSN: 2582-6433

WHAT IS CYBERCRIME?

Any criminal behavior involving a computer, networked device, or comparable technology is referred to as cybercrime. While some cybercrimes are conducted with the intention of making money for the perpetrators, other crimes are chosen with the goal of causing direct injury or turning off the computer or gadget. Moreover, other people might disseminate viruses, illicit data, photographs, or other kinds of content via computers or networks. Cybercrime can result in a wide range of profit-driven criminal actions, such as ransomware attacks, email and internet scams, identity theft, and frauds involving credit cards, financial information, or any other typeof payment card. The Information Technology Act of 2000 and the Indian Penal Code of 1860 both encompass cybercrime in India. It is the IT Act of 2000 that talks about cybercrime and electronic commerce. However, the Act was amended in 2008 to define and punish cybercrime. Many amendments also were made to the Indian Penal Code 1860 and the Reserve Bank of IndiaAct[3]. Any illegal activity involving a computer, networked device, or network is known as cy- bercrime. Certain cybercrimes are performed directly against computers or devices in an attempt to damage or disable them, however the majority of cybercrimes are committed with the inten- tion of making money for the offenders. Others spread viruses, unlawful information, images,and other content via computers and networks. Computers are the target of some cybercrimes, which aim to infect them with a computer virus that spreads to other devices and, occasionally, entire networks. One of cybercrime's most serious consequences is financial loss. Cybercrime is the umbrella term for a wide range of profit-driven illegal actions, such as ransomware attacks, identity theft, email and internet fraud, and attempts to get credit card or other payment card in- formation. The United States Department of Justice (DOJ) categorizes cybercrime into three types: crimes in which the computer is the target, such as gaining network access; crimes in which the computer is used as a weapon, such as launching a denial-of-service (DoS) assault; Crimes in which a computer is used as an accessory to a crime, such as storing unlawfully ob- tained data on a computer.[4]The United States has ratified the Council of Europe Convention on

 ISSN: 2582-6433

[3] http://cybercrime.planetindia.net/intro.htm (Accessed on 4th February, 2022)

[4] Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National

 ISSN: 2582-6433

Cybercrime, which defines cybercrime as a broad range of destructive acts, including unauthorized data interception, system interferences that compromise network integrity and availability, and copyright infringements. Because cybercrime can now be committed remotely, there is no longer a physical requirement for the criminal to be present; instead, the ease, speed, anonymity, and boundary-less nature of the internet has allowed for a rise in the volume and velocity of cybercrime operations. Computer-based versions of financial crimes, such as ransomware, fraud, and money laundering, as well as crimes like stalking and bullying, are easier to commit. Both highly organized international criminal networks made up of skilled programmers and other knowledgeable individuals as well as individuals or groups with little technical aptitude may be involved in cybercrime. In an attempt to reduce the likelihood of being discovered and facing legal action, cybercriminals often choose to operate in countries with weak or nonexistent cyber- crime laws. If there is digital data, opportunity, and motive, cybercrime can begin anywhere. State-sponsored entities like China's intelligence agencies are examples of cybercriminals, as are individual users engaged in cyberbullying. The act of cybercrime is not isolated; it is a part of nature in many ways. Put differently, hackers usually rely on third parties to complete their crimes. This applies to situations where malware creators sell their code on the dark web, drug distributors use bitcoin brokers to hold virtual currency in escrow, and state threat actors pilfer intellectual property (IP) from IT companies. Cybercriminals employ diverse attack vectors to execute their cyberattacks and are always seeking for novel approaches and plans to accomplish their objectives without being detected or apprehended. Twelve Although social engineering is usually an essential part of the execution of most forms of cybercrime, cybercriminals frequentlyutilize malware and other types of software to carry out their crimes. Email phishing is a major feature of many cybercrimes, especially targeted attacks like business email compromise (BEC), when an attacker poses as a company owner via email to trick employees into paying fictitious bills.

1.3 SCOPE OF CYBERLAW IN INDIA

Phishing, identity theft, and other types of fraud are all part of the rapid rise in cybercrime in recent years.

 ISSN: 2582-6433

However, the present laws do not provide enough or complete coverage.

 ISSN: 2582-6433

Furthermore, we anticipate a higher consolidation of cyber criminal penetration in India.

This highlights the significance of building more effective and deterrent legal frameworks, as well as stricter cybercrime legislation. One of the most anxiously awaited in Indian cyberlegislation is the National Cyber Security Strategy.

This strategy seeks to be a comprehensive guidebook for individuals, policymakers, and other stakeholders, as well as a follow-up to the 2013 National Cyber Security Policy.

The strategy will almost certainly give more insight on the appropriate response mechanisms for increasing cyber security in government and other companies.

India must quickly begin development on a distinct national cyber security law.

The necessity for such a law is crucial because it would be a vital weapon in protecting India's cyber security and cyber sovereign interests.

At a time when many other nations have already begun adopting specific cyber security legislation, India is slightly behind the curve.

In this sense, appropriate action is necessary.

In the future, the government should focus on more effective methods to combat cybercrime.

It is also envisaged that other appropriate improvements in Indian cyber law would be implemented, including allowing legislative measures to handle the challenges created by fast evolving technology

1.4 THE MAIN OBJECTIVES OF THE STUDY ARE AS FOLLOWS:

- To study the reasons why people hesitate to approach court of law in the dispute regarding cyber crime.

 ISSN: 2582-6433

- To study the average time to decide any matter registered under the IT Act 2000.
- To find out the reasons for E-commerce not being widely used instead of enactment of IT Act 2000.
- To compare any general matter with, matter registered under the IT Act 2000.
- To suggest parameters for speedy disposal of the matters registered under die IT Act 2000

 ISSN: 2582-6433

1.5 METHODOLOGY OF THE STUDY

Keeping in the mind the aforesaid objectives, the methodology chosen for the present study is elaborated as under-

1. Survey Method: In order to elicit relevant information pertaining to the problems of Cyber Crimes a survey method was adopted.

2. Observation Method: To have a microscopic view of the IT act-2000, the researcher adopted an observation method too. The objective of this method is to cross examine every statute relatedto cyber law.

1.6 HYPOTHESIS OF THE STUDY:

With the above stated objectives in mind, the following hypothesis was formed for the present study by the researcher.

- . There are no parameters for speedy disposal of the matter registered

under the IT Act 2000.

- People hesitate to file a criminal case under IT Act 2000.
- There are some reasons for E-commerce for not being widely used instead of enactment of the IT Act 2000.

1.7 AREA OF CYBER LAW

Cyber laws contain different types of purposes. Some laws establish guidelines for how people and businesses can use computers and the internet, while others shield citizens from becoming victims of crime as a result of dishonest online activity. [5]

The following are the main areas of cyber law:

1.Fraud: To safeguard consumers from online fraud, cyberlaws are essential. Identity theft, credit card theft, and other financial crimes committed online are prohibited by law. Identity thieves may be charged as accomplices or as state criminals. Cyber attorneys endeavourto both defend

 ISSN: 2582-6433

and prosecute against claims of online fraud

[5] S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary, 2001, p. 81.

 ISSN: 2582-6433

2. Copyright: The internet has led to an increase in copyright breaches. Copyright violations were all too rampant when people first started conversing online. To safeguard both corpo- rations and individuals' copyrights, a legal action must be filed. The field of cyber law knownas copyright violation defends people's and businesses' legal entitlements to financial gain from their creative works. [6]

3.Defamation- Many workers turn to the internet to express themselves. When people use the internet to distribute false information, it can go too far and become defamation. Defamation laws are civil regulations that shield persons from false public remarks that can harm their reputations or the reputations of their employers. When people create statements on the in- ternet that violate civil laws, defamation laws are employed

4.Harassment and Stalking: Online postings can go beyond the law's prohibitions against harassment and stalking. There is a violation of both civil and criminal statutes when someone repeatedly posts threatening comments about another individual online. When stalking occurs over the internet or through other electronic communication, cyber lawyers both prosecute and defend the victim.

5.Freedom of Speech: The free exchange of ideas is a crucial component of cyber law. Free- dom of speech rules also let people to express their opinions, despite the fact that cyber laws prohibit specific acts online. The boundaries of free expression, particularly those imposed by laws against obscenity, must be discussed with clients by cyber attorneys.

6.Trade Secrets: To protect their trade secrets, businesses that conduct business online frequently rely on cyber regulations. For instance, the algorithms that produce search resultsare developed in great detail by Google and other internet search engines. They also put a lotof effort into developing additional features, such as flight search services, intelligent assistance, and maps. Cyber laws support these businesses in taking legal action when requiredto safeguard their trade

 ISSN: 2582-6433

secrets

[6] Talat Fatima, Cyber Crime (1st Edition, Eastern Book Company, Lucknow 2011) p. 64-68

 ISSN: 2582-6433

7. **Contracts and Employment Law**: You have violated cyber law each time you click a button that indicates your agreement to a website's terms and conditions. [7]

Advantages of Cyber Law:

Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.

- Digital signatures have been given legal validity and sanction in the Act.
- It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.
- It allows Government to issue notifications on the web thus heralding e-governance.
- It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.
- The IT Act also addresses the important issues of security, which are so critical to the success of electronic transaction.

 ISSN: 2582-6433

- Cyber Law provides both hardware and software security.[8]

[7] http://www.oxforddictionaries.com/definition/english/cybercrime

[8] Stambaugh, H., et. al, Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice Report, Washington, Dc: U.S. Department of Justice, March 2001.Available at : https://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf

 ISSN: 2582-6433

1.8 NEED FOR CYBER LAW

In today's techno-savvy environment, the world is becoming more and more digitally sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc.. Cyber laws address every legal issue relating to online crime. The demand for cyber laws and their implementation has accelerated along with the growth in internet users.

In today's largely digitalized society, cyber law has an impact on practically everyone.
For example:
1-The majority of share transactions take place in demat form.

2- Virtually all businesses heavily rely on their computer networks and save their important data electronically

.3. Government documents, such as tax filings and contracts

4-Consumers are increasingly using credit/debit cards for shopping.

5-. The majority of people communicate via email, phones, and SMS messages.

6- Even in "non-cyber crime" cases, important evidence is found in computers/cell phones eg: in cases of murder, divorce, kidnapping, tax evasion, organized crime, terrorist operations, counterfeit currency etc.[9]

7- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking,

 ISSN: 2582-6433

denial of service, hacking, pornography etc. are becoming common.

[9] http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf

 ISSN: 2582-6433

CHAPTER-2

CYBER CRIME AND ITS CLASSIFICATION

2.1TYPES OF CYBERCRIME

The following are seen as examples of several sorts of cybercrimes:

CYBER-BULLYING

A cyberbully is someone who harasses or bullies others through the use of electronic devices such as computers, mobile phones, laptop computers, and so on. Social media, messagingplatforms, gaming platforms, and mobile devices may all be used. This frequently entails repeated behavior designed to frighten, anger, or shame those being targeted. [10]

CYBER-GROOMING

The issue of cyber grooming includes someone developing a friendship with a youngster and then tempting, teasing, or even pressuring them to commit a sexual act.

CYBER-STALKING

Cyberstalking is the practice of harassing or stalking someone online using the internet and other

 ISSN: 2582-6433

technology. Cyberstalking happens using texts, emails, social media posts, and other means, and it is frequently persistent, methodical, and planned.

[10] http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf (Accessed on 7th May 2022)

 ISSN: 2582-6433

CHILD SEXUALLY ABUSIVE MATERIAL

Child sexual abuse materials (CSAMs) are defined as any content featuring sexual pictures in any form, in which both the child being manipulated or abused can be observed. The publication or transmission of material depicting children in sexually explicit acts in an electronic form is prohibited under Section 67(B) of the Information Technology Act. 14 [11]

ONLINE SEXTORTION

Online sextortion happens when a cybercriminal threatens to reveal sensitive and private information on an electronic platform. These criminals threaten others to get a sexual image, sexual favor, or money from them.

ONLINE JOB SCAMS

An online job fraud strategy involves deceiving job seekers by offering them a better job with more pay while giving them false hope. The Reserve Bank of India (RBI) warned citizens not to fall victim to job scams on March 21, 2022. The RBI has highlighted how online job fraud is committed, as well as the measures that the average person should take while applying for any employment opportunity, whether in India or overseas. [12]

PHISHING

The information is sold on the dark web when an email that appears to be from a reliable source contains a malicious attachment designed to steal personal information from the user, including their ID, IPIN, Card number, expiration date, CVV, and other information.

 ISSN: 2582-6433

VISHING

Victims' personal information is taken via their phones in vishing. Cybercriminals utilize sophisticated social engineering techniques to trick victims into disclosing personal information and gaining access to personal accounts. 15 Vishing, like phishing and smishing, deceives

[11] Information Technology Act, 2000, S. 67B

[12] Information Technology Amendment Act 2008, Act 10of 2009

 ISSN: 2582-6433

victims into thinking they are being courteous by replying to the call. Callers can frequently pose as representatives of the government, the tax department, the police department, or the victim's bank.

SMISHING

Smishing is a type of fraud that employs text messages sent through mobile phones to fool victims into dialing a phony phone number, accessing a fraudulent website, or installing harmful software that remains on the victim's computer.

IDENTITY THEFT

When a person impersonates another person or uses an electronic signature, password, or another unique identifier on their behalf, they are impersonating that person or exposing them- selves to identity theft. [13]

DEBIT CARD SCAMS AND CREDIT CARD SCAMS

Unauthorized purchases or withdrawals from another's card are performed to get access to their funds in credit card (or debit card) fraud. Credit/debit card fraud occurs when illegal transactions or cash withdrawals are made from a customer's account. When a criminal obtains access to the cardholder's debit/credit card number or personal identification number, fraudulent conduct happens (PIN). Untrustworthy personnel or hackers may get your information.[14]

CYBEREXTORTION: It is a crime that consists of an attack or threat of an attack followed by a demand for money to halt the assault. The use of ransomware as a form of extortion. In this case, the attacker gets access to an organization's networks and encrypts its papers and files (or anything

 ISSN: 2582-6433

else of 16 value), rendering the material inaccessible until a ransom is paid. This is usually in the form of a cryptocurrency, such as bitcoin.

[13] http://indiatogether.org/uploads/document/document_upload/2141/blawobscenity.pdf

[14] //www.indiancybersecurity.com/case_studies/state_of_tamil_nadu_%20suhas_katti.htm

 ISSN: 2582-6433

CRYPTO- JACKING: An assault that employs programs to mine bitcoins within browsers without the user's knowledge. Crypto-jacking attacks may entail the victim's PC is infected with bitcoin mining software. Many attacks, however, are based on JavaScript code that performs in-browser mining if the user's browser has a tab or window open on the rogue site. There is no need to install malware because loading the infected website executes the in-browser mining code.

CYBER-ESPIONAGE: A cybercrime in which a cybercriminal hacks into systems or networks in order to acquire access to secret information held by the government or another entity. Profit or ideology may inspire an attack. Cyberespionage activities can include any type of cyberattack to collect, modify, or destroy data, as well as using network-connected devices, such as webcams or closed-circuit TV (CCTV) cameras, to spy on a specific individual or group and monitoring communications, such as emails, text messages, and instant messages.

SOFTWARE PIRACY

An assault involving the unauthorized copying, dissemination, and usage of software programs for commercial or personal gain. Trademark infringements, copyright infringements, and patent infringements are frequently related to this sort of cybercrime.

EXIT-SCAM

Not unexpectedly, the dark web has given rise to a digital version of an old crime known as the exit scam. Dark web administrators now move virtual cash kept in marketplace escrow accounts to their own accounts, basically stealing from other criminals[15]

 ISSN: 2582-6433

2.2 PREVENTION OF CYBERCRIME

[15] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

 ISSN: 2582-6433

The International Maritime Organization (IMO) regulations state that the following framework should be used to address the risk of a cyberattack:[16]

• The first step is to define the responsibilities of the individuals involved in managing the cyber risk

• The first stage is to establish the roles and duties of the cyber risk management people.

• The second phase is to identify the systems, assets, data, or capabilities that, if interrupted, may jeopardize the operation.

• It is critical to create risk-control processes and contingency plans to defend against a potential cyber catastrophe and ensure operational continuity.

• It is also critical to design and put in place procedures to identify cyber-attacks as soon as feasible.

• Preparation and execution of strategies to restore important systems and ensure their continuing functioning via resilience.

• Finally, determine and execute backup and restoration procedures for any affected systems.

• establish precise procedures and standards for the business and its employees

• To complement these rules and processes, develop cybersecurity incident response plans.

 ISSN: 2582-6433

• detail the security measures taken to protect the systems and business data.

• When feasible, utilize two-factor authentication (2FA) applications or physical security keys;

[16] Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi 67 Barry Collin, "The Future of Cyber Terrorism," Proceedings of the 11th Annual International Symposium on Criminal Justice Issues, the University of Illinois at Chicago, 1996

 ISSN: 2582-6433

enable 2FA on all online accounts.

•; Verify verbally with financial management the legitimacy of money transfer requests.

• establish intrusion detection system (IDS) rules that identify emails with identical extensions to corporate emails

• Examine any email requests for financial transfers carefully to see whether they are out of the ordinary;

• Employees should be regularly trained on cybersecurity rules and procedures, as well as what to do in the case of a security breach.

• maintain all software release updates or patches on websites, endpoint devices, and systems; a

• Back up data and information on a regular basis to mitigate the impact of a ransomware attack or data breach. Encrypting local hard drives and email platforms, utilizing a virtual private network (VPN), and employing a private, secure domain name system (DNS) server can all help to improve information security and resistance to cybercrime assaults.[17]

2.3 ANALYZING RISK EXPOSURE

 ISSN: 2582-6433

To appropriately prepare for a cyber assault, one must analyze the danger and take it into account. Companies should think about the following: They should evaluate all areas where they are vulnerable to cyberattacks, as well as any operational vulnerabilities that may arise as a resultof them. A vulnerability assessment of all systems is required to identify those that are vital tothe organization, understand the possible vulnerabilities of each, and determine the impact of any

[17] . Coleman, 'Cyber Terrorism' (2003) Directions Magazine, http://www.directionsmag.com/articlephp?article also at http://www.ijiee.org/papers/126-I149.pdf

 ISSN: 2582-6433

cyber-attack on business continuity. The chance of exposure or loss as a result of a cyber attack or data breach on your firm is referred to as cybersecurity risk. A broader, more comprehensive definition is the potential loss or injury caused by an organization's technological infrastructure, use of technology, or reputation. Because of the increasing reliance on computers, networks, programmes, social media, and data worldwide, organisations are becoming increasingly exposed to cyber attacks. Data breaches, a typical cyber assault, have a large negative corporate impact and are frequently the result of inadequately safeguarded data. Global connection and the increased usage of cloud services with inadequate default security measures increase the danger of cyber assaults from outside your firm. 22 What was formerly addressed by IT risk management and access control now requires sophisticated cyber security people, software, and cybersecurity risk management. It is no longer sufficient to rely on traditional informationtechnology personnel and security procedures to secure information.[18] Threat intelligence tools and security programs are clearly needed to lower your organization's cyber risk and expose possible attack surfaces. When prioritising third-party providers, decision-makers must assess risk and have a risk mitigation strategy and cyber incident response plan in place for when a breach occurs.

2.4 PREVENTIVE MEASURES FOR CYBERCRIME

Businesses should implement national or international technological standards that give a high level of protection. These general preventative measures are advised for businesses that lack the essential technical or financial skills.

The following are some preventative measures:

• Using many layers of defense, starting with physical security and progressing to management policies and procedures, firewalls and network design, computer policies, account management,

 ISSN: 2582-6433

[18] Wilson, C. (2005). "Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress". CRS Report for Congress.
also at http://www.history.navy.mil/library/online/computerattack.htm and
http://resources.infosecinstitute.com/cyberterrorism-distinct-from-cybercrime

 ISSN: 2582-6433

security upgrades, and eventually antivirus programs.

• Implementing the concept of least privilege, which limits information and access to just those individuals who require that information.

• Implementing network-hardening measures, ensuring adequate patch management, and proactively reviewing patch management.

• Using technologies such as protocol-aware filtering and segregation to secure vital systems.

• Assuring that removable devices are encrypted and that any USB used in conjunction with another device is virus-free.

• Moreover, it is critical to build business continuity strategies, identify key individuals, and execute processes to minimize the negative impact of a cyberattack from increasing further and to restore corporate operations.

• Organizing regular training and awareness seminars for all staff might also assist[19].

2.5 CYBERCRIME LAWS IN INDIA

There are five major sorts of cybersecurity legislation that must be obeyed.

Cyber laws are becoming increasingly essential in nations with widespread internet use, such as India.

Cyberspace is governed by tight rules that oversee the usage of information, software, electronic

 ISSN: 2582-6433

commerce, and financial activities in the digital world.

India's cyber laws have aided the growth of electronic commerce and electronic government in the country by ensuring maximum connection while reducing security issues.

[19] Gabriel Weimann, Cyber terrorism: How Real Is the Threat? Special Report No.119, United States Institute of Peace, December, 2004.also at https://thepeacemission2013.files.wordpress.com/2013/03/study-guide-united-nationscounter-terrorismcommittee.pdf

 ISSN: 2582-6433

This has also increased the breadth and efficacy of digital media by making it available in a larger range of applications.

In a nutshell, cybercrime is any illicit conduct in which a computer is either a tool, a target, or both.

Cybercrime can entail classic criminal behaviors like as theft, fraud, forgery, defamation, and mischief, all of which are punishable under the Indian Penal Code.

Computer misuse has also given rise to a slew of new-age crimes, which are addressed under the Information Technology Act of 2000.

There are two types of cybercrime.

The Computer as a Target: Using one computer to attack another. For example, hacking, virus/worm assaults, DOS attacks, and so forth.

Using a computer as a weapon: Using a computer to perform real-life crimes. For example, cyber terrorism, IPR infringement, credit card fraud, EFT fraud, pornography, and so on.

Cyber law (also known as cyberlaw) refers to the legal difficulties associated with the use of communications technology, namely "cyberspace," or the Internet.

It is a nexus of numerous legal topics, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to reconcile the issues posed by human activity on the Internet with the legacy legal system that governs the physical world.[20]

 ISSN: 2582-6433

[20] Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf

 ISSN: 2582-6433

Chapter -3

INFORMATION TECHNOLOGY ACT, 2000 OVERVIEW OF THE ACT

3.1 INTRODUCTION

The Indian Parliament has enacted the country's first cyberlaw.

The Act's object is defined as follows:

To provide legal recognition for transactions carried out through electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and information storage, to facilitate electronic filing of documents with Government agencies, and to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934, and for matters concerned Nevertheless, as cyber-attacks become more serious, as well as humans' proclivity to misinterpret technology, various changes are being made to the regulation. [21]

It emphasizes the severe fines and punishments set by the Indian Parliament to safeguard the egovernance, e-banking, and e-commerce industries.

It is vital to highlight that the scope of the IT Act has now been expanded to embrace all modern communication devices.

The Act specifies that, unless otherwise agreed, contract acceptance can be represented

 ISSN: 2582-6433

electronically and that it has legal validity and is enforceable. 28 Furthermore, the Act isdesigned to fulfill its goals of encouraging and establishing an environment suitable for electronic commerce implementation. In 1996, the United Nations Commission on International Trade Legislation produced a model law on e-commerce and digital complexities.

[21] Terror on the Internet: The New Arena, the New Challenges USIP Press Books, 2006. also at http://www.usip.org/sites/default/files/sr119.pdf

 ISSN: 2582-6433

It also mandated that each country establish its own rules governing e-commerce and cybercrime. The Act was established in 2000 to safeguard people and the government's data, making India the 12th country in the world to implement cybercrime laws. It is also known as theIT Act, and it establishes a legal framework for the protection of data relating to e-commerce and digital signatures.[22]

It was revised in 2008 and 2018 to better fulfill the requirements of society. The Act also establishes the powers and restrictions of intermediaries. .

There are 13 chapters, 90 sections, and 2 schedules in the Act.

The Act is divided into the following chapters:

The first chapter discusses the Act's application as well as definitions of key terms used in the Act.

The second chapter discusses digital and electronic signatures.

Chapters 3 and 4 covers electronic governance and electronic recordkeeping, respectively. Chapter 5 is concerned with the protection of these documents, whereas 29 Chapter 6 is concerned with certifying authority requirements.

Chapter 7 also contains the certifications required to issue an electronic signature.

The obligations of subscribers are described in Chapter 8, and different punishments are described in Chapter 9.

Chapter 10 contains parts of the Appellate Tribunal. Chapter 11 discusses numerous data breach offenses and associated penalties.

Chapter 12 specifies the situations under which intermediaries are not accountable for any crime or violation of data privacy. The miscellaneous chapter is the final chapter, i.e., Chapter 13. [23]

The Act has two schedules: Schedule 1 lists the documents and data to which the Act does not apply. Schedule 2 addresses electronic signatures and authentication mechanisms.

 ISSN: 2582-6433

[22] See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyberterrorism-the-new-normal/

[23] http://www.thehindu.com/todays-paper/tp-national/prevent-access-to-child-pornographycentretold/article8287151.ece

 ISSN: 2582-6433

Section 1 of the Act states that it applies to the entire country, including the state of Jammu and Kashmir. This Act's application also includes extraterritorial jurisdiction, which means it applies to someone who commits such an offense outside of the nation. If the source of the offense, i.e., a computer or similar equipment, is in India, the offender shall be penalized by the Act, regardless of nationality.

The Act, on the other hand, does not apply to materials listed in Schedule 1.

They are as follows:

• Any negotiable document that is not a cheque, as defined in Section 13 of the Negotiable Instruments Act of 1881.

• Any power of attorney granted by Section 1A of the Powers of Attorney Act of 1882.

• According to Section 3 of the Indian Trusts Act of 1882, any type of trust.

• Any will, including testamentary distribution, made by the Indian Succession Act of 1925.

• Any contract or deed of sale of immovable property.

3.2 OBJECTIVE OF THE ACT

The Act was enacted to address e-commerce and all of the complexities associated with digital signatures, having the following goals in mind:

• The Act's goal is to safeguard all electronic transactions.

• E-commerce has reduced the number of papers required for communication.

• It also provides legal protection for electronic communication and information sharing.

• It safeguards digital signatures that are needed for legal authentication.

 ISSN: 2582-6433

• It limits the activity of intermediaries by limiting their authority.

• It outlines several offenses linked to people's data privacy and so safeguards their data.

• It also governs and safeguards sensitive data kept by social media platforms and other electronic intermediaries.

 ISSN: 2582-6433

• It recognizes electronic books of accounts as required by the Reserve Bank of India Act of 1934.

3.3FEATURES OF THE ACT

The following are the Act's features:

• The Act is based on UNCITRAL's Model Law on E-Commerce.

• It has extraterritorial authority.

• Section 2 specifies several terms used in the Act, such as cyber cafés, computer systems, digital signatures, electronic records, data, asymmetric cryptosystems, and so on (1).

• It safeguards all electronic transactions and contracts and declares that all such contracts are legitimate. (10A Section)

• It also recognizes digital signatures and provides authentication mechanisms.

• It includes laws about the Controller's appointment and authority.

• It accepts foreign certifying authorities (Section 19).

• It also specifies potential penalties if a computer system is harmed by someone other than the system's owner.

• The Act also includes provisions for the establishment of an Appellate Tribunal. The Appellate Tribunal hears all appeals from judgments of the Controller or other adjudicating authorities.

• Furthermore, the High Court hears appeals from the tribunal.

• The Act outlines several data-related offenses and associated penalties.

 ISSN: 2582-6433

• It establishes conditions under which intermediaries are not held accountable even if data privacy is violated.

• The Act establishes a cyber regulatory advisory body to advise the Central Government on all topics about e-commerce or digital signatures

 ISSN: 2582-6433

3.4 ELECTRONIC RECORDS AND SIGNATURES

Section 2(1)(t) of the Act defines electronic records as "any data, picture, record, or file conveyed by an electronic medium." Section 2(1) (a) defines an electronic signature as any signature used to authenticate any electronic record in the form of a digital signature.[24]

However, asymmetric cryptosystems and hash functions, as specified in Section 3 of the Act, will have an impact on such authentication.

Section 3A further specifies the requirements for a trustworthy electronic signature.
They are as follows:

- Signatures are regarded as credible if they are connected to the signing or authenticator
- If the signatory has control over the signatures at the moment of signing.
- Any change to such a signature must be identifiable after it has been fixed or altered.
- Any changes made to information verified by the signature must be detectable.
- It must also meet any additional requirements imposed by the Central Government. According to Section 10 of the Act, the government can create rules for electronic signatures at any moment.

Section 11 of the Act specifies the attribution of an electronic record. If an electronic record is supplied by the creator or anybody acting on his behalf, it is credited.
If the originator has not indicated a specific way, the person receiving the electronic record shall acknowledge receipt of the record in any manner.
According to Section 13, an electronic record is dispatched when it enters another computer

 ISSN: 2582-6433

source that is not within the originator's control.

The following factors influence the timing of receipt:

• Receipt happens when an electronic record is entered into the targeted computer resource after

[24] India Cyber Law and Cases, one of the largest Database of Cyber Law and Cases from India. Available at: http://cybercases.blogspot.com/.

 ISSN: 2582-6433

the addressee has donated any computer resource.

• If the record is sent to another computer system, the reception happens when the recipient retrieves it.

• When the addressee has not designated a computer resource, the reception happens when the record enters the addressee's computer source.

3.5 RECORDS AND SIGNATURES

Section 17 discusses the appointment of the controller, deputy controllers, assistant controllers, and other certifying authority officials.

The controller directs the deputy controllers and assistant controllers, who carry out the tasks assigned to them. The Central Government will set the term, qualifications, experience, and working conditions of the Controller of certifying authorities[25].

It will also determine the location of the Controller's headquarters.

3.6 FUNCTION OF CONTROLLER

The following are the functions of the Controller of certifying authority, according to Section 18:

• He is in charge of overseeing the actions of certifying authorities.

 ISSN: 2582-6433

- He is the one who certifies public keys.
- He establishes the norms and criteria that certifying authorities must follow.
- He outlines the qualities and experience needed to work for a certification body.
- He describes the technique to be followed in keeping authority accounts.
- He sets the terms and conditions for auditors' appointments.
- He monitors corporate transactions and government affairs.

[25] http://www.ibnlive.com/news/india/delhi-police-arrests-con-man-for-credit-card-frauds623798.html

 ISSN: 2582-6433

• He assists in the creation of an electronic system, either jointly or independently.

• He keeps track of all the certifying authorities' information and explains the officers' responsibilities.

• He must handle any disagreements between authorities and subscribers.

• All information and official papers issued by the authorities must contain the Controller's seal.

[26]

3.7 LICENSE OF ELECTRONIC SIGNATURE

To issue an electronic signature, a licensing certificate must be obtained. Section 21 of the Act states that any such license can be obtained by applying to the controller, who will determine whether to accept or reject the application after reviewing all of the papers.[27]

The license is transferrable and heritable and is valid for the duration specified by the federal government.

It is governed by the government's terms and conditions.

An application must meet the following conditions, according to Section 22 of the Act:

• A practice certificate statement.

• The identity of applicant must be verified.

• Fees of Rs. 25,000 are required.

 ISSN: 2582-6433

• Any other document that the central government specifies. The license can be re apply application within 45 days of its expiration date, along with a cost of Rs. 25000. (Chapter 23) Section 24 of the Act allows for the suspension of any license for any reason. No certifying body, however, may suspend the license without first providing the applicant with a reasonable

[26] Understanding Denial-of-Service Attacks (US CERT) http://www.us- cert.gov/cas/tips/ST04-015.html. also at http://www.cybercellmumbai.gov.in/html/cybercrimes/denial-of-service-attack.html

[27] India Cyber Law and Cases, one of the largest Database of Cyber Law and Cases from India. Available at: http://cybercases.blogspot.com/.

 ISSN: 2582-6433

opportunity to be heard. [28]

The following are the grounds for suspension:

• The applicant submits a fake renewal application with false and forged information.

• Failure to comply with the license's terms and conditions.

• A person fails to comply with the Act's terms.

• He did not adhere to the method outlined in Section 30 of the Act.

3.8 POWERS OF CERTIFYING AUTHORITY

The powers and functions of certifying authority are as follows:

• Every such authority must employ hardware that is not vulnerable to intrusion.

• It shall use security procedures to preserve the confidentiality of electronic signatures.

• It is required to provide information about its practice, electronic certifications, and the state of

 ISSN: 2582-6433

these certificates.

• Its job must be dependable

.• The authority has the authority to issue digital certificates.

• The authority must issue a digital signature certificate and confirm that the subscriber holds a private key in addition to the public key specified in the certificate.

• The key can create a digital signature and be validated.

•All of the information provided by subscribers is correct and dependable.

• The authorities may suspend the digital signature certificate for a maximum of 15 days.

[28] Gabriel Weimann, Cyber terrorism: How Real Is the Threat? Special Report No.119, United States Institute of Peace, December, 2004.also at https://thepeacemission2013.files.wordpress.com/2013/03/study-guide-united-nationscounter-terrorismcommittee.pd

 ISSN: 2582-6433

• The authorities may with withdraw a certificate under Section 38 for the following reasons:

• If he passes away.

• If the subscriber is a corporation, the certificate is revoked upon the firm's dissolution[29]

3.9 PENALTIES UNDER IT ACT

The Act imposes fines and compensation in the following situations:

Penalty for causing computer system damage If someone other than the owner uses the computer system and destroys it, he must compensate for all such damages (Section 43).

Other justifications for sanctions and compensation include:

• If he downloads or copies any data from the system.

• Any virus is introduced into the computer system.

• The system is disrupted.

 ISSN: 2582-6433

• Denies access to the computer's owner or authorized user.

• Manipulates or tampers with the computer system.

• Deletes, destroys or modifies the information contained in the system.

• The information kept is stolen. Compensation in the event of a data breach Section 43A states that if a corporation or firm stores the data of its workers or other people, or other sensitive data, in its computer system but fails to safeguard it from hackers and other similar actions, it must pay compensation. Failure to provide the necessary information

[29] Cyber Attacks during the War on Terrorism" India/Pakistan Conflict, Institute for Security Technology Studies - Dartmouth College Vatis, Michael A - September 22, 2001. also at http://www.ists.dartmouth.edu/docs/cyber_a1.pdf (

 ISSN: 2582-6433

If a person is required to provide information or a certain document or to keep books of accounts and fails to do so, he is liable to pay a penalty.

The punishment for falsifying reports and papers ranges from one lakh to fifty thousand rupees.

The punishment for falsifying books of accounts or records is Rs. 5000. (Chapter 44)

3.10 APPELLATE TRIBUNAL

According to Section 48 of the Act, the Telecom Dispute Settlement and Appellate Body established under Section 14 of the Telecom Regulatory Authority of India Act, 1997 shall serve as the Information Technology Act, 2000's appellate tribunal. This change was made once the Finance Act of 2017 went into effect. [30]

All appeals from the controller's or adjudicating officer's orders will be heard by the tribunal, but if the decision is decided with the parties' permission, there will be no appeal. The tribunal will rule on the appeal as quickly as feasible, but no later than six months from the date of filing.

According to Section 62 of the Act, any individual who is dissatisfied with the tribunal's order or judgment may file an appeal with the High Court within 60 days of receiving such an order.

Powers The tribunal is not required to follow any rules of the Code of Civil Procedure, 1908, and must make decisions based on natural justice, according to Section 58 of the Act. [31]

It does, however, have the same powers as a civil court under the Code.

They are as follows:

- Call anyone and get their attendance.
- Examine anybody under oath.
- Request that papers be discovered or produced.
- Accept affidavit evidence.

[30] Information Technology Act, 2000,

 ISSN: 2582-6433

[31] Information Technology Act, 2000, S. 58

 ISSN: 2582-6433

- Witness interrogation
- Decisions should be reviewed.
- Any application will be rejected.

3.11 IMPORTANT PROVISIONS OF THE IT ACT,2000

The IT Act is essential in the Indian legal structure since it governs the whole investigation process for cybercrime.

The relevant portions are as follows: SECTION 43:

This section of the IT Act relates to those who commit cybercrimes, such as harming the victim's computer without the victim's consent.

If a computer is damaged without the owner's consent, in this case, the owner is completely entitled to a reimbursement for the whole damage. Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) directed Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Matharu, MD of Pune-based business Poona Auto Ancillaries, in Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018). [32]

In this case, a fraudster deposited Rs 80.10 lakh from Matharu's PNB, Pune account after the latter responded to a phishing email.

The complainant was requested to share the culpability since she reacted to the phishing email.

 ISSN: 2582-6433

However, the bank was determined to be irresponsible since no security checks were performed on bogus accounts established to deceive the Complainant.

Section 66:

[32] Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

 ISSN: 2582-6433

Applies to any dishonest or fraudulent behavior outlined in Section 43. In such cases, the penalty might be up to three years in prison or a fine of up to Rs. 5 lakhs. During the course of the inquiry in Kumar v. Whiteley (1991), the accused acquired illegal access to the Joint Academic Network (JANET) and removed, added, and modified files. [33]

According to investigations, Kumar had been signing on to a BSNL broadband Internet connection as if he were a legally authorized user and changing computer records relevant to customers' broadband Internet user accounts.

After discovering unlawful usage of broadband Internet on Kumar's PC, the CBI launched a cybercrime case against him and began investigations based on an anonymous allegation. Kumar's unlawful behavior also resulted in a Rs 38,248 loss for the subscribers.

The Additional Chief Metropolitan Magistrate condemned N G Arun Kumar.

The magistrate sentenced him to a year in jail and a Rs 5,000 fine under Sections 420 of the IPC and 66 of the IT Act.

Section 66B:

This section explains the penalty for receiving stolen communication devices or computers fraudulently and affirms a three-year jail term. A fine of up to Rs. 1 lakh may also be levied, depending on the gravity of the offense[34].

Section 66C:

 ISSN: 2582-6433

Is concerned with digital signatures, password hacking, and other types of identity theft. This clause carries a maximum sentence of three years in jail and a fine of one lakh rupees.

[33] http://www.thefreedictionary.com/obscene

[34] Information Technology Act, 2000, S. 66B

 ISSN: 2582-6433

Section 66D:

This section deals with cheating by personation using computer resources. If found guilty, the penalty might be imprisonment for up to three years and/or a fine of up to Rs 1 lakh.[35]

Section 66E:

Taking photographs of private regions, publishing, or transferring them without the agreement of the subject is a crime under this section. If found guilty, the penalties include imprisonmentfor up to three years and/or a fine of up to Rs 2 lakh.

Section 66F:

Cyberterrorism Acts A person guilty of a crime may face life imprisonment. A threat email was addressed to the Bombay Stock Exchange and the National Stock Exchange, challenging security forces to prevent a terror assault on both institutions. The offender was captured and charged under Section 66F of the Information Technology Act.

Section 67:

This covers the electronic publication of profanity. If convicted, the sentence may be up to five years in prison and a fine of up to Rs 10 lakh.

 ISSN: 2582-6433

AMENDMENTS TO IT ACT,2000

[35] Information Technology Act, 2000, S. 66C

 ISSN: 2582-6433

With the passage of time and technology, various adjustments to the Act were required to fulfill the demands of society, and thus it was revised.

2008 Amendment Section 66A of the Act was changed as a result of the revision in 2008.

This was the most contentious provision since it stipulated the penalty for delivering any insulting communications via technological means.

Any statement or material that incites hate or jeopardizes the country's integrity and security were outlawed.

However, it had not defined the term "offensive" or what comprises such communications, and as a result, many individuals were jailed on this basis.

The Supreme Court upheld this clause in the case of Shreya Singhal v. Union of India (2015).

Another change was made to Section 69A of the Act, which gave the government the authority to prohibit internet sites for national security and integrity.

Authorities or intermediaries may be able to monitor or decrypt personal information stored with them. Amendment Bill of 2015 the bill was introduced to alter the Act to defend the basic rights provided to people under the country's Constitution.

The measure attempted to amend Section 66A, which defines the penalty for delivering insulting material via electronic means.

The clause did not specify what constitutes offensive communications or what behaviors would constitute an offense.

It was also declared a violation of Article 19 by the Supreme Court in the case of Shreya Singhal.

2018 Guidelines for Information Technology Intermediaries (Amendment) Rules 46 In 2018, the government released rules for intermediaries to hold them accountable and regulate their operations.

Among these are:

 ISSN: 2582-6433

• The intermediaries were forced to post and change their privacy policies to protect citizens from unethical activities such as pornography, offensive communications and photos, hate messages, and so on.

 ISSN: 2582-6433

• They must submit the information to the government within 72 hours if it is requested for national security purposes.

• Every intermediary must appoint a "nodal person of contact" for 24-hour service.

• They must have technology that can aid in the reduction of illegal internet activity.

• End-to-end encryption is also broken if necessary to establish the origin of malicious communications. 2021 Rules on Information Technology (Intermediaries Guidelines and Digital Media Ethics Code)

In 2021, the Indian government created laws for intermediaries to follow.

The guidelines required intermediaries to do due diligence and establish a grievance officer. They also had to establish a Grievance Appellate Tribunal. Every customer complaint must be notified within 24 hours and handled within 15 days.

It also includes a "Code of Ethics" for those who write news and current events, which makes it contentious. Many people argue that the regulations restrict free speech and expression, as well as press freedom.

If there was a threat to the country's security or integrity, the intermediaries were also compelled to submit the information and details of a suspected user to the government.

 ISSN: 2582-6433

As a result, writ petitions challenging the rules were filed in several high courts.

The Bombay High Court recently delayed the two sections of the regulations relating to the Code of Ethics for digital media and publishers in the cases of Agij Promotion of Nineteenonea Media Pvt. Ltd. vs. Union of India (2021) and Nikhil Mangesg Wagle vs. Union of India (2021).[36]

[36] Nikhil Mangesg Wagle vs. Union of India (2021)

 ISSN: 2582-6433

3.12 LANDMARK JUDGEMENTS ON IT ACT,20003.12.1Union of India v. Shreya Singhal (2015)

• Facts In this case, two females were detained for making online remarks on the Mumbai shutdown following the death of a Shiv Sena political leader.

They were prosecuted under Section 66A for making abusive comments online. As a result, the Section's constitutional legitimacy was challenged in the Supreme Court, claiming that it violates Article 19 of the Constitution.

Issue Whether or whether Section 66A is constitutionally legitimate.

• Judgment In this instance, the Court recognized that the Section's language is confusing and imprecise, infringing on people's freedom of speech and expression. The entire Section was then overturned because it violated Article 19 of the Constitution. It was argued that the Section enabled police officers to arrest anyone they suspected of posting or messaging anything unpleasant.

They construed the phrase "offensive" differently in each case since it was not defined anywhere in the Act. This amounted to police misuse of authority and a threat to peace and harmony.

3.12.2 Union of India v. M/S Gujarat Petrosynthesis Ltd and Rajendra Prasad Yadav (2014) [37]

 ISSN: 2582-6433

• Facts In this case, the petitioners sought the appointment of a chairman to the Cyber Appellate

[37] http://www.infoplease.com/ipa/A0872842.htm

 ISSN: 2582-6433

Tribunal so that disputes could be resolved swiftly, and someone could keep an eye on CAT's operations. According to the answers, a chairman will be named soon.

• Issue Appointment of the Chairperson of the CAT

• Judgment The Court ordered the nomination of the chairman, which must be seen as an urgent matter by Section 53 of the Act.

3.12.3 Nakul Bajaj and Others v. Christian Louboutin SAS (2018)

• Facts In this instance, a shoe business filed a lawsuit seeking an injunction against thedefendants for utilizing its trademarks and insignia.

• Issue Is the "safe harbor" protection provided by Section 79 of the Act applies in this case?

• Judgment In this instance, the Court determined that the defendant was not an intermediary since their website operated as a platform for the supply of numerous items. It exploited third-party data and promoted companies to gain customers for them. The Court determined that e-commerce platforms are distinct from intermediaries and the rights provided to them under Section 79 of the Act. It ordered the intermediaries to exercise due diligence and not violate the trademark owner's rights. When dealing with any merchant or dealer, they must take efforts to ensure the authenticity and validity of the items. The Court further said that if the intermediaries act carelessly concerning

 ISSN: 2582-6433

IPR and engage in any type of abetment or instigation of unlawful or illegal activity, they would be exempt from the protection of safe harbor under Section 79 of the Act. Any active engagement in e-commerce would result in the same thing. It also alluded to the standards for intermediaries, which stipulate that no intermediary may infringe anyone's intellectual property rights when showing information on its website.[38]

[38] India Cyber Law and Cases, one of the largest Database of Cyber Law and Cases from India. Available at:

 ISSN: 2582-6433

What Causes Cyber Crime

Easy Access System

When using complicated technologies, protecting a system from data breaches is frequently difficult or impossible. Security can only be jeopardised when hackers have easy access to the system. Hackers with advanced skills can gain unauthorised access by defeating speech recognition, retinal scans, and access codes. They can simply trick the biometric system and get past the system's firewall.

Storing Data in a Small Space

One of the main causes of cyber attacks is the fact that computers are known to hold atremendous amount of data in a small amount of space. Cybercrime was developed following theinvention of computers. A little storage area makes it simpler for hackers to quickly grab dataand use it for their own gain. Therefore, it is advisable to separate the data and not keep it all on the system at once

Complex Codings

 ISSN: 2582-6433

One of the main causes of cyber attacks is the fact that computers are known to hold a tremendous amount of data in a small amount of space. Cybercrime was developed following the invention of computers. A little storage area makes it simpler for hackers to quickly grab data and use it for their own gain. Therefore, it is advisable to separate the data and not keep it all on the sys-

---

http://cybercases.blogspot.com/.

 ISSN: 2582-6433

tem at once.[39]

Negligence

Anything we overlook and think is simple to disregard might develop into a serious problem. The same principles apply to cybercrime. You might get into a lot of trouble if you don't take care to keep your system secure. A little carelessness on your part could open the door to cybercriminals. As a result, it's important to keep an eye on what's going on with your system.

Loss of Evidence

Hackers typically assault your system in phases, and it is simple to erase any proof of their initial intrusion. This strengthens their crime so that it cannot be found during a cybercrime investigation. Loss of evidence can become a significant factor in cybercrime, which might potentially disable your system and increase its susceptibility to attacks

LOOPHOLES IN IT ACT,2000

The Act includes provisions for digital signatures and electronic records, as well as the culpability of intermediaries, but it falls short in several other areas. They are as follows:

• There is no provision for data breaches. The Act's provisions exclusively mention obtaining and disseminating citizens' information and data. It makes no mention of anyone's obligation or

 ISSN: 2582-6433

accountability if it is compromised by any entity or government institution, nor does it give any recourse for the breach and release of data. It solely penalizes individuals or intermediaries who refuse to comply with the government in monitoring.

• There is no mention of privacy concerns. The Act fails to meet an individual's privacyconcerns. Any middleman might store an individual's sensitive personal data and provide it to the

[39] http://www.wsj.com/articles/SB12505366992133775

 ISSN: 2582-6433

government for monitoring. This constitutes an invasion of an individual's privacy. The creators have ignored this concern.

• Simple penalties Though the Act mentions specific offenses committed by electronic means, the penalties are substantially easier. To reduce such crimes, harsh consequences are required.

• Officers who are not properly trained One may easily avoid culpability with the assistance of money and influence. These crimes are sometimes not reported because of a societal stigma that police will not investigate such accusations. According to research, police personnel must be taught to manage cybercrime and have technical skills to promptly investigate a case and send it for prompt disposition.[40]

• There is no oversight of cybercrime. Cybercrime is rising at an alarming rate as technology advances. 50 The acts mentioned in the Act are restricted, but many forms of cybercrime are already prevalent, which, if not treated correctly and promptly, may pose a threat. These crimes do not directly impact any human body, but they might do so indirectly by exploiting any person's sensitive data. As a result, it is critical to control such offenses. This is where the Act falls short.

POSITIVE AND NEGATIVE ASPECTS OF IT ACT,2000

The following advantages are provided by this legislation:

• Because of the availability of this Act, several businesses may now perform e-commerce without concern. Until recently, our country's development of internet commerce was hampered chiefly by a lack of a legal framework to control business transactions conducted online.

• Corporations may now employ digital signatures to perform online transactions. The Act legally

 ISSN: 2582-6433

recognizes and sanctioned digital signatures.

[40] https://www.sans.org/security-resources/idfaq/distributed-denial-of-service-attack-toolstrinoo-and-wintrinoo/9/10

 ISSN: 2582-6433

• Furthermore, the Act allows business organizations to serve as Certification Authorities for the issue of Digital Signature Certificates under the Act. The Act makes no distinctions as to what legal organization may be recognized as a Certifying Authority, as long as the government's conditions are met.

• Furthermore, the Act allows businesses to electronically file any papers with any office, authority, body, or agency owned or managed by the proper government using the electronic form defined by that government.

• It also discusses the security considerations that are so important to the success of electronic transactions. The word secure digital signatures were established and accepted as part of the Act, and they must have been submitted to a system of security procedures. As a result, it is safe to infer that digital signatures are now secure and will play a significant role in the economy[41]

Evolution Of Laws Governing And Regulating Cyber-Crime In India Information Technology Act, 2000

The Information Technology Act of 2000 ("IT Act") and the IT Amendment Act of 2008 neither define cyber-crime, but the IT Act has the authority to address it because it contains provisions relating to cyber-offenses or crimes. The IT Act's definitions of terms like computer, computer network, computer resource, data, and information, among others, are crucial because cybercrime involves the targeting or assault of a computer or computer network[42]

The Information Technology Act, which was passed into law in 2000, primarily:
1-Recognises electronic records, electronic signatures as valid,

 ISSN: 2582-6433

2-Recognises electronic signatures, digital signatures,

[41] http://academickids.com/encyclopedia/index.php/Phreaking

[42] Ling Rich, The Mobile Connection: The Cell phone's impact on society, 2000

 ISSN: 2582-6433

3-Deals with computer related offences and other offences through electronic means, contraventions.

4-Constant critiques, evaluations, and the interpretation of some portions as harsh led to the IT Amendment Act, 2008 ("IT Amendment Act"), which took effect in 2008.

The IT Amendment Act brought in some notable changes such as:

1-Focus on data privacy,

2-Introduction of information security practices,
3-Definition of cybercafe,
4-Responsibility on companies to implement reasonable security practices to protect information from unauthorised access, damage, use, modification, disclosure, or impairment.

•Section 43 of the IT Act provides recourse in the form of compensation to an owner of a computer or computer system when a person or entity damages or destroys the computer or computer system belonging to such owner (civil liability for data theft).

•Section 43A of the IT Act provides compensation to a person, if the company dealing with or handling the person's sensitive personal information in its computer resource, fails to protect the said person's information.

 ISSN: 2582-6433

•Section 66 of the IT Act punishes the person who dishonestly or fraudulently commits the act referred to in Section 43, with imprisonment for a term extending to 3 years or with fine extending to Rs. 5 lakh or with both (criminal liability for data theft).

 ISSN: 2582-6433

•Section 66B, 66C & 66D of the IT Act punishes a person who:

•Section 66B:. A violation of this section results in the receiving or retention of a stolen computer resource by dishonest means.

•Section 66C: Using another person's electronic signature or password through dishonest or fraudulent means is punishable by up to three years in prison and a fine of Rs. 1 lakh.

•Section 66D: using a computer or communication device to impersonate someone else, punishable by up to three years in prison and a fine of Rs. 1 lakh.

•Section 66F: (a) threatens India's sovereignty, unity, integrity, or security;

(b) refuse entry to anyone with permission to use a computer or

(c) make an unauthorised attempt to enter or breach a computer,

(d) introduce a computer contaminant, such as a virus, Trojan, or malware, and cause someone's death or serious injury, or damage to or destruction of property, etc.; this offence carries a life sentence.[43]

POCSO Act, 2012

 ISSN: 2582-6433

A child may not be used for pornographic purposes, including for sexual pleasure online,according to the Protection of Children from Sexual Offenses Act of 2012 (the "POCSO Act"). Iffound guilty of the aforementioned offences, a person could face up to 5 years in prison, a maximum of 7 years in prison, and a fine. The POCSO Act also allows for up to three years in prison, a fine, or both as punishment for anyone who retains child-related pornographic material

[43] Information Technology Amendment Act, 2008, Act no 10 of 2009

 ISSN: 2582-6433

with the intent to profit from it.[44]

Indian Penal Code, 1860 (IPC)

Cyberfraud and crimes involving identity theft are also punishable under the IPC. Making a false document or false electronic record is prohibited under Sections 464 of the Indian Penal Code (IPC), 465 of the Forgery Punishment Act, 468 of the Forgery for the Purpose of Cheating Act, 469 of the Forgery for the Purpose of Harming Reputation Act, and Section 471 of the Forgery for the Purpose of Harming Reputation Act (Using as genuine a forged document or electronic record**).**[45]

 ISSN: 2582-6433

[44] http://blog.ipleaders.in/cyber-pornography-law-in-india-the-grey-law-decoded/

[45] Indian Penal Code, 1860.,

 ISSN: 2582-6433

CHAPTER-4
EVOLUTION OF
CYBER CRIME

4.1 INTRODUCTION

The first successful computer was developed in the 1950s, and today's users of palmtops and microchips would be astounded to learn that it was enormous and required the entire room to fit it, in addition to being prohibitively expensive to run. Few people had direct access to these computers and the technical know-how to operate them since the way these computers worked was difficult for most people to understand. For obvious reasons, computer technology was prohibitively expensive and out of reach for almost the entire population until IBM came into existence and introduced its stand-alone "personal computer" in 1981, allowing many people to benefit from the benefits of rapid data access and manipulation that, up until that point, had only been experienced by a select few. At the beginning of the twenty-first century in India, personal computers became more affordable and became a common commodityd. After World War II, the US Department of Defense created the initial version of the Internet with the goal of creating a network that could securely transfer information in the event of a tragedy or conflict. The first network was called ARPANET, and after the creation of the World Wide Web, Internet Protocol, and hypertext, the internet gained popularity all over the globe. The quantity and quality of information increased with the development of the Internet. However, nobody had any idea at the time what opportunities the internet would give tech-savvy crooks. In India, the government-owned Videsh Sanchar Nigam Limited launched internet services in 1995. In 1998, the government abolished VSNL's monopoly and allowed private operators to enter the market. At that time, 0.1% of India's population used the internet, but today, with 33.22% of the world's population using the internet, India has overtaken China as the second-largest internet user nation. In common law jurisdictions, the process of criminalising human behaviour deemed to be harmful to the public often develops gradually.Before undesired behaviours are labelled as

 ISSN: 2582-6433

"criminal," momentum built via problem identification and pressures from special interest groups can easily last decades. In some cases, this process is sped up by the occurrence of specific " catalyst events" that attract the public's and lawmakers' attention. In the year 1820, the first

 ISSN: 2582-6433

cybercrime was officially documented. That is not surprising given that the abacus, which is considered to be the earliest type of a computer, has been used in India, Japan, and China since 3500 B.C. However, it was Charles Babbage's analytical engine that marked the beginning of the era of modem computers. The loom was created in 1820 by French textile producer Joseph-Marie Jacquard. This tool made it possible to repeat a sequence of procedures forweaving unique fabrics. Employees at Jacquard became concerned that their traditional jobs and means of support were in jeopardy as a result. In order to stop Jacquard from using the new technology in the future, they committed acts of sabotage. The first cybercrime to be documentedis this. As corporations became more dependent on computerization and as catalytic eventinstances showed substantial vulnerabilities to computer crime violations, legislators became more and more concerned with the issue of computer crime in the 1980s. Criminals can now easily encrypt data that serves as proof of their crimes, store the data, and even transport it without worrying about being found out by law authorities. Due to the Internet's remarkable influence, a computer crime scene can now extend from the victim's physical location (such as their home computer) to any other location on the planet, significantly complicating criminal investigation operations. In practise, advances in computer technology have fundamentally changed the landscape of criminal justice, leading resourceful and opportunistic criminals to consciously use computers to carry out their illegal activities in both situations where the victim'scomputer or computer system serves as the target of the act or as the instrument of the crime.And as was already mentioned, the development of new computer technology facilitates cybercrime when the use of a computer is just incidental to the crime; for example, when the computer is used to store and safeguard data that links the perpetrator to criminal activity. The fact that the criminal relies heavily on the lack of technological expertise of law enforcement to successfully commit the crimes and escape unnoticed is a commonality among these types of crimes. Based on the actual evidence that has been made available and the self-assessed competency of investigators in this sector, computer criminals would have ample reason to feel some confidence in their prospects to avoid discovery of their crimes. As we move closer to the twenty-first century, it will become clear that technological advancements have paved the wayfor all of the people who use computers today to enjoy a variety of new and wonderful conveniences in their daily lives, including the ability to learn, shop, entertain, and gain an

 ISSN: 2582-6433

understanding of business strategies and work processes. Rapid advancements in computer technology have permanently altered the way we conduct our daily lives.[46]

4.2INDIAN PENAL CODE,1860

If the IT Act is insufficient to cover certain cyber offenses, law enforcement agencies can use the IPC sections listed below:

Section 292:

Originally intended to handle the selling of obscene materials, this section has developed to encompass a variety of cyber offenses as well. This section also governs how obscene content or sexually explicit activities or exploits of youngsters are published or disseminated online.

Such crimes are punishable by imprisonment and penalties of up to 2 years and Rs. 2000, respectively. For repeat (second-time) offenders, the punishment for any of the aforementioned offenses may be up to five years in jail and a fine of up to Rs. 5000.

Section 354C:

defines cybercrime as "taking or disseminating images of a woman's intimate parts or acts without her consent." Voyeurism is handled specifically in this section since it considers observing a

 ISSN: 2582-6433

woman's sexual activity as a crime. In the absence of the fundamental features of thisprovision, [47]

Sections 292:

[46] Lance James, "Phishing Exposed", Elsevier 2005. also at https://en.wikipedia.org/wiki/Phishing

[47] Indian Penal Code (Act No. 45 of Year 1860)

 ISSN: 2582-6433

of the IPC and 66E of the IT Act are wide enough to cover analogous offenses. Depending on the offense, first-time offenders may face up to three years in jail, while repeat offenders may face up to seven years in prison. [48]

Section 354D:

This chapter describes and punishes stalking, including physical and cyberstalking.

Cyber-stalking is the tracking of a woman by technological means, such as the internet or email, or the effort to contact her despite her reluctance. This offense is punishable by up to 3 years in jail for the first offense and up to 5 years in prison for the second offense, as well as a fine in both circumstances. [49]

In the matter of Kalindi Charan Lenka v. State of Odisha(2017), a victim got a series of vulgar texts from an unknown number, which harmed her reputation. The accused reportedly sent emails to the victim and set up a bogus Facebook account with modified photographs of her. As a result, the accused was declared prima facie guilty of cyberstalking on several offenses under the IT Act and Section 354D of the IPC by the High Court.

Section 379: The punishment for theft under this section can be up to three years in prison in addition to a fine. Because many cybercrimes include hijacked electronic devices, stolen data, or stolen computers, the IPC Section comes into play. [50]

Section 420: This section discusses cheating and deception in the conveyance of property. Under

 ISSN: 2582-6433

this clause, cybercriminals who commit offenses such as building false websites and cyber fraud face a seven-year jail sentence as well as a fine. This part of the IPC deals with offenses

[48] Indian Penal Code (Act No. 45 of Year 1860) S 292

[49] Indian Penal Code (Act No. 45 of Year 1860)S 354D

[50] Indian Penal Code (Act No. 45 of Year 1860) S 379

 ISSN: 2582-6433

involving password theft for fraud or the development of bogus websites.

Section 463: This section deals with electronically fabricating papers or records. Under this clause, spoofing emails is punished by up to 7 years in jail and/or a fine.

Section 465: This section usually deals with the penalty for forgery. Offenses such as email spoofing and the creation of fake papers in cyberspace are dealt with and punished with imprisonment of up to two years, or both, under this clause. [51]

In Anil Kumar Srivastava v. Addl Director, MHFW (2005), the petitioner faked the AD's signature and then filed a complaint alleging false charges against the same person. Because the petitioner also sought to pass it off as a real document, the Court found him responsible under Sections 465 and 471 of the IPC. In addition to the regulations listed above, there are many additional parts of the IT Act and the Indian Penal Code that deal with cyber offenses.

Despite the existence of cybercrime legislation, the rate of cybercrime continues to rise dramatically.

According to reports, cybercrime in India would climb by 11.8% by 2020, despite just 50,000 incidents being recorded.

Cybercrime is one of the most difficult crimes for police to investigate because of several problems such as underreporting, the jurisdiction of crime, public ignorance, and the increasing expenses of investigation due to technology.

 ISSN: 2582-6433

Due to the overlap between the provisions of the IPC and the IT Act, certain offenses may wind up being bailable under the IPC but not under the IT Act and vice versa, or compoundable under the IPC but not under the IT Act and vice versa.

[51] Indian Penal Code (Act No. 45 of Year 1860) S 465

 ISSN: 2582-6433

For example, if the behavior involves hacking or data theft, charges under sections 43 and 66 of the IT Act are both bailable and compoundable, but offenses under Section 378 of the IPC are neither bailable nor compoundable. [52]

Furthermore, if the offense was receiving stolen goods, the offense under Section 66B of the IT Act was bailable, but the violation under Section 411 of the IPC was not.

Similarly, under sections 66C and 66D of the IT Act, the offenses of identity theft and cheating by personation are compoundable and bailable, whereas the offenses under Sections 463, 465, and 468 of the IPC are not compoundable and the offenses under Sections 468 and 420 of theIPC are not bailable.

The Bombay High Court examined the problem of non-bailable and non-compoundable offenses under Sections 408 and 420 of the IPC in conflict with those under Sections 43, 65, and 66 of the IT Act, which is bailable and compoundable, in **Gagan Harsh Sharma v. The State of Maharashtra (2018).**[53]

4.3INFORMATION TECHNOLOGY RULES

The IT Rules address several elements of data collection, transfer, and processing, including the following:

 ISSN: 2582-6433

• The 2011 Rules on Information Technology (Reasonable Security Practices and Procedures and

[52] Preliminary Consultation Paper On Mobile Phone Theft, Telecom Regulatory Authority Of India, New Delhi, January, 2004. also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf

[53] Gagan Harsh Sharma v. The State of Maharashtra (2018)

 ISSN: 2582-6433

Sensitive Personal Data or Information)

These laws require companies that possess sensitive personal information about persons to adhere to specific security requirements.

• The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: These regulations govern the role of intermediaries, especially social media intermediaries, in preventing the transmission of dangerous information on the intruder to protect the safety of consumers' data online

• The Rules for Information Technology (Guidelines for Cyber Cafes), 2011:

These recommendations require cybercafés to register with an oorganizationnisation and keep a record of users' names and internet usage.

• The 2011 Information Technology (Electronic Service Delivery) Regulations: Essentially, these laws provide the government the ability to stipulate the electronic delivery of certain services, such as applications, and certificate-licensed licenses.

• The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (the CERT-In Rules): The CERT-In regulations provide for the 56 operation of CERT-In in a variety of ways.

A 24-hour Incident response helpdesk must be operational at all times, according to CERT-In

 ISSN: 2582-6433

rule 12.

If an individual, organization, or company is suffering a cybersecurity event, they can report it to Cert-In.

The Rules include an Annexure that lists certain Incidents that must be reported to Cert-In right

 ISSN: 2582-6433

away.[54]

4.4EMERGING TRENDS & CHALLENGES IN CYBER LAW

With the rising use of digital technology, numerous new themes are anticipated to affect cyber law.

The various emerging trends include

A. CHALLENGES IN MOBILE LAWS

B. LEGAL ISSUES OF CYBER SECURITY

C. CLOUD COMPUTING & LAW

D. SOCIAL MEDIA & LEGAL PROBLEMS

E. SPAM LAWS

 ISSN: 2582-6433

A. CHALLENGES IN MOBILE LAWS

There are many activities taking place in the mobile ecosystem nowadays. The increasing competition has introduced new models of mobile phones, personal digital assistors (pda), tablets and other communication devices in the global market. In many jurisdictions throughout the world, where the use of mobile devices for input and output activities is growing daily, there are

[54] Middle East E-mail Flooding and Denial of Service (DoS) Attacks" – National Infrastructure Protection C enter – October 26, 2000 and also at http://www.nipc.gov/warnings/assessments/2000/00-057.htm and https://www.sans.org/reading-room/whitepapers/threats/conventional-terrorismthe-cyberassault-931

 ISSN: 2582-6433

no specific regulations regarding the use of these new communication devices and mobile platforms. The need to address the legal issues arising from the usage of mobile devices and assure mobile privacy and protection is growing as a result of the rise in mobile crimes.[55]

B. LEGAL ISSUES OF CYBER SECURITY

The requirement to adopt suitable legal frameworks for preserving, promoting, and developing cyber security is the other new trend in cyber law. Increasingly frequent cyber security incidents and network attacks result in breaches of cyber security, which could have a significant negative effect on the country. However, the challenge before a lawmaker is not only to develop appropriate legal regimes enabling protection and preservation of cyber security, but also toinstill a culture of cyber security amongst the net users..

C.CLOUD COMPUTING AND LAW

The world is shifting to cloud computing as internet technology develops. The cloud computing presents new difficulties for legislators. The distinct challenges may include data security, data privacy, jurisdiction and other legal issues. Legislators and other stakeholders in the cyberspace would be under pressure to create a legal framework that would be beneficial to the sector and allow for efficient remedies in the event of cloud computing incidents.[56]

1. SOCIAL MEDIA & LEGAL PROBLEMS

 ISSN: 2582-6433

In recent years, social media has started to have an impact on society and the law, posing serious

[55] Article by Praveen Dalal, Cybercrime and cyber terrorism: Preventive defence for cyberspace violations, Computer
Crime Research Center, March 10, 2006.

[56] See "Is Cyber-Terrorism the New Normal?" Available at http://www.wired.com/insights/2015/01/is-cyberterrorism-the-new-normal/

 ISSN: 2582-6433

problems and difficulties. According to a recent study, social networking sites are to blame for a number of issues. Since social media sites are a target for law enforcement and intelligence organisations, they are the preferred location for any data. Inappropriate use of social media is a catalyst for crimes including identity theft, cyberstalking, and other types of harassment. Despite the efforts of key stakeholders, the privacy in social media will be severely eroded. The difficulty for online lawmakers would be to effectively control social media abuse and offer compensation to victims of social media crimes. The difficulty for online lawmakers would be to effectively control social media abuse and offer compensation to victims of social media crimes. Social media lawsuits involving a connection or nexus to social media output are also likely to rise. Thenumber of lawsuits involving defamation and matrimonial disputes is steadily rising, and withthe data and information stored on social media networking sites, there is a growing trend of several more lawsuits in the upcoming years

2. SPAM LAWS

Spam has significantly increased in both emails and mobile devices. Spam production hasalready taken off in many nations. Spammers utilise cutting-edge techniques to target online consumers as the number of mobile and internet users rises. Therefore, it is essential to have strong legislative provisions to combat the spam threat.

CASE STUDIES

 ISSN: 2582-6433

1.Two managers of Chennai based Radiant Software a Computer Education Company were arrested for an alleged violation of the licensing terms of Software. The top management team had to obtain anticipatory bail to avoid arrests until a compromise was worked out.

 ISSN: 2582-6433

2. Napster, a very successful E-Venture was hauled to the Court and beaten to death for having caused violation of Copyright of music companies. Despite willing customers and working technology, the business of the Company had to be shelved under an enormous loss to the promoters.

3. There are many websites in India which could be held to be infringing the Patent rights of somebody abroad and asked to shut down or pay compensation putting an end to their entrepreneurial dreams.These are a few of the trends in cyber law that have been identified through a review of new cyber law case law. With the speed at which technology is developing,it may be impossible to stop any new technological trend that might have an impact on cyberlaw, either directly or indirectly. In the jurisprudence of cyber law, a number of intriguing and significant challenging risks can emerge.

 ISSN: 2582-6433

CHAPTER-5

INTERNATIONAL PERSPECTIVE OF CYBER LAW

5.1 INTRODUCTION

Cyber crime is becoming ever more serious. The 2002 Computer Crime and Security Survey results reveal an upward trend that highlights the need for a prompt review of current strategies to combat this novel phenomenon in the information age. In this essay, we give a general overview of cybercrime and discuss how it is addressed internationally. We examine howvarious nations are currently combating cybercrime, using organisational, technological, andlegal means, and we make four recommendations for policymakers, legislators, intelligence agencies, and law enforcement. and researchers to combat cybercrime.[57]

Within Country Strategy

The U.S. Congress has crafted new regulations to control online behaviour in order to safeguard the interests of internet firms. The United States has enacted a variety of laws against cybercrime, including the "National Infrastructure Protection Act of 1996," the "Cyberspace Electronic Security Act of 1999," and the "Patriot Act of 2001," in addition to passing the first digital signature law in the history of the world. The FBI, National Infrastructure Protection Center, National White Collar Center, Computer Hacking and Intellectual Property Unit of the Doj, and other organisations have also been established in the United States to combat cybercrime. The FBI

 ISSN: 2582-6433

has created Carnivore and established specialised technical groups.

The Data Protection Act of 1984 and the Computer Misuse Act of 1990 are two Acts that have been passed by the British parliament that deal with cybercrime. The first one deals with the actual acquisition and use of personal data, while the second outlines the policies, processes, and

[57] http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf

 ISSN: 2582-6433

sanctions related to breaking computer security. The British government has implemented screening and rating technology to shield manors from objectionable content on the Web. [58]

In 2001, the Criminal Law Amendment Act, which consists of two sections, was passed by the Canadian parliament. The terms unauthorised access to a computer system and transmission interception are defined in the first section. The second portion makes it illegal to actually destroy, change, or interrupt data.

The Kenya Communications (Amendment) Act was approved by the Kenyan legislature and became a law on January 2 after being signed by the president. Sections 83 W to Z and 84 A to F of the Act include provisions on cybercrime, including: unauthorised access to computer data, access with the intent to commit crimes, unauthorised access to and interception of computer services, unauthorised modification of computer material, damage to or denial of access to computer system, unauthorised disclosure of passwords, unlawful possession of devices and data, electronic fraud, tampering with computer source documents, and publishing of offensive material.

In Norway, a Bill on a New Criminal Law (2008-2009) introduced a provision on identity theft in 202 that reads as follows: "With a fine or imprisonment not exceeding 2 years shall whoever be punished, that without authority possesses of a means of identity of another, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of a) procuring an economic advantage shall be punished." On May 28, the Norwegian Parliament (Stortinget) adopted the New Penal Code, which contains a number of laws pertaining to cybercrime. [59]

British law on cybercrime

The Computer Misuse Act 1990, Part 5 sections 35 to 38, are amended according to Police and Justice Act 2006 Chapter 48. The updated rules went into effect on October 1st, 2008.

Indian Republic's cyber law

 ISSN: 2582-6433

[58] http://timesofindia.indiatimes.com/city/delhi/DU-law-student-charged-withcyberstalking/articleshow/8917937.cms

[59] //www.thehindu.com/news/national/curb-websites-circulating-pornography-sayscji/article425172.ece

 ISSN: 2582-6433

The Indian government first revealed proposals for a comprehensive cybercrime law in 2003.

66. Computer system hacking.

I A hacker is anyone who destroys, deletes, or modifies any information stored in a computer resource, diminishes its value or utility, or otherwise negatively affects it using any method with the intent to cause, or knowing that he is likely to cause, wrongful loss or damage to the general public or any person.

(ii) Anyone found guilty of hacking faces a sentence of up to three years in prison, a fine of up to two.[60]

5.2 CYBER LAW IN PEOPLE'S REPUBLIC OF CHINA

Many cybercrime issues are covered in China's laws and regulations that deal with crimes related to the Internet. The Public Security Bureau (PSB), which is in charge of internal security, and the Ministry of State Security (MSS), which is in charge of external security, are the two most significant organisations in charge of internal and external security. The "Computer Information Network and Internet Security, Protection and Management Regulations," approved by the State Council on December 11, 1997, formally codify the duties of the Public Security Bureau (PSB), and published December 30, 1997.

Article 285 says whoever violates state regulations and intrudes into computer systems within formation concerning state affairs, construction of defense facilities, and sophisticated science and technology is be sentenced to no longer than three years of fixed-term detention or imprisonment.

According to Article 286, whoever violates state laws by deleting changes, advertisements, or interference in computer information systems, leading to abnormal operations of the systems and

 ISSN: 2582-6433

serious consequences, shall receive a sentence of not less than five years' fixed-term

[60] http://www.haltabuse.org/resources/laws/india.shtml

 ISSN: 2582-6433

imprisonment or criminal detention, or not less than five years' fixed-term imprisonment when the consequences are particularly severe.

According to the sentence above, anyone who breaks state law by deleting, altering, or adding data or application programmes that have been installed in, processed by, or transmitted by computer systems and causes serious consequences faces punishment.

According to the first paragraph, whoever knowingly develops and disseminates computer viruses and other programmes that obstruct the regular operation of the computer system and have serious consequences will be punished.

According to Article 287, anyone found guilty of using a computer to commit financial fraud, theft, corruption, misappropriation of public funds, theft of state secrets, or any other crime will be sentenced in accordance with this law's applicable rules.[61]

5.3 CYBER LAW IN UNITED STATES OF AMERICA

President Barack Obama has tasked the National Security and Homeland Security Advisors with reviewing the government's cyber security strategy, programmes, and initiatives, including any new laws to combat cybercrime.

On February 7, 2010, US Vice President Joe Biden spoke at the 45th Munich Conference on Security Policy. He focused on the need to address cyber-security and terrorism among other issues.

5.4 APPLICATION OF CYBER LAW IN PRESENT DAY SOCIETY

 ISSN: 2582-6433

We are living in highly digitalized world.

[61] Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Also available at https://www.sans.org/reading-room/whitepapers/threats/conventionalterrorismthe-cyber-assault-931

 ISSN: 2582-6433

1- All companies depend upon their computer networks and keep their valuable data in electronic form.

2-Government forms, such as tax returns and company law forms, can now be completed electronically.

3-Consumers are increasingly using credit cards for shopping.

4- The majority of people communicate via email, mobile devices, and SMS messages.

5-Even in "non-cyber crime" cases, important evidence is found in computers/ cell phones .

6-Since it touches all the aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace therefore Cyber law is extremely important.

lakh rupees, or a combination of the two**.**

Recent change with respect to cyber law

The advent of the internet in the 1960s marked a turning point in history. Despite the fact that the internet was initially created to serve military purposes, we had no idea how quickly it would expand and come to play a crucial role in our daily lives. More than ever before, we are connected to the internet. Due to the internet's rapid growth, businesses have been able to move their operations online.[62]

 ISSN: 2582-6433

We can order anything from the comfort of our homes and have it delivered to our doorstep, including clothing, food, bags, equipment, electrical goods, and furniture. The internet has made life easier for us. However, there is always a drawback to everything good.. The growth in occurrences of cyber-crime has been attributed to the advent and development of the internet, as well as the accompanying increase in the number of people online.

[62] India Cyber Law and Cases, one of the largest Database of Cyber Law and Cases from India. Available at: http://cybercases.blogspot.com/.

 ISSN: 2582-6433

CHAPTER-6

CONCLUSIONS, SUGGESSTIONS AND FINDINGS

6.1 FINDING

Research study, findings and conclusions to the problems of cyber law especially IT Act 2000 is presented in this chapter. Similarly, the researcher has made certain suggestions based on observations in the light of the conclusions for strengthening the effectiveness of IT Act 2000. These conclusions and suggestions will definitely increase the use of e-commerce and decrease the number of cyber crimes.

Findings

By reviewing the data analysis, interpretation and onsite observations the researcher observed the following findings

• It is observed that, majority of the respondents (69.3%) were hesitant to lodge a complaint about the dispute regarding cyber crime. There are various reasons such as people are worried about their reputation, people don't have time for lodging the complaint regarding cyber crime, people are not sure about whether they will get justice, it requires more time to decide the case due to technicality and people think that the goodwill of the business in the market maydiminish. According to category of respondents such as gender, profession, age wise etc, stated that all the reasons for the hesitation are supporting that people are hesitatingtoapproachthe courtincaseofcybercrimes.

 ISSN: 2582-6433

• It is found that majority of the respondent said that the time required to get the justice for the case registered undo- IT Act 2000 is less than one year and one to two years. Average time to get justice regarding cyber crime is 1.82, approximately two years. By observing actual cyber cases filed in the court of law and considering the pending cases the average time required is in between two to three years.

 ISSN: 2582-6433

• It is observed that there are various reasons such as poor enforcement of IT Act, peoples are not sure about security, poor knowledge about how to use E-commerce, non availability of infrastructure facility (i.e. Computer machine, internet connection, etc) and lack of awareness of Act 2000 are affecting on the uses of e-commerce instead of enactment of IT Act 2000. According to category of respondents such as gender, profession and age wise etc, stated that all the reasons for not using e-commerce widely even enactment of IT Act.

• It is observed that the average time for getting justice for the cases registered under IT Act 2000 is 1.82 year along with Standard Deviation time is 1.012. Where as Mean time for getting justice for the cases registered under non IT related matter (General) is 2.58 years and Standard Deviation time is 1.329.[63]

• It is observed that there are eight parameters which are affecting the speedy disposal of the matters. Theses parameters are lodging early complaint, role of police as investigation authority, role of prosecutor, role of advocate of accused, role of Judicial Officer, appointment of Special tribunal, non availability of number of Cyber Forensic Labs in comparison with population, and no proper machinery for implementation of the Cyber law. According to category, respondents stated that all the parameters are affecting the speedy disposal of the matters registered under IT Act.

• During the visit at Cyber cell of commissioner office at Mumbai and Pune it is observed that the number of staff appointed at the cell is very less as compare to the registration of the cyber cases. While for other districts like Kolhapur, Satara, Sangli there is no such cyber cell.

• It is found that the staffs in the cyber cell of Police commissioner office are not much qualified where technicality is concerned. They have been given the training of how to investigate the cyber crime but still due to shortfall in technicality they are not comfortable about the cyber crime investigation

• It is observed that the software and hardware available in the Cyber cell are not up to the mark so the ssaff of Cyber cell has become handicapped in case of emergency investigation. They

 ISSN: 2582-6433

[63] Preliminary Consultation Paper On Mobile Phone Theft, Telecom Regulatory Authority Of India, New Delhi, January, 2004. p. 4-5 also available online at http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf

 ISSN: 2582-6433

need to depend upon the cyber forensic lab which is time consuming, and during this case evidence may get tampered with the offender.[64]

• Numbers of Cyber forensic labs are very less as compared to the number of Cyber Crimes taking place in the country.

• There is dependency on Police of Cyber cell that until the forensic report is not received they are not able to take further step of making charge sheet and approaching the concerned court of law. It is observed that there is much delay in this step. So after making complaint in the Police the case may take few months for registration of case in the court oflaw.

• It is observed that as Police is under state government authority and their service is transferable, the transfer of officer may break link of cases and the new place of transfer may or may not be related to cyber crimes. In this regard even though the willingness of the officer does nothing if he is transferred from any another department to cyber cell or vice versa.

• As U/S 48 of IT Act Cyber Appellate tribunal will consider the cases registered under IT Act but there is no such court existing till date. So it is affecting on getting the justice regardingcyber crime.

• It is found that Cyber law practitioners as an Advocate are less in number and those who are doing this "practice they are doing by accidently i.e. when a relevant brief is there the lawyer will buy the IT Act book for it and he will study the case as well as related provisions. It shows that what ever the justice the people are getting might be biased or offender may escape due to non availability of evidence beyond doubt.

• Security for the e-commerce is not up to the mark, VPN-SSL (Virtual Private Network - Secure Socket Layer) technology is not being used by every e-commerce transactions.

• The use of digital signature in the country is very less or negligible even though the lack of awareness of digital signature, they do not know how to take digital signature. Getting digital signature is a complex and expensive procedure and its use for common man is approximately nil.

• It is observed that unsecured Wi Fi connections and networks invite the hackers and terrorists to do their job very easily. It is found that two major terror incidents including the Ahmedabad

 ISSN: 2582-6433

[64]Jim Boulden, Mobiles used in high-tech terror, CNN, Apr 4, 2004 http://www.cnn.com/2004/TECH/04/04/mobile.terror/index.html.

 ISSN: 2582-6433

serial blasts and Mumbai attacks, where the terrorists had used Internet and communication networks in their operations. Unsecured networks and unprotected IP address are misused by terror outfits and other cyber criminals.

• It is observed that because of jurisdiction problem, criminal sitting seating at out of country can do any offence and no government can arrest the offender if there is no such treaty of exchange of criminals in between these countries.

• As International law is considered as a weak law, the crimes related to cyber space also some what related to international category because the offender may be in or out of country, if it is out of country and doing against the sovereignty of the nation it is very difficulty to arrest the offender and punish accordingly.

6.2 CONCLUSIONS

Based on the observations, analysis and statistical techniques the researcher made following conclusions:

The study concludes that people are hesitant to report cybercrime for a variety of reasons, including the possibility that their reputation may be ruined, the lack of time to file a complaint about the dispute involving cybercrime, the length of time needed to resolve the case because of legal technicalities, and the uncertainty that they would receive justice in cases of grave severity. Nevertheless, people do have faith in the justice system in these situations. It also concludes that all responder categories have endorsed using a court of law to address cybercrimes for the reasons stated above. A handful of the classifications and findings discussed here are, Experts doubt that there would be justice in cases of cybercrime. Due to a lack of knowledge of cyber law, the judiciary, police, and advocates are more concerned with protecting their reputations in cybercrime cases than are businesspeople and specialists. Because they are at the pinnacle of their careers, respondents between the ages of 37 and 54 are more concerned about their reputation.

• It is concluded that the time required to get justice in case of cyber crime is less than three years,

 ISSN: 2582-6433

exceptionally it may go above three years.

 ISSN: 2582-6433

• It is concluded that there are four reasons why people are not using e- commerce widely instead of enactment of IT Act. Those reasons are a poor enforcement of IT Act 2000, People are not sure about security, Poor knowledge about how to use e-commerce., Non availability of infra-structure facility (i.e. Computer machine, internet connection, etc) and Lack of awareness of IT Act 2000.[65]

The conclusion is that cases filed under the IT Act 2000 require less time to be decided than cases registered under other categories (general matters unrelated to IT). It doesn't take long to resolve the cyber case after the expert opinion and forensic lab report are obtained.
It has been determined that eight factors influence how quickly an IT Act-registered case is resolved. The primary criterion is the timely filing of a complaint. The roles of four individuals are influencing how quickly a cyber case is resolved: the police as the investigating authority; the prosecutor; the accused's counsel; and the judicial officer. Three other factors are also having an impact: the establishment of a Special Tribunal; the lack of cyber forensic labs; and the lack of equipment necessary to carry out cyber law enforcement.

6.3 SUGGESTIONS

6.3.1 HESITATION TO APPROACH COURT OF LAW IN CASE OF CYBER CRIMES

• By using parameters of speedy disposal mentioned in this research; time for the disposal of the matter should be reduced to the months instead of years so that people will not hesitate to approach court of law in case of cyber crimes. If it happens truly for cyber cases then the people will not hesitate to approach the court of law.

• People are not having time to approach court of law in case of cyber cases then Online Dispute

 ISSN: 2582-6433

Resolution System (ODRS) should be applied so that the attendance can be disallowed for the victim.. He can approach ODRS from any remote place. Here victim can get relief without going

[65] Information Technology Amendment Act 2008, Act 10of 2009

 ISSN: 2582-6433

to the court of law & lot of time will be saved. This system is applied for the civil cases and not for criminal cases.

6.3.2 TIME OF DISPOSAL FOR CYBER CRIME

• To reduce the time of disposal of cyber crime it is needed to have separate tribunal for the cyber cases.

• There should be separate cyber cell office with trained staff and well equipped office with latest software and hardware at every district police commissioner office. Region wise Cyber forensic labs should be present.

6.3.3 REASONS FOR NOT USING E-COMMERCE WIDELY INSTEAD OF ENACT- MENT OF IT

• Procedure of getting digital signature needs to be made simple because many people don't know the procedure to acquire digital signature.

- Fees which is mentioned in sec of 35 (2) of IT Act is not exceeding twenty-five thousand rupees needs to be reduced up to Rs. 5000/- for getting digital signature

- Section 35(1) of the IT Act says that an application needs to be submitted to the Certifying Authority for the digital signature certificate; the provision should be such that an application can be submitted to the Collector Office of each district of India. Government will take adequate care to send that application to the Certifying Authority.

- Free training should be given by the Certifying Authority to die public in general for aware- ness of the digital signature.

• Government should make the infrastructure facility available at remote places to increase e-commerce.

 ISSN: 2582-6433

- Government should arrange seminars at district level for training on how to use e-commerce and make people aware about the IT Act 2000.
- VPN-SSL technology should be made compulsory for the traders to trade their business through e-commerce.

 ISSN: 2582-6433

• Enforcement of IT Act should be in such way by the authority so that people should feel secure while using e-commerce transaction.

6.3.4 PARAMETERS FOR SPEEDY DISPOSAL FOR THE MATTER REGISTERED UNDER IT ACT.

• Cyber Appellate Tribunal which is mentioned in U/S 48 of IT Act 2000 which is in black and white it needs to be implemented. At least in the Special Cyber Appellate tribunal needs to be established minimum at capital city of state on the experimental basis.

• The presiding officer working at this cyber Appellate tribunal must possess minimum bachelor degree of computer science or engineering.

• The investigating authority, like cyber cell of Police Commissioner office and Cyber forensic Labs should be equipped with latest software like Header analyzing software, Advanced Search software, Steganography software, Password cracking tools, Disc imaging tools, image recovery tools and hardware like Powerful computer systems with standard peripherals like CD-ROM drives and CD-writers, desktop and laser printers, scanners, Card readers for examination of various kinds of cards that store data used for authentication and communication e.g. SMART cards, Micro Drives, GSM SIM cards etc. and latest software required for investigation.

• The number of cyber forensic labs need to be increased on the basis of population & use of network in particular area.

• Implementation of IT Act by the authority should be in such a way that people will not hesitate to approach the court of law, so that people will lodge the complaint early regarding cyber crime and it will help to resolve the case early.

• The subject of IT Act 2000 should be made compulsory in the syllabus of LL.B. so that the up coming lawyers will be aware about the cyber law. This will help both the prosecutor as well as the advocate of accused.

• The number of Forensic labs should be increased by considering cyber crime cases. The latest

ISSN: 2582-6433

software should be equipped in the cyber forensic labs so that the forensic report can be sent

 ISSN: 2582-6433

back to the police authority as early as possible. So that police can file charge sheet in the concerned court of law according to the jurisdiction.

Following are some of the software tools that need to be available in the lab.

- Byte Back- Data recovery and computer investigation program software.

- Digit- Digital information and gathering and investigation technologies.

- Drive spy- It is a forensic dos shell. It is designed to evaluate and extend the capabilities of dos to meet forensic needs.

- Encase- It is capable of making forensic quality, recording of data stored on pc's and of recovering some insecurely deleted data.

- Forensic Tool Kit (FTK) - Access data product.

- Gdisk- For Re-portioning purpose.

- Ghost- Create a new record from old file.

- Drive works- Reuse of drives.

- Linux DD (SMART)- Self monitoring, analysis and reporting technology.

- Hash Keeper- Password manager or create.

- Ilook (LEOs only)- Used to acquire and analyse digital media.

- Maresware- Date analysis and electronic data security.

- Microsoft Technet- Is a Microsoft program and resource for technical information news and events for IT.

- Password Recovery Toolkit (PRTK)- Password recovery purposes.

- Safeback- for the purpose of maintaining file..

- Thumbs Plus- For graphics maintaining purpose.

- Drive Image- Disk image

 ISSN: 2582-6433

6.3.5 GENERAL SUGGESTIONS

 ISSN: 2582-6433

• There should be provision in cyber law throughout the entire world for creation of e-mail account. The provision should be like the procedure of getting phone number. So that e-mail can be treated as evidence. It will help in for reducing the number of cyber crimes.

• The Police officers appointed at the cyber cell of commissioner office should possess at least bachelor's degree in computer science or engineering along with latest training about how to investigate the cyber crimes.

• Cyber space is available across the whole world. So the problem of jurisdiction becomes very complex. This problem can be solved by all the nations together. There should be one law throughout the world for.

6.4 FOR CYBER LAW INSTEAD OF CRIMINAL PROCEDURE COURT (CR. P. C).

there should be separate procedural law which the whole world should accept and recognize.

Scope for further Research

• Further Research can be done on the topic of Nigerian Fraud which is not in the ambit of this research.

• Research can be done to solve the problem of Jurisdiction in case of Cyber Crime, because the area is not binding to the internet, any one sitting at any place, can commit cyber crime and the nation out of their territory can not do much cyber crimes.Government should make public announcement about Nigerian Fraud. So that the innocent citizens of India will not be cheated by the criminals.

• Online Dispute Resolution System can be studied more critically; additional parameters can be suggested to establish this ODRS system world wide.

 ISSN: 2582-6433

• A common law which is uniformly implemented through out the world should be developed. A research can be done in this regard.

CONCLUDING REMARK:

 ISSN: 2582-6433

It is concluded that, Cyber Law is not effectively implemented and hence the main objective of enactment of IT Act 2000 is not achieved. If the suggestions given by the researcher are properly incorporated; the Cyber Law will be implemented more effectively.

 ISSN: 2582-6433

Biblography

Information Technology Amendment Act 2008, Act 10of 2009

Preliminary Consultation Paper On Mobile Phone Theft, Telecom Regulatory Authority Of India, New Delhi, January, 2004. p. 4-5 also available online a http://trai.gov.in/WriteReaddata/ConsultationPaper/Document/mobile%20theft%20rev.1.pdf

Jim Boulden, Mobiles used in high-tech terror, CNN, Apr 4, 2004 http://www.cnn.com/2004/TECH/04/04/mobile.terror/index.html.

http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf

http://timesofindia.indiatimes.com/city/delhi/DU-law-student-charged-

Gorman, L. and Maclean, D. Media and Society in Twentieth Century, Blackwell publishing, 2003.

http://www.thefreedictionary.com/obscene

 ISSN: 2582-6433

Coleman, 'Cyber Terrorism' (2003) Directions Magazine, http://www.directionsmag.com/articlephp?article also at http://www.ijiee.org/papers/126-I149.pdf

Wilson, C. (2005). "Computer Attack and Cyber terrorism: Vulnerabilities and Policy Is-

 ISSN: 2582-6433

sues for Congress". CRS

Report for Congress

Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi

Dr. Sirohi M. N., Cyber Terrorism and Information Warfare, Alpha Editions Delhi 67

Barry Collin, "The

Future of Cyber Terrorism," Proceedings of the 11th Annual International Symposium on Criminal Justice

Issues, the University of Illinois at Chicago, 1996