CYBERCRIME AND CYBER LAWS IN INDIA: A STUDY WITH SPECIAL REFERENCE TO FINANCIAL SECTOR IN MUMBAI

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Law

By

Nuruddin Khan

Registration Number: 41900708

Supervised By

Dr. Shobha Gulati (25990)

Law (Professor)

Lovely Professional University

LOVELY PROFESSIONAL UNIVERSITY PUNJAB

2024

TABLE OF CONTENTS

CHAPTER V

INTERNATIONAL LEGISLATIVE FRAMEWORK TO COMBAT CYBER CRIMES-COMPARATIVE STUDY OF INDIA, ISRAEL AND USA.

DECLARATION

I, hereby declare that the present work in the thesis titled "Cybercrime and Cyber Laws in India: A Study with Special Reference to Financial Sector in Mumbai" in fulfilment of degree of Doctor of Philosophy (Ph. D.) is outcome of research work carried out by me under the supervision Dr. Shobha Gulati, working as Associate Professor, in the School of Law, Lovely Professional University, Punjab, India. In keeping with general practice of reporting scientific observations, due acknowledgements have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.

Scholar

Khan Nuruddin Serajuddin

41900708

School of Law

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph. D. thesis entitled "Cybercrime and Cyber Laws in India: A Study with Special Reference to Financial Sector in Mumbai" submitted in fulfillment of the requirement for the reward of degree of Doctor of Philosophy (Ph.D.) in the Law Department , is a research work carried out by Khan Nuruddin Serajuddin, Registration No. 41900708, is bonafide record of his original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

Supervisor

Dr Shobha Gulati

Associate Professor

School of law

Lovely Professional University,

Punjab, India

ABSTRACT

This study delves into the critical intersection of cybercrime and cyber laws in India, focusing specifically on the financial sector within the bustling metropolis of Mumbai. With the rapid digital transformation of financial services, the vulnerability of financial institutions to cyber threats has increased exponentially. This thesis examines the evolving landscape of cyber threats, their impact on the financial sector, individuals and whether current cyber law is effective or not in safeguarding against such crimes.

This thesis discusses, a comprehensive analysis of cybercrime trends and incidents in Mumbai's financial sector is undertaken, shedding light on the various forms of cyberattacks that target banks, financial markets, individuals and other financial entities. Furthermore, the thesis assesses the legal framework governing cybercrimes in India as well as USA and Israel there relevant law and acts which India is missing at the current state, and made a comparison of all the law including the Information Technology Act, 2000, and its subsequent amendments.

The thesis also investigates the adequacy of cyber laws in addressing the ever-evolving techniques employed by cybercriminals. It explores challenges related to the detection, prevention, and prosecution of cybercrimes, as well as the role of regulatory authorities and law enforcement agencies in ensuring cybersecurity within the financial sector.

In addition, this thesis explores best practices and cybersecurity measures implemented by financial institutions in Mumbai, highlighting successful strategies to mitigate cyber threats. It also assesses the role of cybersecurity awareness and education in reducing the vulnerability of financial institutions and their customers to cybercrimes.

By analyzing data, case studies, and expert opinions, this thesis aims to provide valuable insights into the state of cybercrime and cyber laws in India's financial hub, Mumbai. Ultimately, it seeks to contribute to the enhancement of cybersecurity measures, the refinement of cyber laws, and the safeguarding of critical financial infrastructure in the digital age.

ACKNOWLEDGEMENT

I am thankful to the Almighty for showering the choicest blessings on me for completing my research work. I am deeply indebted and would like to express my sincere gratitude to my learned supervisor, Dr Shobha Gulati, Associate Professor, school of Law, Lovely Professional University, Phagwara, for her indispensable guidance, full support, meticulous supervision and confidence in the completion of my research work. Her kind encouragement and microscopic supervision inspired me always throughout the progress of my research work.

I am highly thankful to Dr Sanjay Modi, head of faculty School of Law, Lovely Professional University, Phagwara, for his invaluable guidance and support during my research. I am thankful to the Staff and Officials of the Central Library and Departmental Library of Lovely Professional University, Phagwara. They met my demands for material and assisted me in getting relevant information on the subject.

I am thankful to the Librarians and staff of Oriental College of law, Navi Mumbai for their help rendered to me in providing relevant books, journals and data concerning my topic. Also special thanks to Dr. Navpreet Kaur, School of law LPU for her unwavering support, motivation & guidance throughout this difficulty journey Any research is incomplete without fieldwork, and many people helped me in the field study. I would take this opportunity to appreciate the Authorities, Police Personnel and Cyber Experts, Respondents, law faculties, advocates and financial sector employees. Without their support, this research work would not have been possible.

The award of PhD is dedicated to my deceased father - Mr. Serajuddin Khan; his insight brings inspiration to me and unwavering support. While busy with my research, some people patiently kept encouraging me with their wisdom and blessings. My mother- Mrs. Husnara Begum, who always encouraged me to achieve my dream of becoming a doctorate, and my Brother-Mr. Kamaluddin Khan, my sister- Mrs. Fatima Sabnoor khan always supported me as my backbone. This profession and award owe to you all. A word of thanks to you is too little for your support. I am indebted to God for having blessed me with a wonderful family.

KHAN NURUDDIN SERAJUDDIN

ABBREVIATIONS

Internet Protocol:	IP
World wide web:	WWW
National Crime Record Bureau:	NCRB
Information Technology:	IT
Indian Penal Code:	IPC
Computer Emergency Response Team:	CERT-In
Centre for Development of Advanced Computing:	CDAC
Central Bureau of Investigation:	CBI
Department of Electronics:	DOE
World Trade Organization:	WTO
Information& Communication Technology:	ICT
Information Technology Enabled Services Industry:	ITES
Controller of Certifying Authorities:	CCA
Denial of Service attack:	DDoS
Indian Computer Emergency Response Team:	ICERT
One time password:	OTP
Local area network:	LAN
Wide area network:	WAN
Direct-to-Home:	DTH
Compound Annual Growth Rate	CAGR
Intellectual Property Right:	IPR
National Cyber Security Policy:	NCSP
Public personal Partnership	PPP
National Cyber Security Strategy	NCSS
United Nations Commission on International Trade Law:	UNCITRAL
Union of India:	UOI
World Summit on the Information Society:	WSIS
United Nations Commission on Trade and Development	UNCTAD
World Intellectual Property Organization:	WIPO

LIST OF CASES

LIST OF TABLES

Part II: Law Faculties

Part III: Lawyers/Advocates

Part IV: Financial sectors

LIST OF FIGURES

CHAPTER I

Introduction

1.1 INTRODUCTION

Cyber-crime is not something new to the world, as crime is being committed since the evolution of the people and cyber-crime is one of the parts of it. It can be defined as any criminal activity committed on the internet or through computer source or any device which is capable of accessing internet. In the present scenario cyber-crime is most widely used method to earn financial gain or access data or hack something valuable from the other. The term "cybercrime" was coined by William Gibson[1] and it got famous through his novel Neuromancer, the term cyber is generally used with technological innovations. It comes from the Greek word cybernetics, meaning "steersman" or "governor[2]." The first cyber-attack or cyber-crime took place in France and it was committed without the help of internet, attackers stole the financial market information by using the Telegraph system, from that moment the cyber-crime gained importance with new techniques evolving every day[3]. Similarly, the first cyber-crime began when Allen Scherr attacked the MIT computer networks, stealing passwords from their database, at present if calculate the amount of cyber-crime committed and volume of money involved it can surpass an entire economy[4]. Where all these crimes are committed on the Internet is referred to as cyberspace, and the laws that govern it are known as cyber-laws. These are universal laws that apply to everyone in this area. The domain of the law that deals with legal issues involving connected information technology is another definition of cyber law[5]. To put it simply, cyber law is the branch of the law that deals with computers, internet, cyber criminals, use of electronic devices. Since they regulate essentially every aspect of transactions involving the internet and cyberspace, cyber laws are very significant. Every action you take online has legal repercussions. Some elements of cyber law include intellectual property, electronic and digital signatures, data protection and privacy, identity theft, and e-commerce theft[6].

[1] Gibson, W. (2019). Neuromancer (1984). In Crime and Media (pp. 86-94). Routledge.
[2] Dr. Pramod Singh, *Laws on Cybercrime* 98 (Book Enclave, 2007)
[3] Available at https://arcticwolf.com/resources/blog/decade-of-cybercrime assessed on 16 August 2022 at 8am
[4] Available at https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 accessed on 17 Aug 2022 at 11am
[5] Mukta Martolia, *Types of Cybercrime in India and its detection* 38 (7 JCR, 1541)
[6] Ms. Anisha, *Awareness and strategy to prevent Cybercrimes: An Indian Perspective* 2 (Vol 7 Issue 3, IJAR)

Knowing the history of the Internet's development in India is essential for understanding cyber laws because it forms the basis for both these concepts. As the Internet is the mother of all cybercrimes, the Internet first appeared in India in 1986. Still, it wasn't until August 15, 1995, that it was made accessible to the academic and research communities and the general public[7]. The earliest internet service in India was called Educational Research Network (ERNET), and it was only accessible to communities involved in education and research. The Department of Electronics founded it in New Delhi with funding from the government and the United Nations Development Program[8]. Eight universities were involved, including NCST Bombay, the India Institute of Science, five IITs, and the Department of Electronics.

Recent changes in India's internet landscape demonstrate a fast-changing digital environment characterized by tremendous growth and increasing difficulties. With the country experiencing an increase in internet adoption, fueled by low-cost data plans and ubiquitous smartphone use, digital inclusion has become a priority. However, this development brings current challenges to the forefront, such as concerns about data privacy, cybersecurity threats, and the digital divide between cities and rural areas. To address privacy concerns, the Indian government has enacted legislative measures such as the Personal Data Protection Bill, but implementation remains challenging. Furthermore, the spread of misinformation and online harassment presents serious dangers to digital security and democratic discourse. Balancing innovation with strong legal frameworks and ethical standards is critical as India navigates its future.[9]

The importance of having cyber law for India is very important as it will cater to the rising cyber-crime, India has a very extensive and laid-out legal system. The most significant of the various laws that have been passed and followed is the Indian Constitution. These are just a few examples: the Indian Penal Code, the Indian Evidence Act of 1872, the Banker's Book Evidence Act of 1891, the Reserve Bank of India Act of 1934, the Companies Act, etc[10]. On the other hand, the growth of the Internet saw the creation of new, challenging legal issues.

[7] Jyoti, Shirish Mishra & Subodh Kesharwani , *Cybercrime: An Emerging Threat to Banks and NBFCs* 2 (scholasticseed 15)
[8] T. Ahmad, *Challenges of Cyber-crimes in India: A Critical analysis* 03 (WMSCI 2018 - 22nd World Multi-Conference on Systemics, Cybernetics and Informatics, Proceedings, 2018).
[9] Chatterjee, S., & Kar, A. K. (2018). Regulation and governance of the Internet of Things in India. Digital Policy, Regulation and Governance, 20(5), 399-412.
[10] S. Chatterjee, A. K. Kar, Y. K. Dwivedi, and H. Kizgin, *Prevention of cybercrimes in smart cities of India: from a citizen's perspective* 10 (Inf. Technol. People, 2019)

Considering the political, social, economic, and cultural conditions of the time, all of India's present laws were passed many years ago. At the time, no one could have predicted the Internet. The needs of cyberspace could never be anticipated, notwithstanding the extraordinary foresight of our expert drafting technicians. Due to the numerous legal issues and concerns that were created due to the arrival of the Internet, cyber laws had to be passed[11].

Second, despite the most forgiving and liberal interpretation, India's current laws could not be understood to encompass all facets of varied online activities in light of the developing cyberspace. In actuality, interpreting current laws in developing cyberspace without introducing new cyber laws will not be without severe hazards and issues, as evidenced by experience and wise judgment. Therefore, it is essential to pass pertinent cyber legislation. Third, no law at the time provided legal legitimacy or validity for actions taken in cyberspace. For instance, the vast majority of users access the Internet for email. In our country, email is still not regarded as "legal." In the nation, no law gives email legal standing and consequences. Our courts and judges have been cautious about giving email's legality judicial credibility because there isn't a formal statute that has authorized. A need for cyber law has arisen as a result. Fourth, the Internet requires a cutting-edge legal framework that is both enabling and beneficial. Adopting appropriate Cyber laws can offer this legal framework, as customary laws have failed to do so. Only if the necessary legal framework is in place can e-commerce, the most promising aspect of the Internet, be viable. These and other elements have made India need to develop effective cyber security measures.

If we see the recent trends of cyber-crime in India and number of transactions taking place on daily basis, the number of people who are at risk and are on the verge of losing their hard-earned money to the cyber criminals. The Internet brings the world to your doorstep and provides services with one click. The development of technology and the use of the Internet on computers, mobile phones, and other devices are making it more accessible to individuals. Such usage of the Internet brings advantages as well as disadvantages to individuals. One aspect is the cybercrimes towards individuals, corporations, financial sector, communications, defense sector, and every other sector related to technology or the Internet, which is at disposable in the hands of cybercriminals. Recent trends in cyber-crime reveal huge data breaches. Due to

[11] R.C Dikshit, *Cyber Crime* 09 (CBI Bulletin 2016)

the pandemic, the workforce is more vulnerable to attacks as they are not equipped with cyber security programs or applications corporations also face a similar situation.

According to Gartner, the world data safety market is most likely to reach $170.4 billion in 2022[12]. This is because large organizations are developing their defenses against cyber threats. According to cybint[13] 95% of cybersecurity breaches are due to human error. To bring to attention the impact of cybercrime in the contemporary world, the following stats are eye opener to society. They are as follows.

1. In 2019, attempts at spear phishing (the fraudulent technique of sending emails purporting to be from a recognized or trustworthy sender to persuade targeted individuals to give confidential information) were made by 88% of enterprises and organizations worldwide[14].
2. Most business executives of which 68%[15] believe their cybersecurity risks are rising.
3. In the first half of 2020, data breaches revealed 36 billion records[16].
4. Hacking accounted for 45% of breaches, followed by malware at 17% and phishing at 22%[17].
5. Both humans and machines use 300 billion passwords, according to estimates[18].

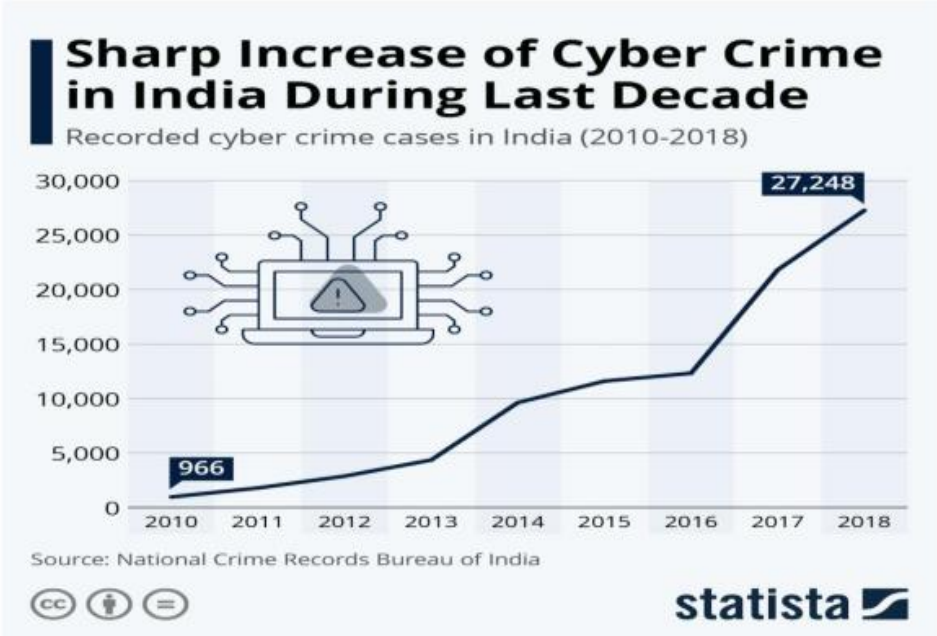
The following data shows how vulnerable industries, individuals, and common people are to cybercriminals.

Now we will look at the recent trends in cybercrime in India and how India copes with the cyber criminals in recent times. The pandemic and the lockdown made people work from home and spend time online daily, relying on the Internet to access services. The impact of cybercrime increased a lot as more people got connected to the Internet. This gave cybercriminals more opportunities to take advantage of individuals and conduct cybercrime. Due to the widespread usage of the Internet, common techniques are being overtaken by cybercrime. According to the report, 52 Lacs local cyber threats in India were found and

[12] Available at https://www.gartner.com/en/documents/3889055 accessed on 11 Jan 2020 at 11:13am
[13] Available at https://www.cybintsolutions.com/cyber-security-facts-stats accessed on 11 Jan 2020 at 11:20am
[14] Available at https://www.proofpoint.com/us/resources/threat-reports/state-of-phish accessed on 11 Jan 2020 at 11:45am
[15] Available at https://www.cybintsolutions.com/cyber-security-facts-stats accessed on 11 Jan 2020 at 11:20am
[16] Available at https://pages.riskbasedsecurity.com/en/en/2020-q3-data-breach-quickview-reporty," Q3 report 2020 data breach quick view" accessed on 11 Jan 2020 at 11:50am
[17] Available at https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf accessed on 11 Jan 2020 at 12:10pm
[18] Available at cmagazine.com/video-300-billion-passwords-by-2020-report-predicts/article/634848 accessed on 12 Jan 2020 at 8:00am

neutralized using “Kaspersky Security Network (KSN)” products between January and March of this year. In terms of the number of web risks discovered by the company in Q1 2020, India is currently rated 27th internationally, up from 32nd in Q4 2019".

"There has been a significant increase in the number of attacks in 2020 Q1 that may continue to rise in Q2, especially in the current scenario where we are seeing an increase in cybercriminal activities, particularly in the Asia Pacific region," said Saurabh Sharma, Senior Security Researcher, GReAT Asia Pacific at Kaspersky. How frequently people are the target of malware spread via detachable USB sticks, CDs and DVDs, and other "offline" approaches are shown by the number of local attacks in India in Q1 2020 (52 Lacs). To defend against such attacks, you need more than just antivirus software that can handle infected objects; you also require access to removable devices, a firewall, and anti-rootkit functionality. The company reports that 40 Lacs local threats were found in Q4 of 2019[19].



(Source of Image: www. Statista.com)

The following statistics show an increase in cybercrimes in India over the past ten years, with a progressive increase over time. One thing is certain: cybercrime will continue to exist unless cyber security mechanisms are enhanced to combat cybercriminals in the future[20].

[19] Available at https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf Kaspersky Security Bulletin 2020 accessed on 12 Jan 2020 8:15am

[20] Hamid Jahankhani, *Cyber Criminology* 33 (Springer, ISSN 1613-5113 ISSN 2363-9466 (electronic) Advanced Sciences and Technologies for Security Applications,2018)

Cyber-crime in Maharashtra, particularly in Mumbai, is an important trend in my topic. In recent decades, Maharashtra and Mumbai have been subjected to the fury of cybercrime. The state has reported 16,512 cybercrime cases in the last five years, with 4,530 cases cracked thus far. In 2018 and 2019, 3,511 and 4,822 cybercrime instances were reported, respectively.

In 2019, 7,500 criminal cases were filed in Pune, with the same number of cybercrime cases. This emphasizes the seriousness of the problem," he stated. In 2019 and 2018, police reported 799 and 867 cases, respectively, involving obscene and insulting comments addressed to women and girls via social media and e-mail[21].

According to statistics given by the Mumbai Police Department, there will be 2,435 cases of cybercrime in Mumbai in 2020, up from 2,225 cases in 2019. There were 207 of them, or 8.5 percent, detected in 2020. The cybercrime detection rate in Mumbai is just 7%, so it's very rare that once under cybercriminals, there are fewer chances one would receive his or her hard-earned money, data, and information in Mumbai. (January 10, 2021)[22].

SR.NO	CYBERCRIME REPORTED IN MUMBAI	YEAR
1.	1361	2017
2.	1375	2018
3.	2225	2019
4.	2435	2020
5.	2883	2021
6.	4718	2022

Source: NCRB 2023

The recent trends in cybercrimes worldwide, then in India after that Maharashtra, and lastly Mumbai gives a broader view of how cyber criminals have a far-reaching effect on the individuals, corporations, economy, and critical infrastructure of the nation.

[21]Available at https://www.hindustantimes.com/cities/mumbai-news/mumbai-ranks-third-in-country-in-cybercrimes-in-2020 accessed on 12 Jan 2020 at 8:40am.
[22] Available at https://www.htsyndication.com/ht-mumbai/article/beware%2C-city-recorded-more-cybercrimes-in-2020%3A-data/48244555 accessed on 12 Jan 2020 at 9am

1.2 STATEMENT OF PROBLEM

The main aim behind my research is that infrastructure vulnerability and current laws do not cater to cybercrime problems in the current scenario. The stats show how the world is facing the problem of cybercrime in the current pandemic, and it will have a long-lasting effect on the world if not catered to suitably. This research deals with cybercrime and cyber laws concerning the financial sector in Mumbai. The financial sector of any nation is the most important in any form; if such a sector crumbles into the hands of cyber criminals, then it will throw an economy past, we can say, behind 20 years. Cyber criminals can bring an economy down by getting into the critical infrastructure of a nation's system. The reason behind selecting this topic is that the following issues should be dealt immediately.

1. “The Information Technology Act of 2000” present rules cannot keep up with technological advancements, and on the same point, cybercriminals are always one step ahead of cyber security.
2. The cyber security mechanism needs a revamp at the earliest so that if cybercriminals hit the nation's critical infrastructure, such as the defence sector, electrical grids, stock exchanges, and monetary sector, it will pose a huge threat to the nation.
3. The rise in Internet usage as India will be among the top countries to consume Internet and such population should be vulnerable to cyber criminals as mostly the population is unaware of cybercrime one OTP shared by an uneducated citizen can cause huge loss to him.
4. The awareness part of the cybercrime is also an issue in India as it is not given due importance and on a similar note the cybersecurity.
5. The Cyber terrorism is also gaining impetus, and people are brainwashed in the cyber world; this has led to the growth of terrorism in the cyber world and given the upper hand to cyber criminals to recruit individuals for the wrong purposes.
6. The financial sector in Mumbai is the heart and soul of India; an attack on the financial hub of India can bring the economy down, and crores of rupees will be at stake if cybercriminals hack into financial bodies such as stock exchanges, RBI, which is there in Mumbai and Private sector banks such as ICICI, HDFC has headquarters in Mumbai. This financial sector is not equipped with top cyber security mechanisms.

The above said problems are to be addressed immediately so that cyber criminals cannot get into our nation's critical infrastructure.

1.3 LITERATURE REVIEW

Acharya, Suman &Sujata. "*Impact of cyber-Attacks on banking institutions in India: A study with special of safety mechanisms and preventive measures*." PalArch's Journal of Archaeology of Egypt/Egyptology 17.6 (2020): 4656-4670. The impact of cyberattacks on banking institutions was discussed in the research paper that followed. Case studies of banks that had been attacked were used, such as the 2017 attack on UBI, which was carried out through phishing through an email that triggered the attack, and the malicious attack on Cosmos Bank in Pune, which was carried out through malware attack and disrupted the bank's services. A comparison of the number of cyber cases involving nationalised banks and private sector banks was done to determine the impact on the financial sector after ATM services were attacked[23].

Jyoti, Shirish Mishra & Subodh Kesharwani , "*Cybercrime: An Emerging Threat to Banks and NBFCs*", 2 scholastic seed 15. This research paper covered the cybercrime and its threats to banks and NBFCs and how it crippled the system and occasions and digital transactions were manipulated used for financial gains by the cybercrime experts for their benefits. The paper has thrown light on the methods of cyber security and Blockchain systems which is a method used for digital transactions. The Blockchain system covers a lot of systems which does not let the cybercriminals bypass the system easily and it's more secure. Cyber security with the hands of the Blockchain system is a convenient method to curb cybercrimes and protect the banks and NBFCs[24].

Harshita, "*Cybercrime in Banking sector*", International Journal of Research Granthaalayah, Vol 7 issue 1 (2019) 148-161. In the research article, cybercrimes in the banking industry were discussed, as well as examples that frequently occurred there. It supplied information and statistics on the instances in which the banking industry was targeted, including emails that are initially open to vulnerability and are promptly targeted by cybercriminals, as well as information on internet banking, mobile banking, and other services and discussed how the number of cell phones with internet connection and the heinousness of cybercrime crimes have surged. Mobile devices are utilised for various internet-based

[23] Acharya, Suman & Sujata. *Impact of cyber-Attacks on banking institutions in India: A study with special of safety mechanisms and preventive measures* 03(PalArch's Journal of Archaeology of Egypt/Egyptology 17.6 (2020): 4656-4670.**)**

[24] Jyoti, Shirish Mishra & Subodh Kasarani, *Cybercrime: An Emerging Threat to Banks and NBFC 0*2 (scholastic seed 15)

activities, such as online shopping, service fee payment, and money-saving. Cell phones are frequently used by criminals to gain sensitive information.[25]

S. Kumudha and Aswathy Rajan, "*A Critical Analysis of Cyber Phishing and its Impact on Banking Sector*," International Journal of Pure and Applied Mathematics Vol 119 No. 17 (2019) 1557- 1568. The research scholar looked at the effects of cyber phishing and how it affected the banking industry. Cyber phishing involves the theft of important data, such as a customer's login credentials, which provides cybercriminals access to the customer's bank accounts. The paper also discussed the various crimes towards the financial sector using the cyberspace, such as hacking, credit card fraud, Phishing, or identity theft, and used the case of Pune Citibank Mphasis bank call center fraud. The paper described the impact of cybercrimes to the extent with support of case laws and provided suggestions also[26].

Steve Morgan, "*Cybercrime to Cost the World $10.5 Trillion Annually By 2025*", Nov. 13, 2020, PRNewswire Cyber security ventures. The following sectors were examined in the article that looked at how much money is spent on cybercrime globally each year, which is more than India's economy. Internet safety Over the next five years, costs associated with cybercrime are predicted to increase by 15% annually, reaching USD 10.5 trillion in 2025 from USD 3 trillion in 2015. It threatens investment and innovation incentives, is ten times greater than the annual damage caused by natural disasters, and will be more profitable than the global trade in all major illegal substances combined. It is also the greatest transfer of economic wealth in history.[27]

Regina Mihind kulasuriya , "*If cybercrime were a country, its economy would be bigger than India's, says US firm's report,"* The Print Tech edition. The following article by Print tech online edition provided insight into the research report by cyber security ventures. Because if cybercrime were a country, its GDP would be larger than India's; it's easy to see how serious cybercrime is in India and worldwide. In comparison, India's economy is currently rated fifth. India's GDP was projected to be slightly less than $3 trillion in 2019, which means that the cost

[25] Harshita, Cybercrime in Banking sector 04 (International Journal of Research Granthaalayah, Vol 7 issue 1 (2019) 148-161)

[26] S. Kumudha and Aswathy Rajan, *A Critical Analysis of Cyber Phishing and its Impact on Banking Sector* 03 (International Journal of Pure and Applied Mathematics Vol 119 No. 17 (2019) 1557- 1568)

[27] Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually By 2025* 20 (Sausalito, Calif. Nov. 13, 2020 PRNewswire Cyber security ventures)

of worldwide cybercrime has just surpassed the amount of the Indian economy. The report's projection was based on yearly cybercrime growth and a "dramatic surge in hostile nation-state sponsored and organized crime gang hacking activities," according to the report. It has also considered how, by 2025, many linked devices and individuals will be online, which would further increase the "cyber-attack surface" for business hackers.[28]

CSO India, "*India's IT act 2000 a Toothless tiger",* SOUMIK GHOSH. This article covered the loopholes in India's IT act 2000 and discussed with India's eminent cyber law expert Dr. Pavan Duggal advocate supreme court, who stated that "The IT Act also doesn't address privacy issues – privacy is now a fundamental right and the law needs to address privacy concerns specifically, but that's not the case."[29]

Anam Ajmal, "*Need surveillance reform, privacy law: Cyber experts,"* Times of India. The following article from the Times of India covered the need for Privacy law at the earliest as the security breach of the Pegasus software turns the privacy into a play for hackers to track, and it provides power unlimited access to one's mobile and intercepts calls of the target and also provides the gps location this Pegasus software turned out to be the privacy breaches of the new world in India. Such a spyware with no policies on privacy which can be breached by the spyware easily and leaving the vulnerabilities of the citizens at the hands of the cybercriminals. [30]

Bharat Panchal Chief Risk officer, "*Getting cyber defenses ready",* financial express. India needs a robust security policy, this article from financial express and from the Chief risk officer of India, Middle East and he recommended that there is need to amend the Information Technology 2000 to tackle the rising cyber-attack and cyber-attacks[31].

Morya, Kishore K., and Mahesh Singh. "*Study of Latest Cybersecurity Threats to IT/OT and their Impact on e-Governance in India*", International Journal on Emerging

[28] Regina Mihindkulasuriya , "*If cybercrime were a country, its economy would be bigger than India's, says US firm's report",* The Print Tech edition November 2020 7:30Pm IST.

[29]https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html (12 Nov 2019) dated 20 oct 2020 3:31pm.

[30] https://timesofindia.indiatimes.com/india/need-surveillance-reform-privacy-law-cyber-experts/articleshow 26 oct 2020 12:37pm.

[31] Bharat Panchal Cheif Risk officer, *getting cyber defenses ready,* Financial express/ inancialexpress.com/opinion/getting-cyber-defences-ready-india-needs-a-robust-cybersecurity-policy/2077314/ 15 December 2020 10:17am.

Technologies 11(2): 939-947(2020). The study discussed cyber security challenges in today's times, when technology permeates all aspects of society, including e-Government apps. The study also looked at how e-Government can be made more secure and what kind of security features should be implemented. A number of e-Government technologies, including cloud computing, e-commerce, social networking, online government banking, online bill payment, and others requires a safe, secure, and dependable environment. However, it was discovered throughout the research that there have been few studies on cyber security of IT/OT infrastructure utilized for e-Government in India. The study focused on cyber security and e Governance, a vital aspect in the current scenario.[32]

Virmani DC, Kaushik N, M, Mathur V, Saxena S (2020), "*Analysis of cyber-attacks and security intelligence: Identity theft.*" Indian Journal of Science and Technology 13(25): 2529-2536. The following paper discussed security intelligence and identity theft, the most crucial tool cybercriminals use. Identity theft was critically examined, including medical, child, and biometric identity theft. It also provided the systems and tools that were employed by cybercriminals for identity theft. The report and information below There were 410927 identity theft occurrences in 2018, but there are now 562864 cases, a phenomenal growth of 37.0 percent over 2018. This shows that identity theft cases are rising daily and greatly worrying society.[33]

Rajasekharaiah, K. M., Chhaya S. Dule, and E. Sudarshan. "*Cyber Security Challenges and its Emerging Trends on Latest Technologies*." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020. The study attempted to address cyber security concerns and trends, focusing on the financial sector. To prevent personal information from slipping into the wrong hands, the finance sector should track and develop its systems regularly. The banking sector has traditionally been the first to develop safety systems and behaviors, as well as the first to invest in cyber security. According to cyber security experts, malware is the most common way for bad arms to circumvent cyberspace security efforts. Malware is a broad category of attacks installed on a device without the rightful owner's consent. Viruses, worms, Trojan horses, spyware, and bots are examples of malicious

[32] Morya, Kishore K., and Mahesh Singh, *Study of Latest Cybersecurity Threats to IT/OT and their Impact on e-Governance in India* 04 (International Journal on Emerging Technologies 11(2): 939-947(2020).
[33] Virmani , Kaushik & Mathur (2020) Analysis of cyber-attacks and security intelligence: Identity theft. Indian Journal of Science and Technology 13(25): 2529-2536 https://doi.org/ 10.17485/IJST/v13i25.580.

software executables, malware infects computers in several ways; the paper pointed out the vulnerabilities in the infrastructure, such as the network, hardware, and software[34].

Robert Birtstone, "How *cyber attackers are coming after in 2021*", The Register. The following article in The Register online newspaper discussed the impact of cybercrime in the year 2021 and how the cyber criminals will be targeting the the society cyber security company Darktrace knows the pattern of cybercriminals and they have found the pattern by looking into 4000 organizations that rely on technology attacker are increasingly targeting businesses using the most volatile assets its people.[35]

Money control, "*Apple supplier Foxconn suffers ransomware attack, hackers demand $34 million in bitcoin*", Money control Technology 8 December 2020. The following showed that electronic giants such as Foxconn is also not safe it suffered ransomware attack from cybercriminals, Foxconn being one of the major players in manufacturing iPhone and many popular devices the cybercriminals encrypted over 1000 servers at Foxconn and demanded 34 Million in Bitcoin one bitcoin equals to 16 lakhs in INR such level of attack can bring the whole system down and can cripple the whole infrastructure.[36]

Times now News, "Credit, *debit card data of over 70 lakh Indians leaked online*", Times now news Business Industry. The article brought into picture the amount of data theft that is being carried out in the current scenario, Data was collected from Dark web forums and disseminated to potential clients, according to cyber security researcher Rajshekhar. and the data belonged to third party banking partner operator. Such level of data theft with precious information can damage more as compared to normal crime.[37]

[34] Rajasekharaiah, K. M., Chhaya & E. Sudarshan. "*Cyber Security Challenges and its Emerging Trends on Latest Technologies*." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020
[35] Robert Birtstone, "How cyber attackers are coming after in 2021", The Register, www.theregister.com/2020/12/17/attackers_are_coming_in_2021 December 18th 9:15 Pm
[36] Money control, "Apple *supplier Foxconn suffers ransomware attack, hackers demand $34 million in bitcoin",* Money control Technology https://www.moneycontrol.com/news/technology/apple-supplier-foxconn-suffers-ransomware-attack-hackers-demand-34-million-in-bitcoin-6206791.html 18th December 9:28Pm
[37] Times now News, "Credit, *debit card data of over 70 lakh Indians leaked online*", Times now news Business Industry https://www.timesnownews.com/business-economy/industry/article/credit-debit-card-data-of-over-70-lakh-indians-leaked-online/693288 December 9:40Pm

CISO.in, "India *approves game-changing framework against cyber threats*," CISO Latest Security IT news. The CISO article below highlighted the revolutionary advancement in cyberattacks. The Union Cabinet passed the "National Security Directive on Telecom Sector" in response to the terrifying scope of cyberthreats to India. According to the ministry of Electronics and Information Technology Security, ransomware attacks and data and identity thefts have been a top cause of concern for India's National Security Council[38].

Vallabh Ozarker, "*Cybercrime detection in Mumbai is just 7%*", Mumbai Mirror 20th December 2020. An article was released in Mumbai; the detection rate of cybercrime in Mumbai, according to Mirror, is just 7%. Even if there are more cybercrimes every day, the detection rate is quite low. Mumbai claims that as of November 2020, 2000 incidents had been reported, and 150 cases had been resolved. According to cyber specialist Riteish Bhatia, the police have given up simply because they cannot keep up with the technologies used by scammers.[39]

Hindustan Times Tech, "Hackers *continue targeting remote employees in India, 36mn attacks reported till Nov*", Hindustan Times Tech 20 December 2020. The following covered the attacks on remote employees in India, 36 million being a huge number the following number of people are attacked. Researchers from Kaspersky discovered a 242 percent rise in brute force attacks against Remote Desktop Protocols (RDP) compared to the previous year. In addition, 1.7 million malicious files posing as corporate communication programs were discovered. According to researchers, the people working in such small spaces are vulnerable to attackers.[40]

Ajay Sarangam , " *cyber security challenges In India*," Jigsaw academy September 2020. The threats to cyber security were discussed in the article after that. Ajay Sarangam pointed out several problems in India, including the absence of a national cybersecurity infrastructure.

---

[38] CISO.in, "India approves game-changing framework against cyber threats", CISO Latest security IT news. https://ciso.economictimes.indiatimes.com/news/india-approves-game-changing-framework-against-cyber-threats 18th December 2020 9:53 Pm

[39] Vallabh Ozarker, "*Cybercrime detection in Mumbai is just 7%*", Mumbai Mirror 20th December 2020 https://mumbaimirror.indiatimes.com/mumbai/other/7-per-cent-thats-it/articleshow/79817972 21st December 2020 8:34Pm

[40] Hindustan Times Tech, "Hackers continue targeting remote employees in India, 36mn attacks reported till Nov", Hindustan Times Tech 20 December 2020 https://tech.hindustantimes.com/tech/news/hackers-continue-targeting-remote-employees-in-india-36mn-attacks-reported-till-nov- 8:41pm 21st December 2020

The armed forces, ONGC's digital assets, banking operations, and other functions are all vulnerable to cyber-attacks since cyberspace has no boundaries, unlike countries or states. Because there is no cybersecurity regulatory body, this could result in national security breaches that cause loss of money, property, or life as well as ignorance. In the next days, these kinds of obstacles must be overcome if national cybersecurity is to be established.[41]

Dr.Sudhir Kumar, " *Cyber Security: A Legal Perspective*", International Journal of Computer and Internet Security. ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 1-11. The reseach paper provided the legal perspective of cyber security and cyberlaws as they have become an integral part of our lives and technology is upgrading faster. Even though we use a variety of countermeasures, the internet security problem is rapidly worsening, and cybercrime is on the rise. And the research paper covered the various laws relating to cybercrimes such as Indian Penal code, Information Technology and jurisdiction and procedure[42].

Rao, Yerra Shankar, et al. "*Digital Crime and its Impact in Present Society*." International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol 8 Issue 1, 1-6. The focus of a research report was on the effects of cybercrime in contemporary society. The author discussed the various forms of data crime that take place online, such as data alteration, data interception, and data theft, as well as the impact on society, including how crime affects socioeconomic policy, how it affects teenagers, how private industry is affected, how it affects the digital economy, how consumers behave, and how it affects business. The researcher claims that "research has shown that no rule can successfully be imposed that can remove the scourge of cybercrime." Although there have been local and international initiatives, these laws have not yet been overturned.[43]

Singh, Tejinder, and Nitin Pathak. "*Emerging role of artificial intelligence in Indian Banking sector*" Journal of critical reviews ISSN- 2394-5125 VOL 7, ISSUE 16, 2020 1370-1373. The following research paper covered the role of artificial intelligence in banking sector and provided various artificial technologies used by different banks. The artificial

[41] Ajay Sarangam, "cyber security challenges In India", Jigsaw academy September 2020 https://www.jsa.com/cyber-security-challenges-in-india/ 8:54pm 21 st December 2020
[42] Dr. Sudhir Sharma, *Cyber Security: A Legal Perspective* 1-11 (IJCIS. ISSN 0974-2247 Volume 9, Number 1 2017)
[43] Rao, Yerra Shankar, et al. *Digital Crime and its Impact in Present Society* 1-6 (International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol 8 Issue 1)

intelligence is the next step in the banking sector and provides for non-interference of human during the process but sometimes the AI technology is vulnerable and can be bypassed by the cybercriminals and steal the relevant information of the relevant customer which is very personal and can cause huge loss to the individual. The researcher provided that the Implementation of AI suffers from There are numerous hurdles. Because of the increasing risk of online fraud, many still prefer the traditional banking channels, i.e. the brick-and-mortar approach, to the automated tools. hacking etc[44].

Satya Prakash, "*Information Technology legislation falls far short*" The Tribune January 2020. The following article published in the tribune newspaper written by Satya Prakash brought up the defects of the Information Technology act as many loopholes it provided that the amendment made in the information technology act was just cosmetic and doesn't cover any aspects of cybercrimes and pointed out the example of china that they have cyber security laws and similarly India should frame cyber security policies on that line to curb cybercrimes.[45]

Kashyap, Sunidhi, and Kuldeep Chand. "*Cyber Security and Safe Computing: Need of an Hour which needs to be solved*." The International journal of analytical and experimental modal analysis vol 12 issue 9 September 2020 720-722. The next research article addressed the issue of cyber security because the Indian Evidence Act, Indian Penal Code, and Indian Penal Code were all created centuries ago and solely addressed traditional crimes. And now, the time has changed, and modern crimes are being committed. Similarly, the following legislation should be an amendment in the coming days to curb the cybercrimes and give a deterrent effect to the cybercriminals. Similarly, essential adjustments to the Indian Evidence Act have been made to consider the papers stored in the computer system and its accessories so that they can be used as evidence during the trial.[46]

Prashant Mali, et al. "Analyzing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study", International Journal of Mechanical Engineering and Technology 9(2), 2018, pp. 110–124. The study provides an

[44] Singh, Tejinder, and Nitin Pathak., *Emerging role of artificial intelligence in indian banking sector* 1370-1373 (journal of critical reviews ISSN- 2394-5125 VOL 7, ISSUE 16, 2020)
[45] Satya Prakash, "Information Technology legislation falls far Short" The Tribune January 2020
[46] Kashyap, Sunidhi, and Kuldeep Chand, *Cyber Security and Safe Computing: Need of an Hour which needs to be solved* 02 (The International journal of analytical and experimental modal analysis vol 12 issue 9 September 2020)

overview of current theories regarding the challenges provided by cybercrime. It started by looking at the definitions of cybercrime and cyberwarfare that were currently in use, discovering two problems that needed to be resolved. First of all, it was found that neither cybercrime nor cyberwarfare have a widely recognized definition. This is problematic because, in the absence of a shared nomenclature, it is challenging to examine the most serious issues or even identify instances of cyberwarfare. The researcher claims that every aspect of modern life has been impacted by cybercrime. However, the most vulnerable sectors are the government and the financial institutions. [47]

Times Now, *"Facilitate academic fraternity to work on cyber security, awareness measures: UGC tells varsities"* Times Now, Education news. The University Grants Commission (UGC) has asked all colleges and universities to help and support academics who are working on cyber security and to incorporate it into their curricula. The government is now creating a national cyber security strategy paper, according to the commission, and until then, cyber security instruction should start in elementary schools. According to the UGC's directive, cybersecurity and cybercrime are significant issues that need to be addressed in society for everyone's general welfare.[48]

ETNOW NEW.COM, "*Chinese launch covert cyber-attacks on India: Millions of online shoppers targeted," ET now digital.* The following article discusses how Chinese hackers secretly attacked millions of Indians during the festival months of October and November by targeting online shoppers. According to the CyberPeace Foundation, a cybersecurity think group, during India's busiest shopping season, hackers from China's Guangdong and Henan regions repeatedly attacked unwary Indians. These hackers created fake URLs that appeared to be offers from Flipkart and Amazon and persuaded internet users to click on them by promising fake prizes. These URLs were distributed via WhatsApp to a sizable number of online shoppers in India. CyberPeace asserts that hackers registered these domains using Alibaba's cloud computing platform. These fake URLs are still active and continue to target certain people. The

[47] Prashant , Sodhi, Triveni , Sanjeev , *Analysing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study* 110-124 (International Journal of Mechanical Engineering and Technology 9(2), 2018)

[48] Times Now, *"Facilitate academic fraternity to work on cyber security, awareness measures: UGC tells varsities"* Times Now, Education news. 03rd December 2020.

following attack on the people and lure them was targeted by the Chinese and gained access into the credentials of online portal[49].

NDTV, "*62% Of Cybercrime Complaints In 2020 Linked To Financial Frauds: Delhi Police",* Press Trust of India. The following article covered the financial crimes in Delhi as most of them were cybercrime and related to financial frauds. Twenty-four percent of the complaints were about online harassment on social media, and the remaining fourteen percent were about crimes like hacking and data theft. "Of the various cybercrime complaints received, the most common are online financial frauds, accounting for around 62% of the total," according to the statement.[50]

News18 India, "*Cyber Frauds are Calling Up UP Residents for 'Vaccine Registration' to Swipe Their Aadhaar, Bank Details."* News18. The following article on cybercrime brings into the role of technology and others can be duped, authorities are planning to conduct coronavirus vaccinations in the next weeks, unscrupulous elements have started phoning Uttar Pradesh citizens to obtain personal information under the guise of vaccine registrations. Authorities have since become aware of a slew of similar frauds. Cybercriminals have called many people in Gorakhpur, Deoria, Basti, Mau, Ghazipur, and Pratapgarh in search of crucial personal information such as Aadhaar numbers, bank account numbers, and insurance policy numbers. People were forced to register, and as a result, cybercriminals stole their personal information.[51]

Carin Smith, "Watch *out for these financial crimes threats in 2021",* Fin 24. The kasperkey researchers pointed out the latest financial crimes to be aware in 2021, they are as follows financial cyber criminals are likey to target bitcoins more often, extortion practices will become more widespread and magecarting (stealing data from e commerce) , hoax emails will rise so financial crimes will be an threat to the whole community at large.[52]

---

[49] ETNOW NEW.COM, "*Chinese launch covert cyber-attacks on India: Millions of online shoppers targeted", ET now digital 19*Dec 2020

[50] NDTV, "*62% Of Cybercrime Complaints In 2020 Linked To Financial Frauds: Delhi Police",* Press Trust of India 30 December 2020.

[51] News18 India, "*Cyber Frauds are Calling Up UP Residents for 'Vaccine Registration' to Swipe Their Aadhaar, Bank Details".* News18, https://www.news18.com/news/india/cyber-frauds-are-calling-up-up-residents-for-vaccine-registration-to-swipe-their-aadhaar-bank-details-3236567.html 22 Feb 2020 5:19 pm 2021

[52] Carin Smith, "Watch *out for these financial crimes threats in 2021",* Fin 24, https://www.news24.com/fin24/companies/ict/watch-out-for-these-financial-cybercrime-threats-in-2021-20201231 22 Feb 2021 5: 28pm

Aman Nair, *"Pandemic technology takes its toll on data privacy*," Deccan Herald. Technology is being used to combat covid 19 and various apps have been developed in order to look into the signing of individuals for taking vaccine more than 70 apps have been made since 2020-21 for the covid vaccination or to give information on the vaccine related queries. It poses a threat to the date collected specially the personal data collected from individuals and due to that there are greater chance of misuse of data collected from various sources. One may use the illustration of Aarogya Setu gathers personal data including name, age, sex, career, and location. Major privacy issues regarding the gathering, storing, and use of personal data have developed as a result of the absence of supporting legislation and a personal data protection bill.[53]

Archana More, "cybercrime *101: dissecting the ongoing trend",* Pune Mirror. The following article covered the aspects of ongoing trend in as it becomes difficult for the police to after verifying the IP address of cyber criminals and investigate in other states due to KYC problems while searching for addresses of cyber frauds. The ongoing trend in the city of pune is the sextortion cases are rising day and police have identified the sources still they have failed to catch the cybercriminals. In this regard cyber expert Guarav Jachak opined that, victim should approach the police as early as possible and he also said that the victims are negligent and fall for honey trap by seeing the profile of females and vice versa. The dating apps are being used sextortion from victims and extort money from specially youngsters. [54]

Chandra Shrikanth, "Personal *Data Protection bill/ Hackers having Field Day as centre dither's: Justice BN SriKrishna,"* Money control. In a personal interview with Money Control about the data protection bill, Justice BN Srikrishna criticized the government, claiming that citizens have no recourse from frequent data breaches because the bill to protect their data is still pending. Justice BN Srikrishna chaired the 10-member committee that proposed India's personal data protection bill three years ago. Because there is no law to prevent it. The draft is pending before the Joint parliamentary committee. He commented on the data breach of 18crore customers information was leaked of dominos and it was made public it was due to compromise of amazon web services. The last six months various data breaches such as air India, Big basked Mobikwik. There are rules under consumer protection e commerce rules

[53] Aman Nair, *"Pandemic technology takes its toll on data privacy*", Deccan Herald, June 13 2021 at 9: 18am
[54] Archana More, "cybercrime *101: dissecting the ongoing trend",* Pune Mirror , May 29, 2021 at 6:00am

2019 but there haven't been any precedents where companies have been accountable. He emphasized that a new law is necessary. IT regulations were not created with the security of personal data in mind. If your data is stolen, the data fiduciary who stores the data is accountable under the personal data protection bill. Dominos would have been held accountable as the data fiduciary in this case if PDP was law. [55]

News18 Technology, "How *critical infrastructure cyber-attacks can change the way we live",* New18. Power grids, energy distribution networks, defence, healthcare, and other aspects of our Indian infrastructure are increasingly under threat. These are done for various reasons, such as to create diplomatic pressure or obtain sensitive system data. We are moving towards smart cities, but at the core of the problem, we don't have a comprehensive security plan for public spaces.[56]

Ankita Chakravarti, "*leaked data of Dominos India users now available on search engine created by hacker",* India Today News. According to security experts, the data of 18 crore consumers was exposed on the dark web as a result of a data breach at the prominent pizza chain Dominos. If a dominos player is frequent, his personal information is easily accessible on the dark web. The data includes the name, email, phone number, and even the GPS location of the user. The data breach occurred in April and was 13TB in size. According to security expert Rajshekhar Rajaria, the same hacker accessed Mobikwik and afterwards sold the data to resellers; however, because he was not compensated in the case of Dominos, he made the data openly available for viewing on the dark web. People are exploiting the data to spy on people and track their movements in the past, posing a serious threat to our privacy[57].

Jitesh Vachhatani, "Air *India data of 45 lakh passengers including credit cards leaked in massive breach",* Republic world. The following data breach was done to the Air India and 45 lakh passengers' information was breached. information such passport details, credit cards, although all of the frequent flyer information was gathered, Air India insisted that the

[55] Chandra Shrikanth, "Personal *Data Protection bill/ Hackers having Field day as centre ditheres : Justice BN SriKrishna",* Money control, May 25, 2021 at 6:31am
[56] News18 Technology, "How *critical infrastructure cyber-attacks can change the way we live",* New18, May 22, 2021 at 5: 40 pm
[57] Ankita Chakravarti, "*leaked data of Dominos India users now available on search engine created by hacker",* India Today News May 22 2021 at 10:57 am

CVV/CVC numbers of the passengers had not been compromised. Similar data breaches involving client theft occurred at Spice Jet as well.[58]

Erum Salam, "*cyber-attack forces shutdown of one of the US's largest pipelines",* The Guardian. The one of the largest pipelines of the US was shut down after an apparent cyber-attack took place on the infrastructure. The pipeline carries gasoline, diesel and jet fuel. Such a high-level attack on the critical infrastructure shows the nature of cyber criminals as they can reach the important infrastructure to cripple the economy on this note India is also on the verge where critical infrastructure can be attacked[59].

HT TECH, "59*% of Indian Adults fell prey to cybercrime in the past 12 Months",* Hindustan times. 7 out of 10 Indian adults, according to the report, think that remote working has made it simpler for hackers and cybercriminals to take advantage of them. Almost 59% of Indians were victims of cybercrime in the 12 months prior, according to the Norton Life Locks 2021 Norton Cyber Safety Insights research. Its conclusions are based on a survey of over 10,000 adults across ten nations, with 1000 participants from India.[60]

Zee News Tech, "cybercrimes *at its peak New techniques used for financial fraud",* Zee news. The economic offence wing claimed that following a digital transaction, hackers send fraudulent links to people in order to steal their phones and then force them to enter a one-time password that they use to empty their bank accounts.[61]

The Mint Tech, "*WhatsApp new privacy policy 'exploitative and exclusionary CCI orders detailed probe,"* Mint News. The Indian Competition Commission has directed its investigation arm to look into WhatsApp's amended privacy policy and terms and conditions, claiming that the company's exploitative and exclusionary behavior has violated competition law provisions. According to the regulators, a thorough investigation is needed to determine the actual degree, scope, and effect of data sharing through users' involuntary assent. WhatsApp

[58] Jitesh Vachhatani, "Air *India data of 45 lakh passengers including credit cards leaked in massive breach",* Republicworld , May 21, 2021 at 11: 23pm
[59] Erum Salam, "*cyber-attack forces shutdown of one of the US's largest pipelines",* The Guardian May 08 2021 at 1:03pm
[60] HT TECH, "59*% of Indian Adults fell prey to cybercrime in the past 12 Months",* Hindustan times 19April 2021 at 9:50am
[61] . Zee News Tech, "cybercrimes *at its peak New techniques used for financial fraud",* Zee news April 06 2021 at 11:23 pm

policy is that the users must accept in its entirety with respect of sharing information across all formats among Facebook companies.[62]

Bloomberg, "India *plans a new national strategy on cybersecurity amid china hacking concerns,"* Mint Tech. India is preparing to improve cybersecurity as the attacks on the Mumbai electric grid by the Chinese counterparts pose a serious issue for the vulnerable cybersecurity systems of India. This plan will coordinate with Home affairs, information technology and defense in case of an attack and set audit measures and same will be approved by the Prime minister Narendra modi. [63]

Money control News, "Government *operationalizes national helpline 155260 to combat cyber-crime losses",* Money control. The Government of India introduced national helpline number 155260, a reporting platform that will help prevent financial loss due to cyber fraud. A positive step towards cyber fraud still loses its impact as it is available in few states and not in India's financial hub. It is operational in the following states Chattisgarh, Delhi, MP, Rajasthan, UP, Telangana, and important cities are left in the lurch a positive step with lack in implementation[64].

HT TECH, *"Cyber threats in online education sector increased by 60% in 2020",* Hindustan times. The report from Kaspersky the educational sector continues to attract the attention of cyber criminals on the Internet. It was observed that 2,70,171 users encountered various threats on learning platforms during July to Dec 2020. And it was zoom the most popular software to lure users. Similarly google classroom google meet encountered the same.[65]

Express new service "Bank *swipe machines emerge as latest tool of fraud for cyber criminals in Mumbai",* The Indian Express. The Mumbai police arrested people who were involved in a cybercrime circle, wherein the accused would steal information from ATM kiosks, have counterfeit debit cards made, buy swipe machines from banks based on a fictitious

[62] The Mint Tech, "*Whatsapp new privacy policy 'exploitative and exclusionary CCI orders detailed probe",* Mint News 24 March 2021 10:50am
[63] Bloomberg, "India *plans a new national strategy on cybersecurity amid china hacking concerns",* Mint Tech 08 March 2021 09:54 am
[64] . Money control News, "Government *operationalizes national helpline 155260 to combat cyber-crime losses",* Money control June 17 2021 at 8:52 pm
[65] HT TECH, "Cyber threats in online education sector increased by 60% in 2020", Hindustan times 14 Feb 2021 at 5:46pm

company they had created to commit the crime, and transfer money into their own bank accounts. Using skimmers and tiny cameras, they have been stealing card information and pin numbers from ATM kiosks for the previous three months. They would use counterfeit cards to transfer funds into bank accounts by using a swiping machine. [66]

Suhasini Haidar, "*some states using cyberspace skill to execute cross border terror: Shringla,"* The Hindu. According to the report, India's cybersecurity skills are lacking. Before the UN Security Council, foreign secretary Harshvardhan Shringla stated that there were many concerns about the manipulation of ICT products by both state and non-state actors. A non-profit organisation called the International Institute of Strategic Studies conducts research. The IISS rated India as a third-tier cyber power that has concentrated its cyber intelligence and offensive capabilities too narrowly after evaluating 15 countries and finding that India's cyber security capabilities are deficient. The government said that there has been a 300% increase in cyberattacks from 3,94,499 in 2019 to 11,58,208 in 2020 in march, according to the Ministry of Home Affairs.[67]

Shubhajit Roy, "*India in Tier 3 as cyber power: IISS",* The Indian Express. India has reportedly made some headway towards developing its cyberspace security philosophy and policy. The International Institute of Strategic Studies qualitatively analyzed 15 nations with significant cyber capabilities (IISS). The seven categories in which a country's capability has been evaluated include strategy and doctrine, governance, command and control, core cyber intelligence capability, cyber empowerment and dependence, cyber security and resilience, global leadership in cyberspace affairs, and offensive cyber capability. India was assigned to the third tier for nations with significant weaknesses in some of these areas but potential strengths in others. The United States was the sole nation in the first tier; in the second tier, it was followed by China, France, Israel, Russia, and the United Kingdom; in the third tier, it was followed by India, Indonesia, Japan, and Malaysia; and in the fourth tier, it was followed by India, Indonesia, Japan, and Malaysia. The study finds that India has been working on institutional reform of cyber governance over a long period of time and gradually, with the

[66] Express new service "Bank *swipe machines emerge as latest tool of fraud for cyber criminals in Mumbai",* The Indian Express June 25, 2021 at 7:04 am
[67] Suhasini Haidar, "*some states using cyberspace skill to execute cross border terror: Shringla",* The Hindu 29 June 2021 at 8:00 pm Indian standard time.

establishment of key coordinating authorities for cyber security in the civil and military domains only in 2018 and 2019.[68]

Sarthak Dogra, "*Data of over 700 million LinkedIn users exposed, it includes numbers, addresses and salary details",* India Today. User names, email addresses, phone numbers, and physical addresses were purportedly compromised due to a cyberattack on LinkedIn, and the following data is now for sale on the dark web. The hacker advertised the following data, which was accurate and current from 2020 to 2021. The data points are nonetheless very useful even though no passwords have been exposed since they can be used to further internet phishing scams that impersonate other people. LinkedIn admitted the intrusion, but claimed that publicly available profile data was really taken from LinkedIn.[69]

Deccan Herald, "*India 2nd biggest target of cyber criminals in Asia Pacific in 2020: IBM",* Deccan Herald news. According to IBM's research, after Japan, India would be Asia's second most targeted country by cyber criminals in 2020. Hospitals, medical and pharmaceutical firms, as well as energy companies that support the covid 19 supply chain were among the targets of the attackers. Other companies targeted included businesses that depend substantially on global covid 19 response operations and, most importantly, financing companies and insurance most attacked in the country in India followed by manufacturing and professional services.[70]

India Tv, "*SBI OTP scam: Chinese hackers targeting state bank of India users offering free gifts,"* India Tv News. According to the research, hackers are sending out WhatsApp messages to individuals encouraging them to update their KYC via a certain website link in exchange for free presents from the bank valued at Rs. 50 lakhs. Cyber peace and autoboT research wing studied the incidents smartphones users faced. The link which is provided by the cybercriminals redirects the users to the page of sbi which the genuine website of SBI is not and then it asks to enter sensitive information such as account number password captcha and it sends an otp which the hackers itself provide and it causes amount to be debited from the sbi customers.[71]

---

[68] Shubhajit Roy, "*India in Tier 3 as cyberpower : IISS",* The Indian Express June 28 2021 at 7:20 am
[69] Sarthak Dogra, "*Data of over 700 million LinkedIn users exposed, it includes numbers, addresses and salary details",* India Today June 29 2021 at 12:25 pm
[70] Deccan Herald, "*India 2nd biggest target of cyber criminals in Asia Pacific in 2020: IBM",* Deccan Herald news February 24 2021 11;42pm
[71] . India Tv, "*SBI OTP scam: Chinese hackers targeting state bank of India users offering free gifts",* India Tv News, July 08 2021 at 12:08 Pm

Neeti Gupta, "*Freedom of speech Restored- 66A of IT act Struck down"* Indian Journal of Applied Research. The following case commentary on Shreya Singhal vs Union of India constituted a landmark Indian judgement. The IT Act, Section 66A, provides of the arrest of a person for uploading offensive content. on websites as unconstitutional. This was very important as many were on this section and this section violated the freedom of speech granted by the constitution of India. The court termed the section vague and supreme court heavily relied on foreign judgements delve deeper into the impact and content of free speech.[72]

Babak Akhgar et al. "*combatting cyber-crime and cyber terrorism challenges, trends and priorities"* Springer, Advanced Sciences and Technologies for Security Applications /10.1007/978-3-319-38930-1/ ISSN 2363-9466. The following book covered the aspects the challenges of cyber-crime and and cyber terrorism its trends and challenges, and it was brought upon that it is huge concern not only to nation but to the whole world in general. And combatting the cybercrime and cyber terrorism requires different actions and in policy and research, strategies involving a number of pathways are used. The real challenge, and the most daunting of all, is to bring these disparate actions together into a coherent whole, based on a vision that considers current trends and strives not just for individual policy measures and short-term research projects, but for long-term solutions to the challenges of cyber-crime and cyber terrorism.[73]

Kenneth J Knapp, "*Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions*" Information Science Reference / 978-1-60566-326-5 / 978-1-60566-327-2. This book is useful because it discusses the most important global and national cyber security issues. Risk and threat assessment, organizational and human security, emergency response planning, and security technologies are the keys to combating cyber security nationally. The following issues must be resolved to level the playing field for all sectors, i.e. mentioned must be covered to stop cybercrime.[74]

[72] Neeti Gupta, "*Freedom of speech Restored- 66A of IT act Struck down"* Indian Journal of Applied Research ISSN NO 2249-555X, vol 5 issue 05th May 2015.
[73] Babak Akhgar et al. *combatting cyber-crime and cyber terrorism challenges, trends and priorities* 45 (Springer, Advanced Sciences and Technologies for Security Applications /10.1007/978-3-319-38930-1/ ISSN 2363-9466)
[74] Kenneth J Knapp, *Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions* 11 (Information Science Reference / 978-1-60566-326-5 / 978-1-60566-327-2)

Suvarna shirke et al. "*cyber security and laws*" Tech knowledge publications, 2019, Mumbai. The book provided information on cybercrime and its impact on the outside world, how to use information security standards compliance during software design and development, and how to interpret the IT Act and its implications in legal concerns. It was a basic over view of all the aspects mentioned. The author failed to touch upon the aspects of cyber terrorism, the growing nature of cyber-crime, recent trends, and technological development.[75]

Henry Prunckun, "cyber *weaponry issue and implications of digital arms*" Advanced Sciences and Technologies for Security Applications, Springer, 978-3-319-74107-9, 10.1007/978-3-319-74107-9. The book gave the background how the computers are weaponized by software approach and hardware approach, The owner does not want a software program that, when run, performs an activity. Programs or components of larger programs that allow damaging tasks to be carried out. The electronic device is used to harm the computer via the hardware method. It's wired into a computer's circuit and records mechanical input from computer keyboards. A software application is weaponized when written to accomplish a destructive function. The system has been weaponized when software and hardware are configured to work in tandem to carry out destructive actions. The following aspects are used by cyber criminals in day to day functioning to overcome the unaware citizens and cause harm.[76]

Amos N Guiora, "*cyber security -Geopolitics, law and policy*," Routledge 2017, 978-1-498-72911-6. The book covers the legal and policy issues of cyber security, as well as taking a much broader geopolitical view of cyber security. It included perspectives from corporations, law enforcement, political considerations, regulatory authorities, and citizens' knowledge of the complicated nature of cyber security. This made the understanding at same footing and why it is important to know the cyber security measures are needed to be dealt with top most priority by all the nations[77].

[75] Suvarna shirke et al. "cyber security and laws" Tech knowledge publications, 2019, Mumbai.
[76] Henry Prunckun, *Cyber weaponry issue and implications of digital arms* 120 (Advanced Sciences and Technologies for Security Applications, Springer, 978-3-319-74107-9, 10.1007/978-3-319-74107-9)
[77] Amos N Guiora, *Cyber security -Geopolitics, law and policy* 65 (Routledge 2017, 978-1-498-72911-6)

Indian Express, "*Pegasus: Panel to probe spying charges submits its report to SC", Bloombergquint.* Pegasus row in India reached the supreme court, the apex court of India, the SC appointed a committee to look into the row of states using Pegasus software and the committee submitted its report to the supreme court. There were strong indicators as the states were using Pegasus software for surveillance on the officials of the states[78].

Express News, "Mumbai*: 64-year-old actress falls for Airtel KYC cyber-fraud, loses Rs 1.48 lakh"* Indian Express. A Marathi actress aged 64yr lost 1.48 lakhs just by sharing the details of her card, a sms was sent by the cyber criminals posing as telecom operator and asked for her details. The fraudster asked for the KYC details and asked her to pay Rs.10 as KYC charges and similarly the cyber-criminal used the credentials entered by the lady and used to withdraw the following amount. Literacy regarding usage of debit and credit details among the generation of 60s are lacking they find it very difficult to differentiate among the fraudster and relevant officials[79].

Money control news, "Cyber-*attacks on Indian oil companies run up to 3.6 lakhs in six months"* Money control. The cyber criminals attacked Indian oil companies that come under the critical infrastructure of any country in the last six months; this study was conducted by the cyber peace foundation. The most recent attack was on the oil India limited Assam a ransom note demanding of Rs. 57 crores from the company[80]

.

Hindustan times, "*Cyber fraud case: Arrest of WB man exposes ₹3,000 cr online job racket",* Lucknow News, HT. This report on the cyber fraud is gaining importance among the state officials in west Bengal. A arrest of man in relation to cyber fraud in Bareilly he was caught in west Bengal exposed a 3,000 cr job racked scam which is going around in India. The incident of Bareilly case, the victim received a message of online part-time job and was directed to a WhatsApp number and, thereafter, to an app when she clicked on a given link[81].

[78] https://indianexpress.com/article/india/pegasus-panel-to-probe-spying-charges-submits-its-report-to-sc

[79] https://indianexpress.com/article/cities/mumbai/mumbai-64-year-old-actress-falls-for-airtel-kyc-cyber-fraud-loses-rs-1-48-lakh

[80] https://www.moneycontrol.com/news/technology/indian-oil-companies-suffered-3-6-lakh-cyberattacks-in-six-months

[81] https://www.hindustantimes.com/cities/lucknow-news/cyber-fraud-case-arrest-of-wb-man-exposes-3-000-cr-online-job-racket

Shivani Shinde, "*Hackers steal Rs 7.3 cr in 831 transactions over three months from Razorpay*", Business Standard, May 21, 2022 at 8:46pm. Hackers stole Rs 7.3 crore in 831 transactions over three months, according to online payment provider Razor pay. The scam was discovered during an examination of the company's transactions. "During a routine payment process, an unauthorized actor(s) with malicious intent used the browser to tamper with authorization data on a few merchant sites that were using an older version of Razor pay's integration, due to gaps in their payment verification process," according to a Razor pay spokesperson. The razor pay incident is new to payment gateway method by the cyber criminals[82].

Syed Omar, "*Hacker's prey on coop banks with cheap security software: Police*" Deccan Chronicle, May 05, 2022 at 9:00pm. The co-operative banks are vulnerable to the cyber criminals because they lack updated software, giving them an upper hand to beat the banks. Cyber security software which the cooperative banks are lacking and most of the cooperative on the LAN so it gives cyber criminals to hack the system and transfer money as per there convenience[83].

Abhishek chaudhari, "*Digital payment frauds will continue unless second half of process is streamlined"*, Times of India, June 12, 2022. The following article in times of India by cyber expert Mahendra Limaye pointed out the struggle of cops as how difficult is to catch the cyber criminals as the process involved is tedious and challenging as information is to be shared at different stages of the process state officials, private bodies. The second half of the process as pointed out by cyber expert suggested that the money can be retrieved if its lying in the criminals account[84].

DC, "*Cyber fraud, cloned fingerprints: 7 arrested for fraudulent withdrawal of Rs 14L*", Deccan Chronicle, June 16, 2022. This report by deccan chronicle in Hyderabad unearthed the new way of cyber-crime, cyber criminals used documents accessed from the AP registration and stamps department's official website, IGRS (inspector General, Registration and Stamps),

---

[82] https://www.business-standard.com/article/companies/hackers-steal-rs-7-3-cr-in-831-transactions-over-three-months-from-razorpay

[83] https://www.deccanchronicle.com/nation/crime/050522/hackers-prey-on-coop-banks-with-cheap-security-software-police

[84] https://timesofindia.indiatimes.com/city/nagpur/digital-payment-frauds-will-continue-unless-second-half-of-process-is-streamlined

to fraudulently withdraw a total of Rs 14.64 lakh from 149 customers. A gang of seven has been busted. They did the crime by cloning their fingerprints, said the cybercrimes police of Cyberabad here on Thursday. "They obtained the AEPS (Aadhaar Enabled Payment System) licence to access digital payments using the information obtained from IGRS portal," an official said. The mastermind, downloaded land registration documents from the official website of registration and stamps department of the AP government. He captured fingerprints and took customer service points using forged documents to withdraw funds from banks using cloned fingerprints, police explained. Explaining the modus operandi, Cyberabad police commissioner Stephen Raveendra said that the fraudsters had vast experience in the banking, lands and registration fields. By noticing the vulnerabilities in the IGRS Portal of AP, they had downloaded the state's land registration documents. "From the website, they collected the name, Aadhaar number and fingerprints of customers, with which they prepared polymer fingerprints using chemicals. After preparing the fingerprints, they registered with AEPS applications and used it to go to the linked bank accounts and find their balance. E-Point India applications were used for withdrawing the amounts using the prepared polymer fingerprints. In this way, they prepared more than 10,000 fake fingerprints," explained the commissioner[85].

Jignasa Sinha, "*New headache for cops: Cyber criminals buying personal data in bulk*", Indian Express, June 26, 2022. This report from Indian express how data is being sold for mere 600 to 7000rupees. The methods adopted as many might be aware your account is suspended, complete your kyc, your loan amount is due, lookalike websites, such messages are sent in bulk so that people start filling the link and data is generated by just one click. They mostly target senior citizens, retired officials and frequent shoppers. Data of these people are easily available on the websites[86].

NB Gupta, "Accounts of Bank in Thane hacked, 2.59 cr Stolen", Hindustan times, 28 June 2022 at 9am. The server of a private bank based in Thane and Palghar district was hacked into by some unknown hackers and ₹2.59Cr stolen from several accounts. The bank employees at the head office realized that there was a glitch in their online transactions that had stopped

[85] https://www.deccanchronicle.com/amp/nation/crime/160622/cyber-fraud-cloned-fingerprints-7-arrested-for-fraudulent-withdrawal

[86] https://indianexpress.com/article/cities/delhi/new-headache-for-cops-cyber-criminals-buying-personal-data-in-bulk

for a few days, police said. Such instances where bank also is not aware of glitches in their system can cause huge losses at one click of cyber criminals[87].

Shruti kakkar, "Cybersecurity In India Hasn't Received The Attention It Deserves': Plea In Supreme Court Seeks Guidelines To Combat Hacking, Cyber Crimes, Data Theft", Solegal , 17 Nov, 2021 at 8am. The Supreme Court recently adjourned the writ petition which sought for formulation of new guidelines to combat hacking, cyber-crimes, data theft and allied issues. The bench of Justices AM Khanwilkar and CT Ravikumar directed Advocate Vivek Narayan Sharma appearing for the petitioner to serve an advance copy of the petition to Centre's (Ministry of Electronics and Information Technology) Standing Counsel. The petition had sought for guidelines for creation of:

- Toll-free complaint and redressal centres for social media hacks, cyber-crimes and data breach cases.
- New posts in cyber cells.
- Filling cyber cells with technical experts at the district level in every State.
- A temporary body with extensive powers to look into data breaches and redressal.
- Data Protection Rights and Cyber Security measures which would strengthen public trust.
- It was argued that lack of a central authority or a central body with pan-India jurisdiction to tackle cases created huge bottlenecks for the smooth operation of cyber cells[88].

- Bhaswati Guha, "High-Level Probe Against Army Officials Over Cyber Security Breach on WhatsApp", India Today Group, 20 April 2022, 15:03Ist**.** India's military and intelligence services discovered a cybersecurity compromise involving military officials that may be linked to espionage-related actions by a neighboring country. According to reports, defence sources have revealed that "the breach has been reported on certain WhatsApp groups". The action is reportedly being taken against the officials who are accused of wrongdoing. As reported, an investigation is underway. Military officers who violate current instructions, especially involving counterintelligence, are dealt with harshly, under the Official Secrets Act. It was also reported that officials found guilty will face the worst punishment

[87] https://www.hindustantimes.com/cities/mumbai-news/accounts-of-bank-in-thane-hacked-2-59cr-stolen
[88] https://www.soolegal.com/news/cybersecurity-india-received-sc-hacking-cyber-crimes-data

conceivable. The following critical infrastructure is vulnerable to cyber criminals' loss of important data to neighboring countries would be huge drawback for countries like India[89].

Dr. Swapnil Choudhary," *AI and Cyber Security with Reference to Information Technology Act, 2000 and other Laws in India*", International Journal for Research in Applied Science and Engineering Technology,2024. The term artificial intelligence (AI) is prominent in today's world of technology. In so many ways, it is still a developing science considering the problems presented by the twenty-first century. AI use has been established in daily life. Since AI has such a significant influence on human existence now, it is difficult to comprehend a world without it. Simply define, artificial intelligence (AI) is the study of how people think, work, learn, and decide in every situation in life, whether it is connected to problem-solving, learning something new, thinking logically, or coming up with a solution, etc. If Artificial Intelligence mostly connected with the daily life of the human being it must be protecting the relationship between the human being and society people and there should be remedy to the peoples in case of violation of laws by AI machines. Cyber security and cyber law already new concept in the development of modern laws of the country. Cybercrimes are becoming common and frequently reported in the news. It is a global challenge, not simply one that affects one nation. AI is meaningless without strong security measures since it may be readily accessible by outsiders. Governments, banks, and global corporations now face a serious threat because of cyber security threats. Hackers use a lot of private and business data to their advantage, which poses a serious threat to the online community[90].

Rishav Upadhyay, Pratiksha Bharadwaj, "*Legal Framework of E-Commerce*", International Journal for Multidisciplinary Research, 2024, The research article titled "E-Commerce Framework for Consumers' Protection from E-Commerce Fraud" by Mayank Yadav, published in the Jus Corpus Law Journal in 2022, addresses the burgeoning impact of e-commerce on consumer behavior and the legal framework in India. It emphasizes the transformative effect of e-commerce on Indian consumers' habits and business practices, highlighting its role in facilitating digital transactions, online shopping, and electronic payments. The article underscores the importance of understanding the legal complexities surrounding e-commerce to support the growth of the digital economy. Researcher asserts that

[89] https://www.news18.com/news/india/high-level-probe-against-army-officials-over-cyber-security-breach-on-whatsapp
[90] https://doi.org/10.22214/ijraset.2024.58030

e-commerce encompasses a wide range of activities conducted electronically, primarily through the internet, including transactions, purchasing, and commercial operations. It emphasizes the global reach of e-commerce, enabling businesses to access international markets and providing customers with a plethora of goods and services. The article stresses the crucial role of e-commerce in entrepreneurship, economic development, and enhancing customer experiences[91].

Sanjay Mulik, Sachin Sunil Paralkar, "*A Protection of Privacy and Data under India's Legal Regime*", International Journal for Multidisciplinary Research,2024. The research article discusses the importance of privacy as a fundamental right, recognized globally and in India under Article 21 of the Indian Constitution. It highlights the challenges of protecting privacy rights in a technologically advanced and globalized world, where data privacy has become increasingly difficult to achieve. Initially, privacy rights in India were not explicitly recognized as fundamental, and there was no specific legislation addressing data protection. However, there have been numerous cases of privacy rights violations by both government authorities and private entities. Courts have played a significant role in addressing these violations through landmark decisions and rulings. The article emphasizes the need to analyze the legal developments concerning the right to privacy and data protection in India. While some steps have been taken to prevent data theft and misuse, there is still room for improvement in enhancing data protection measures to secure the privacy rights of Indian citizens. Overall, the research concludes that while the Indian legal system has recognized the importance of the right to privacy, further progress is needed to strengthen data protection laws and safeguard citizens' privacy in the modern era[92].

Md. Asaad Raza, "*Cyber Security and Data Privacy in the Era of E-Governance*", Social Science Journal for Advanced Research, 2024, The research article explores e-Governance, which utilizes information and communication technologies (ICTs) to enhance government-citizen relations. It highlights cyber security and data privacy as major challenges in e-Governance implementation. Cyber security refers to protecting information communicated through computing devices, while data privacy concerns the proper handling of sensitive information shared with others. To achieve good governance through e-Governance, the article

[91] https://doi.org/10.36948/ijfmr.2024.v06i01.9715
[92] https://doi.org/10.36948/ijfmr.2024.v06i01.11109

emphasizes the importance of information security best practices and protecting data against cyber-attacks. It suggests the need for national and international frameworks to address concerns related to e-Governance and advocates for the implementation of existing laws to address cyber security issues. The paper delves into factors related to cyber security and data privacy for e-Governance, including administration and enforcement processes, legal frameworks, and national and international considerations. Overall, it underscores the critical role of addressing cyber security and data privacy concerns to ensure effective e-Governance implementation[93].

Akinul Islam Jony, Sultanul Arifeen Hamim, "*Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age*", Journal of Information Technology and Cyber Security,2024. The research article provides a comprehensive review of cybersecurity in the modern digital age, emphasizing the critical importance of robust cybersecurity measures in the face of evolving threats. It highlights various types of cyber-attacks, including phishing, malware, Denial of Service (DoS), Distributed Denial of Service (DDoS), Zero-Day Exploits, Man-in-the-Middle, and SQL Injection Attacks. The article systematically categorizes these cyber threats, examines their unique characteristics, and explains their modus operandi. It delves into the methods and motivations of cybercriminals while evaluating the effectiveness of countermeasures against these attacks. Overall, the review offers essential insights into securing our digital future amidst increasing interconnectivity and technological dependence, providing valuable information for individuals and organizations seeking to mitigate cybersecurity risks[94].

Farheen Zehra, F. S. Khan, S. Mazhar, "*Scanning the surging Indian digital payment gateways through peer-to-peer (P2P) applications and challenges: A literature review*", Journal of Statistics & Management Systems, 2024. The research article conducts a systematic literature review (SLR) to analyze the rapid growth of digital payment gateways in India, particularly driven by peer-to-peer (P2P) applications. The study highlights the need to understand the implications of this growth for various stakeholders, including businesses, consumers, and the economy. Its primary aim is to comprehensively examine existing research to identify factors driving the surge of P2P payment gateways in India. The methodology

[93] https://doi.org/10.54741/ssjar.4.1.2

[94] https://doi.org/10.30996/jitcs.9715

involves thorough search and selection of relevant studies from academic databases, peer-reviewed journals, and conference proceedings. Selected studies are critically analyzed to identify key themes, patterns, and trends in the literature. The findings are expected to shed light on factors contributing to the growth of P2P payment gateways, their impact on the Indian economy, including effects on traditional banking, e-commerce, digital transactions, employment opportunities, and financial inclusion. Implications of the findings are discussed, providing recommendations for policymakers, practitioners, and researchers. Additionally, the review identifies research gaps and potential future directions, including the adoption of Blockchain technology, integration with emerging technologies, cross-border payments, enhanced security measures, and the impact of COVID-19 on digital payment gateways. The novelty of the SLR lies in its comprehensive analysis of the surging Indian digital payment gateways through P2P applications, aiming to provide a valuable resource for understanding the evolving landscape of digital payments in India[95].

Kheelesh Kumar Dewangan et.al, "*Cyber Threats and Its Mitigation to Intelligent Transportation System*", SAE technical paper series, 2024. The research article examines the susceptibility of intelligent transportation systems (ITS) to cyber threats in the context of modern transportation advancements. It emphasizes the need to address potential vulnerabilities and mitigate risks associated with connectivity, automation, and data-driven decision-making in ITS. The paper explores various cyber threats targeting ITS, including unauthorized access, malware and ransomware attacks, data breaches, denial of service, and physical infrastructure attacks. It underscores the potential consequences of these attacks, such as disruptions to critical transportation infrastructure, compromise of user safety, and economic losses affecting various services within ITS. Additionally, the article discusses innovative approaches adopted by cybersecurity professionals to secure ITS operations, including the use of Blockchain, artificial intelligence, and machine learning. It highlights the role of 5G technology in enhancing these approaches by providing high-reliability connectivity and low-latency communication for real-time security in ITS, particularly in secured vehicle-to-everything (V2X) communication. The article also reviews current security practices for ITS and evaluates upcoming technologies for practical implementation in the field. By understanding cyber threats targeting ITS and implementing appropriate safeguards,

[95] https://doi.org/10.47974/jsms-1198

stakeholders can enhance the resilience and security of these systems, ensuring safe and efficient transportation in the digital age[96].

Neha Kumari et.al, *Digital Citizenship Education in Higher Education: A Study in Indian Perspective",* Journal of Higher Education Theory and Practice, 2024. The research article focuses on the transformation of higher education in India due to technological advancements, particularly the integration of technology and innovation into the learning process. It highlights the importance of digital citizenship education in preparing students to become responsible and informed digital citizens in this digital era. The study aims to examine technological innovation in higher education in India, with a specific focus on digital citizenship education, and to analyze factors influencing its integration. It seeks to provide insights into the challenges and opportunities related to the implementation of digital citizenship education in Indian universities and make recommendations for its effective integration into the higher education curriculum. Overall, the article underscores the significance of digital citizenship education in higher education and emphasizes the need to understand and address factors affecting its integration into the curriculum to better prepare students for the digital world[97].

D. Jain, "*Regulation of Digital Healthcare in India: Ethical and Legal Challenges*", Healthcare, 2023. The research article examines the surge in interest and investment in digital healthcare amid the COVID-19 pandemic, particularly focusing on telemedicine. It highlights the World Health Organization's guidelines for implementing telemedicine on a large scale to improve healthcare access and protect against the spread of COVID-19. In the context of India, the article identifies several implementation challenges for digital healthcare, including the absence of explicit laws regulating telehealth and inadequate data protection laws to manage the vast amount of data generated. There are also concerns regarding patient privacy and informed consent in the digital healthcare landscape. The paper analyzes the legal, structural, and ethical issues surrounding digital health in India and discusses the implications of these shortcomings. Furthermore, it offers policy recommendations to address these challenges, aiming to enhance the effectiveness and ethical integrity of digital healthcare implementation in the country[98].

[96] https://doi.org/10.4271/2024-26-0184

[97] https://doi.org/10.33423/jhetp.v23i20.6693

[98] https://doi.org/10.3390/healthcare11060911

Widya Setiabudi Sumadinata, "*Cybercrime and Global Security Threats: A Challenge in International Law*", Russian Law Journal, 2023. The research article explores the challenges associated with combating cyber-crimes and global security threats from the perspective of international law. It underscores the increasing prevalence of cyber-crimes in the digital age and the significant impact they have on both national and international levels. The study employs a descriptive-analytical approach, analyzing regulations, policies, and literature from reputable sources at both international and national levels. The research findings emphasize that addressing cyber-crimes and global security threats requires robust international cooperation and effective law enforcement mechanisms. It concludes that individual countries cannot tackle these challenges alone and stresses the importance of harmonizing international law to combat cyber-crimes effectively. The article highlights the necessity of international collaboration, particularly in the fields of information and technology, to enhance cybersecurity measures globally[99].

M. Syahril, "*Cyber Crime in terms of the Human Rights Perspective*", International Journal of Multicultural and Multi religious Understanding, 2023. The research article examines the handling of cybercrime in the City of Parepare, Indonesia, within the context of human rights recognition and protection, guided by the philosophical foundation of Pancasila. It emphasizes the importance of aligning regulatory efforts with legal ideals to effectively address cybercrime. The study utilizes both normative and empirical methods to assess the extent of cybercrime handling in Parepare. Findings reveal that cybercrime, constituting a violation of human rights, remains prevalent in the city despite regulatory measures. The handling process is deemed ineffective due to the lack of deterrence for perpetrators, stemming from inadequacies in existing regulations. In summary, the article underscores the need for stronger regulatory frameworks and enforcement mechanisms to combat cybercrime effectively in Parepare. It emphasizes the imperative of aligning legal ideals with practical implementation to protect human rights and mitigate cyber threats effectively[100].

Chandra sekhar, M. Kumar, "*An Overview of Cyber Security in Digital Banking Sector*", East Asian Journal of Multidisciplinary Research, 2023. The research article examines the increasing prevalence of cybercrime in the banking sector despite advancements in online

[99] https://doi.org/10.52783/rlj.v11i3.1112
[100] https://doi.org/10.18415/ijmmu.v10i5.4611

technology. It highlights that digital banking, including services like NEFT, Google Pay, and PhonePe, is widely used, but cybercrime related to ATM, debit card, and net banking accounts for a significant portion of cybercrime incidents, accounting for approximately 50%.

The paper emphasizes that the banking sector faces more frequent cyber-attacks compared to other industries. It explores various cyber-attacks targeting the banking sector and proposes strategies for enhancing cybersecurity to mitigate these threats effectively. Overall, the article underscores the importance of addressing cyber threats in the banking sector and offers insights into ways to bolster cybersecurity measures to protect financial institutions and their customers from cybercrime[101].

1.4 SCOPE AND SIGNIFICANCE OF THE STUDY

The following research will cover the historical background of cyber laws in India[102], their various types, and their impact on society. The researcher will incorporate the national legal framework for protecting and controlling cybercrimes and how "the Information Technology Act, 2000" deals with the cyber-crime and protection[103]. The study will cover the judicial perspective in relation to cyber security in India and how the judiciary is looking at the cybercrime and cybersecurity in India. A comparative study of legislative framework of cybercrimes in USA, Isreal and India this will help in gaining the methods incorporated by these top countries for curbing cybercrime and implementation of cyber security mechanism in the nation the following comparative study will be done with the help of secondary sources. With the aid of a survey and in-person interviews with cyber professionals, the researcher try to get the insights on the cybercrime and cyber security on the financial sector in Mumbai. The empirical research will be conducted in Mumbai with questionnaire will be distributed to 500 advocates to gain insights on the cyber laws and what all could be amended in the current scenario and personal interview of 30 cyber experts will give the important methods and system to be adopted for controlling cybercrimes in Mumbai and cybersecurity mechanism also will be discussed with the cyber experts.

1.5 RESEARCH GAP

[101] https://doi.org/10.55927/eajmr.v2i1.1671
[102] Gaur, L. (2022). Evolution of Cyber Laws in India. *Jus Corpus LJ*, *3*, 670.
[103] Maneela. (2014). Cyber Crimes: The Indian Legal Scenario. US-China L. Rev., 11, 570.

The financial sector is at huge risk as most of the times it is attacked by the phishing method, it is the most used method by cybercriminals to do the crime. And how to stop the cyber phishing is missing in many research papers and books (Acharya suman et al. 2020). The banking sector is attacked at a greater pace the usage of internet banking through mobiles is increasing day by day. Mobiles are easily targeted by the cybercriminals as it doesn't have any cyber security mechanism to stop the hacking. New laws should be brought into place to look into the cyber-crimes relating to mobile banking or a separate law would be the key (Harshita Singh Roa 2019). The privacy law in India is also need to be covered as most of the research failed to throw on the privacy law (Anam Ajmal 2020). The cyber security policy should be looked as the top most priority as India needs a Robust cyber security policy to cater the cyber-crimes in the coming times (Bharat Panchal chief Risk officer 2021).

The financial cyber-crimes in relating to bitcoins, magecarting (stealing data from e commerce) are new financial crimes in the cyber world which is untouched and such crimes needs to be covered at the earliest (carin smith 2021). Personal data protection bill should be brought into the nation with looking at the future not the present (Chandra Shrikant 2021). The critical infrastructure of our nation should be brought under one umbrella so that the cyber criminals cannot the breach the critical infrastructure of the nation as it the base of the all the crimes. Awareness of cyber-crimes among the society is left untouched as people are unaware that what is cyber-crime and how it is done by the cyber criminals. The Cyber terrorism is also gaining impetus and people are brainwashed on the cyber world this had led to the growth of terrorism on the cyber world and giving upper hand to the cyber criminals to recruit individuals for the wrong purposes.

1.6 OBJECTIVES OF THE STUDY

The research topic is related to Cybercrime and Cyber laws in India: A Study with Special Reference to Financial Sector in Mumbai, on this basis our objectives of research are as follows. The Objectives of the study are the following:

1. To study the Historical background of cyber law in India.
2. To evaluate the different types of cybercrimes in India.
3. To study legislative framework governing cybersecurity in India.
4. To evaluate the Judicial Perspective towards protection & Prevention of cybercrime.

5. To make comparative study of International legislative framework of Usa, Israel and India.
6. To study the emerging nature of cybercrime in the financial sector.
7. To analyse how cybercrimes affects the financial sector in relation to Mumbai.
8. To provide suitable suggestions in the financial sector for cyber security and in the legal regulatory framework.

   The first four objectives of the research will be covered through Doctrinal research and The latter part will be covered through empirical research.

1.7. CHAPTERISATION

The following chapters are framed for the present research.

Chapter One, titled as *'Introduction'* enunciates upon the titular introduction of the present research wherein the researcher attempts to discuss the problems addressed. The researcher also highlights definition, concept, recent trends, scope & need of cyber-crime and cyber laws in India and present the research design of the thesis comprising of the literature review, objectives, hypothesis and the research methodology of the study.

Chapter Two, titled as *'Cybercrime: Historical Background, Its Types & Challenges to The Society'* talks about the cyber-crime and its challenges to the society such as financial & social. It also discusses the various types of cyber-crime such as phishing, malware, identity theft, email bombing etc. these crimes are grave threat to the society.

Chapter Three, titled as *'Legal Framework Governing Cyber Security in India',* the following chapter discusses about what is cyber security, history of cyber security in India, challenges in cyber security in India which is an evolving concern for the national security of India. The cyber security framework in India and relevant laws of cyber security which caters the cyber security structure in India.

Chapter Four, titled as *'The Judicial Perspective Towards Protection and Prevention of Cybercrime',* endeavor to study the cyber laws and cyber-crimes its judicial perspective, the major acts which got amended after the enactment of Information Technology act, landmark

cyber law cases in India which became precedents in the coming years and lastly the judicial remedies for protection of cyber-crime.

Chapter Five, titled as *'International Legislative Framework of Cyber Crimes: A Comparative Study of Usa, Israel, And India',* discusses about the role of international conventions in relation to cybercrime, various international and national treatises, protocol concerning cyberspace. It discusses the legislative framework of India, legislative framework of Israel and legislative framework of USA and analysis of all these three countries for better application of legislative framework to combat cyber crime and frame cyber laws in India.

Chapter Six, titled as '*Cybercrime- An Emerging Threat to The Financial Sector',* it focuses on introduction and overview of internet banking sector in India, the legal structure of e-banking in India, Data protection bill- Need of the hour in India, prominent cybercrime in the financial sector, impact of cyber-crime on the financial sector, cyber security in the financial sector, biggest threats to a bank security, approaches to deal with cybercrime related financial loss.

Chapter Seven, titled as '*Cybercrimes in The Financial Sector in Mumbai: An Empirical Study',* highlights the empirical research conducted by the researcher and discusses the finding of the research through questionnaire's distributed to advocates, law faculties, professionals, general respondents and personal interviews of cyber experts and police personnel. The hypothesis has also been tested in this chapter. The empirical data provides through the research provides a clear picture of how much impact the cyber-crime is having on the financial sector and as well on the society.

Chapter Eight, titled as '*Conclusions, and Suggestion',* discusses about the conclusive remarks concerning the various aspects of the research. The suggestions have been outlined by the researcher under categories, namely the legislative suggestions, implementation suggestion, financial suggestions and miscellaneous suggestions.

1.8 HYPOTHESES

The researcher hypothesises the following, based on the present study:

- The Information Technology Act is inadequate to tackle cybercrimes. In spite of the existing laws, there is still space for formulating provisions and making necessary amendments to combat the menace of cybercrimes.
- The current cyber security mechanism in India cannot cater to the fast pace of developing technology at the hands of cyber criminals, which could hit the critical infrastructure of India, such as the defense sector, financial sector, the grid lines, and corporations.

1.9 RESEARCH QUESTIONS

The research questions drawn by the researcher are as follows:

- Whether the current Information Technology Act, 2000 is sufficient to tackle the rising the cyber-crimes in India?
- What is the present scenario of cyber-crime in India specially in Mumbai in relation to financial sector in Mumbai?
- What is the legislative framework of different countries in relation to cyber-crime and cyber laws?
- Whether the India have the required cyber security framework to combat the rising the cyber-crimes on daily basis?
- Why it is important to bring new laws in relation to critical infrastructure, cyber security and data protection?

1.10 RESEARCH METHODOLOGY

In view of the above topic relating to cybercrimes and cyber laws in India: a study with special reference to financial sector in Mumbai. The current research is both analytical and empirical in nature. This study primarily uses the doctrinal research approach to compile, organize, interpret, and systematize primary and secondary source material. Both primary and secondary sources were employed by the researcher. For the purpose of gathering literature and data for the study and analysis, the researcher collects secondary data from published sources such as books, Indian and international journals, online journals, newspapers, online newspapers, research articles, and numerous websites on the subject. In this study, the

researcher used the empirical research technique to gather and generalize information from various respondents on the subject at hand. The primary data is collected from the selected general respondents, law faculties, advocates, financial sector employees through questionnaires and personal interviews of 10 cyber experts, personal interviews of 10 police personnel of Mumbai/Maharashtra. The primary data collected from the respondents were also used to prove or disprove the research hypothesis in this study.

1.11 METHOD OF DATA COLLECTION

1. In this instance, the researcher used the empirical research technique to gather data from a wide range of respondents on the study's topic and generalise it. The selected lawyers, cyber experts, police officers, law faculty members, general responders, and financial sector employees from Mumbai, Maharashtra, are the subjects of the primary data collection.
2. In this study, Questionnaire and Personal Interview methods have been used to get the results. An attempt has been made to analyse the views of the legal fraternity and cyber experts through an empirical study on the subject at hand. Questionnaires have been framed for the legal fraternity, law faculties, financial sector employees and general respondents, and personal interviews for cyber experts and police personnel to gain insights and opinions covering cybercrimes and cyber laws.
3. The universe for data collection is Mumbai, the hub of cybercrimes in India, as cases are seen daily. The respondents are financial sector employees -50, law faculties- 50, Cyber experts - 10, Police Personnel – 10, Lawyers - 50, and general respondents 100. The questionnaire contains both open-ended and close-ended questions.
4. The empirical part of the study involved an in-depth analysis of the responses given by the respondents through various questionnaires and personal interviews taken of cyber experts and police personnel. The General Respondents Annexure 1, the ordinary citizens, were selected for the research to understand their experiences and how often they are victims of cybercrime, especially the financial fraud that citizens mostly face.

Data Collection	**General Respondent**	**Cyber Experts**	**Law Faculties**	**Financial Sector Employees**	**Police Personnel**	**Lawyers**

No. of Respondent	**100**	**10**	**50**	**50**	**10**	**50**
Methodology	Questionnaires	Personal Interview	Questionnaires	Questionnaires	Personal Interview	Questionnaires

1.12. LIMITATION OF THE RESEARCH

The current research points out a handful of limitations such as methodological as well as geographical limitations. In terms of geographical limitation, the study pertains only to the geographical area of Mumbai and may only represent that part of the nation. Also, there is another possibility of the restriction of selective memory of the sample population, which would indicate that the respondents participating in this qualitative legal research employed by the questionnaire method for collection of data have a propensity to not recall or remember events from their past correctly, for example, a general respondent may not be aware about the online transactions or strong password requirement for protection from cyber criminals. might tend to forget that and thereby to put an incorrect answer in the questionnaire rendering the credibility of such response to nullify. The cyber experts are rare in numbers specially in Mumbai for personal interviews still the researcher managed to interview the cyber experts, and similarly the police personnel might refrain from giving personal interview to the researcher.

CHAPTER II

Cybercrime: Historical Background, Its Types & Challenges to the Society

With our reality moving towards digitization, the events of digital wrongdoings on frameworks can be profoundly harming. As innovation advances and more individuals rely upon the web abled administrations for consistently exercises, including putting away their Visa subtleties and executing cash on the web, digital violations are getting more normal than any time in recent memory. The outcomes of these advanced assaults are ruinous and can cause some genuine harms[104].

2.1 HISTORICAL BACKGROUND OF CYBER LAW IN INDIA

The Information Technology Act is the consequence of a United Nations General Assembly decision enacted on January 30, 1997, which adopted the Model Law on Electronic Commerce on international trade law. The following resolution recommended, among other things, that all states carefully consider the aforementioned model when revising or enacting new legislation so that the laws governing alternatives to paper-based methods of communication and information storage remain balanced among the various cyber nations. The Department of Electronics drafted the law in July. However, it was not introduced into the House until December 16, 1999, more than a year after the new IT ministry was constituted. After the trade ministry submitted recommendations on e-commerce and WTO commitments, the statute was modified. The ministry of law and company affairs then reviewed this joint Draft[105].

After being introduced in the house, the bill was referred to the 42-member parliamentary standing committee in response to member requests. The bill's standing committee made recommendations that were incorporated into the legislation. However, only recommendations approved by the ministry were implemented. One of the widely debated ideas was that a cyber café owner keeps a record of all guests' names and addresses and a list of the websites they viewed. This concept was developed in order to reduce cybercrime and make it easier to identify hackers. It was, however, not given the attention it deserved. The union cabinet authorized the law on May 13, 2000, and both chambers of parliament passed the Information

[104] Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. International Research Journal of Engineering and Technology (IRJET), 4(6), 1633-1640.
[105] Dr. A Sukumar, *Cyber law* 04, (1st ed, ISBN: 978-93-5321-921-5, 2018)

Technology bill on May 17, 2000. The president signed the bill, known as the Information Technology Act of 2000, on June 9, 2020. On October 17, 2000, the act went into effect. As technology advanced and new methods of committing crime arose on the Internet, it became clear that the IT Act 2000 needed to be revised to combat cybercrime, and it was updated in 2008.[106]

2.2 CURRENT SITUATION OF CYBER LAWS IN INDIA

This year, India is accelerating the web stepping stool, presenting the second largest web client population of a daring 560 million clients. The pandemic will increase this number even further in 2021, with projections reaching at least 600 million clients. Be that as it may, on the other side, these incontestable figures build up the requirement for a powerful network safety system of the country. With consistent digitization and information development, it is vital to protective layer up with the essential assets, including complete preparing, to guarantee information security and network safety in India. Furthermore, with network protection being a $6.7 billion industry, there is a more noteworthy requirement for harsh and inflexible digital laws in India[107].

Attacks on Cybersecurity Systems Growing Significant paper title texts are currently being dominated by cybercrime, which is causing unintended harm to both persons and enterprises. Information penetration, data fraud, financial robbery, and web time robberies are some of the most typical sorts of digital burglaries[108]. Online security is becoming more and more crucial, yet programmers are always honing their craft and figuring out new ways to get past defences. This highlights the requirement for more stringent online protection policies and digital regulations. In order to lessen digital offences and dissuade fraudsters, legislators should also be aware of potential weaknesses in the network security scene and progressively remedy them. Controlling the escalating cross-country risks requires relentless efforts and constant vigilance.

As human reliance on innovation grows, digital laws in India and around the world require continuous improvement and refinement. The epidemic has also pushed a substantial

[106] Available at www. Tax Guru.in, Information Technology 2008 amendment Bill accessed on 12th May 2020 at 2:30pm
[107] Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013, September). A survey of cyber crime in India. In 2013 15th international conference on advanced computing technologies (ICACT) (pp. 1-6). IEEE.
[108] Deepti Chopra and Keith Merrill, Cyber Cops, Cyber Criminals and the Internet, I.K. International Pvt. Ltd., 2012, New Delhi.

portion of the labour force into a remote working module, increasing the need for application security. Administrators must go above and beyond to stay ahead of the impostors and obstruct their approach. Cybercrime can be managed, but it takes the combined efforts of regulators, Internet or network providers, middlemen such as banks and shopping destinations, and, most importantly, clients. Only the prudent efforts of these partners - ensuring their imprisonment to cyberland legislation - can achieve online security and flexibility.[109]

2.3 CYBERCRIME AND TYPES OF CYBER CRIMES

Quite possibly the most well-known and oft-happening types of wrongdoing on the planet, digital wrongdoing can be characterized as the misuse of computer organizations, frameworks, and innovation subordinate ventures deliberately. There are various kinds of digital violations that utilization malevolent code to alter information and gain unapproved access. Cyber-crimes are classified into three general classifications, individual, property and government. In view of every classification of digital wrongdoing, cybercriminals utilize various levels and sorts of dangers[110].

Individual: This digital wrongdoing class incorporates spreading pernicious or unlawful data through the web and computerized applications by one individual. Digital talking, erotic entertainment dissemination, and dealing are a couple of instances of this classification of digital wrongdoing.

Property: This digital wrongdoing is like a genuine occurrence where a criminal keeps the bank or charge card data illicitly. The programmer takes a person's bank subtleties to secure cash or makes phishing tricks online to get data from individuals.

Government: It is the most un-successive digital wrongdoing yet the most real offense. A digital wrongdoing against the public authority is additionally viewed as Cyber Terrorism. Government digital wrongdoing includes the hacking of sites, military sites, or the appropriation of government purposeful publicity.

2.3.1. Web Attacks

Through the internet, a web assault affects the PC. These infections can be obtained on the internet and end up having a huge impact and causing irreversible harm to your system. The most common types of web attacks are sql injections, bots, malware attacks, all these

[109] https://www.appknox.com/blog/cybersecurity-laws-in-india
[110] Dr. R. K. Tewari and others, *Computer Crime and Computer Forensics* 45 (Select Pub., Delhi, 2017)

attacks form the concept of web attacks. Different methods are used by the cyber criminals to attack the system and gain access to the source[111].

2.3.2. SQL Injections

SQL infusion is a sort of crime in which malicious code is used to change backend data sets in order to obtain access to data that is not intended to be displayed. These are usually private and sensitive information, such as any resemblance of customer data and client subtleties. SQLI can have long-term negative consequences such as table erasure, unapproved client list surveying, and unexpectedly authoritative access to data sets. SQL injections helps the hackers to do identity theft, alter data, close all the relevant system files, destroy data or otherwise make it unavailable to the user[112]

2.3.3. Cross-Site Scripting

Cross-Site is another type of infusion penetration in which attackers distribute poisonous content from sites that are thought to be aware or rumored. Aggressors inject malicious code into trusted sites and programs, and when a client views such a tainted website page, the malicious JavaScript code is run on the client's software. This code can be used to obtain sensitive information such as a username and a secret phrase[113].

2.3.4. DDoS Attacks

These are the assaults that target closing down administrations or organizations and making them difficult to reach to the proposed clients. These assaults overpower the objective with a ton of traffic and flood something similar with data that can make the site crash. DDoS Attacks are focused on fundamentally at web workers of high-profile associations, for example, the public authority or exchange firms.

2.3.5. Pass word Attacks

These are just intended to unscramble or even endeavor to get a client's secret word with the assistance of criminal expectations. Assailants can utilize Dictionary Attacks,

[111] Available at https://www.tripwire.com/state-of-security/most-common-website-security-attacks-and-how-to-protect-yourself accessed on 07th March 2021 at 4pm
[112] Available at https://www.w3schools.com/sql/sqlinjection accessed on 07th March 2021 at 4pm
[113] Availabe at https://www.cloudflare.com/learning/security/threats/cross-site-scripting accessed on 07th March 2021 at 4pm

Password Sniffers, or in any event, Cracking projects in such cases. These assaults are directed by getting to passwords that are traded or put away in a document[114].

2.3.6. Eavesdropping Attacks

Listening in assault starts with the block attempt of organization traffic. This sort of digital wrongdoing is otherwise called Sniffing or Snooping. In this kind of digital wrongdoing, people endeavor to take data that PCs, cell phones, or different gadgets get or send. It usually occurs when a user connects to a network which is not secured and send something sensitive to his colleagues or his office members. And due to this the network being unsecured the data is readily available on the web of which the attackers use the information to attack the user[115].

2.3.7. Savage Force and Dictionary Network Attacks

These are organizing assaults where aggressors endeavor to straightforwardly sign into the client's records by looking at and attempting changed potential passwords until they track down the right ones. This form of attack is usually by hackers and new scammers in which they use the method of hit and trial by savage force to gain access in the system by entering the passwords or the login credentials[116].

2.3.8. Insider Threats

Not the entirety of the organization assaults is executed by outcasts. Within assault is a typical kind of digital wrongdoing. It is performed on an organization or a framework by people who have approved admittance to a similar framework. Insider threats are the most common form of data breaches in most of the organizations. Mostly organizations focus on external threats but it’s the insider who breaches the wall for the threat or malware[117].

2.3.9. Man-in-the-Middle Attacks

When aggressors snoop on the correspondence between two substances, a man-in-the-center assault occurs. As the assailant can do anything with the decoded data, this type of digital

[114] Dr. Farooq Ahmad, Cyber Law in India - Law on the Internet, Pioneer Books, New Delhi
[115]Available at https://www.fortinet.com/resources/cyberglossary/eavesdropping accessed on 09th March 2021
[116] Available at https://www.rapid7.com/fundamentals/brute-force-and-dictionary-attacks accessed on 09th March 2021
[117] Available at https://www.microfocus.com/en-us/what-is/insider-threat accessed on 09th March 2021

wrongdoing affects both the transmitting parties. The goal of man in the middle attack is to gain information such as log in details, account details, credit card details and financial apps[118].

2.3.10. Man-made intelligence-controlled Attacks

PC frameworks are presently modified to learn and show themselves, and these AI-fueled assaults mark another sort of digital wrongdoing that will undoubtedly get more complex with time. Man-made intelligence is utilized in numerous regular applications with the assistance of algorithmic cycles alluded to as Machine Learning. This product is pointed toward preparing PCs to perform explicit assignments completely all alone. They can likewise achieve these assignments by showing themselves impediments that can possibly ruin their advancement. Artificial intelligence can likewise hack numerous frameworks, including self-ruling robots and vehicles, and convert them into conceivably perilous weapons. The AI-fueled applications can be utilized for performing digital wrongdoings like Password Cracking, Identity Theft, and mechanized, proficient and vigorous assaults[119].

2.3.11 Drive-by Attacks

Malware is spread through vulnerable websites through drive-by assaults. The harmful content is initially inserted into PHP or HTTP code on one of the pages by programmers after they have found a site with weak security. The content can then instantly download malware onto any user's PC who visits the website. The malicious script makes it download itself on the use system without the permission of the owner of the device and it can happen on any device. This usually happens when the user browses multiple website's which are not secured[120].

2.3.12. Phishing Attacks

When attackers pose as reliable people and dupe victims into accepting dangerous connections, the Phishing Attack is a type of Social Engineering attack that is used to obtain sensitive data, such as login credentials or Visa details. A phishing can look like a simple email, a social message, or even a phone call. It will ask for the basic details or sometimes it gives you all the information regarding your system and on that basis gain access in your system[121].

2.3.13. Spear Phishing Attacks

[118] Available at https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm accessed on 09th March 2021
[119]Available at https://www.belfercenter.org/publication/AttackingAI accessed on 09th March 2021
[120]Available at https://www.ericom.com/glossary/what-is-a-drive-by-attack/ accessed on 09th March 2021
[121] S. V. Joga Rao, Law of Cyber Crimes and Information 'Technology Law, Wadha & Co., 2004

Information about explicit associations is the target of these assaults by those looking for unauthorized access. These hacks are conducted by individuals that want access to explicit data, such as competitive advantages, military intelligence, and so forth. It works in the simplest form by receiving an email from a known source and by clicking or complying the requirements of the email it takes the person to the bogus website in which the actual crime takes place[122].

2.3.14. Whale Phishing Attacks

A particular kind of phishing assault known as a "whale phishing attack" usually targets CEOs or CFOs because of their positions of authority. Because to the fact that these people frequently have unrestricted access to sensitive information, it primarily targets data collecting. Financial institutions and payment services bodies are the most targeted by these whale phishing attacks. Whale phishing are more formal as it usually targets the chief officials of the company to perform a secondary function[123].

2.3.15. Malware

A code or software that is intended to affect or target PC frameworks without the client's authorization is referred to as malware. Any type of malicious software designed to harm or corrupt the system, cyber criminals usually use this system to gain access in the system for financial gain. The data which can be assessed through malware can vary from personal data, medical data, personal emails and sensitive information of corporates[124].

2.3.16. Ransomware

Ransomware mostly prevents victims from accessing their own data and deletes something comparable if a payoff is not made. It’s a malware that denies the origination, institutions or servers to access its own information. And if one wants to gain access to its own data, they have to pay money we can say its one type of extortion in a digital form. It has quickly become the most used by the cyber criminals to attack corporates bodies and huge institutions[125].

2.3.17. Trojan horses

[122] Available at https://www.kaspersky.com/resource-center/definitions/spear-phishing accessed on 09th March 2021
[123]Available at https://www.ncsc.gov.uk/guidance/whaling accessed on 09th March 2021
[124] Available at https://www.mcafee.com/en-in/antivirus/malware.html accessed on 09th March 2021
[125]Available at https://www.checkpoint.com/cyber-hub/threat-prevention accessed on 09th March 2021

Deception is a sort of malevolent programming program which endeavors to mask itself to seem valuable. It seems like a standard application however purposes harm to information documents once executed. In simpler terms trojan horses gets hidden in attachment or free to download file and similarly it gets transferred to the device or the system. After its downloaded it will run its code and attack the system and the gets the access as required by the hacker[126]

2.3.18. Teardrop Attack

Tear assault is a type of assault that causes discontinuity in the overall grouping of Internet Protocol (IP) parcels and sends these divided bundles to the casualty's machine that is assaulted. These attacks use fragments to send data to the other systems as large amount of data cannot be transferred at one go. Its than sent in systematic mannerism so that the othe person is unaware of the attack as its coming in pieces and the file is not heavy. Its difficult to detect the attack[127]

2.3.19. Ping of Death Attack

The Ping of Death Attack is a type of digital misbehavior in which IP combines ping objective frameworks with IP measures that exceed the byte limit by a large margin. It's a hack similar to denial-of-service attack it destabilizes the system or services and even freezes the system totally and makes the user an idol he or she cannot use the system at all[128].

2.3.20. PUPs

This is a sort of malware that is less dangerous than other types of digital misbehavior. This type of attack removes the necessary online search tool and pre-installed programs from your frameworks. As a result, it is a wise idea to use antivirus software to prevent malicious downloads. While installing a legal software it asks for more installation in which it installs unwanted software's that hacks the system and it works in the background and the person who have used this trick is having all the access of the system in which the software is installed[129].

2.3.21. Theft/Burglary of FTP Passwords

This is another another really simple approach for switching websites. FTP secret key hacking exploits the fact that many website managers store their site login data on insecure

[126] Available at https://www.fortinet.com/resources/cyberglossary/trojan-horse-virus accessed on 09th March 2021
[127] Available at https://www.okta.com/identity-101/teardrop-attack/ accessed on 09th March 2021
[128] Available at https://www.fortinet.com/resources/cyberglossary/ping-of-death accessed on 09th March 2021
[129] https://www.google.com/amp/s/www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime

devices. The thief searches the victim's computer for FTP login information, which he subsequently sends to his own distant workstation. He then enters on to the site via a remote PC and customizes the website pages to the individual's preferences[130]. The FTP works through the malware inserted and the malware software seeks the login and passwords and then send it to the hacker it only takes few seconds to the malware to show its powers to get all the relevant information from the source computer.

2.3.22. Logic bomb

A logic bomb, sometimes known as "slag code," is a hazardous piece of code that is purposefully embedded in software to perform a destructive errand when triggered by a specified event. It is not an infection, despite the fact that it frequently continues along these lines. It is discreetly injected into the application and remains inactive until the requirements indicated are met. Infections and worms, for example, commonly contain logic bombs that detonate at a predefined payload or time. A logic bomb's payload is undisclosed to the product's client, and the errand it completes is unwanted. "Delayed bombs" are software codes that are set to execute at a predetermined time. For example, the infamous "Friday the thirteenth" infection, which only attacked host frameworks on specific dates; it "detonated" (copied itself) each Friday that happened to be the thirteenth of the month, resulting in framework lulls[131].

2.3.23. Phishing

Phishing does not necessarily take place via email or websites. Vishing (voice phishing) is a sort of phishing that involves making calls to victims while using a fake identity to make the call appear to be from a trusted source. They may pretend to be from a bank and request that you dial a number (given by the VoIP administrator and claimed by the assailant) and enter your account details. The security of your records is threatened when you do this. Any unexpected calls should be treated with caution, and no personal information should be given. Several banks have issued preemptive warnings to their clients about phishing scams and personal information dos and don'ts. Those of you who have been reading Digit for a while may remember how we successfully phished many of our readers by sharing how to hack other

[130] Available at https://www.vpwsys.net/blog/analysis-of-an-ftp-hack/ accessed on 07th March 2021 at 4pm
[131] Joga Rao S.V. *Law of Cyber Crimes and Information Technology Law*, Wadhwa and Company, Nagpur, 2004.

people's Gmail accounts by sending an email to a bogus account with your own username and secret word... Years ago, we did it in an anecdote about, you guessed it, phishing[132].

2.3.24. Email bombing and spamming

Email bombing/besiegement is defined as a victimizer sending massive amounts of email to a target site, resulting in the casualty's email record or mail employees being slammed. The message is insignificant and excessively long, consuming network resources. If a mail worker's different records are scrutinized, it could have a disavowal of-administration effect. Spam filters can easily identify mail that appears in your inbox on a regular basis. As a DDoS attack, email bombardment is frequently carried out via botnets (private web-connected PCs whose security has been compromised by malware and are under the aggressor's control).

Because of the different source addresses and bots that have been updated to deliver varied messages to crush spam channels, this type of attack is more difficult to control. Spamming is a type of email besiegement. Unpredictably, spontaneous mass communications are sent out to a large number of clients. Opening links in spam messages may lead to phishing sites that facilitate malware. Infected papers may also be included as attachments in spam messages. When the recipient responds to the email, every one of the original addressees receives the response, which degrades email spamming. Spammers obtain email addresses from client records, newsgroups, chat rooms, websites, and infections that harvest customers' address books, and then sell them to other spammers. Invalid email addresses are used to send a lot of spam.

Spamming is a violation of almost every network access provider's acceptable use policy (AUP). If your framework becomes sluggish out of nowhere (email stacks slowly or doesn't appear to have been sent or received), the cause could be that your mailer is preparing a large quantity of messages. Regrettably, it is exceedingly unlikely to completely prevent email bombardment and spam sends at this time, as it is difficult to predict when the next assault will begin. What you can do, though, is figure out where the spam is coming from and configure your switch to block any incoming messages from that source[133].

[132] Available at https://www.ibm.com/topics/phishing accessed on 07th March 2021 at 4pm
[133] Available at https://www.freepressjournal.in/mumbai/fpj-cyber-secure-mumbai-police-issues-advisory-on-email-bombing-for-citizens-to-stay-safe-from-online-threat / accessed on 07th March 2021 at 4pm

2.3.25. Web Jacking

In these types of crimes, the programmer gains access to and control over another's website. He may even alter the information on the website. This could be done to meet political objectives or to make money. For example, the MIT (Ministry of Information Technology) website was recently hacked by Pakistani coders, and some unpleasant content was added to it. In addition, the website of the Bombay wrongdoing branch was hacked. The 'gold fish' case is another example of online jacking. The site was hacked in this case, and the data about gold fish was modified[134]. Gaining access of websites and taking control of the domain, this lead to the extortion as the website can be used by the hacker for his own beneficial purpose or post something offensive or derogatory against the domain hacked. Similarly, web jacking plays an important role in getting access to data of citizens who login or into the website thinking it to be the same website and simultaneously it will direct the individual to some other unauthorized website in which the criminal is having control over it.

2.3.26. Cyber stalking

Another sort of web misconduct among our general public is cyber stalking/digital following, which occurs when an individual is sought after or tracked on the internet. A digital stalker does not literally follow his victim; instead, he collects data about him by following his online movements in order to bother him and intimidate him with verbal bullying. It's a breach of one's online security. Cyber following is similar to disconnected following in that it uses the internet or other electronic techniques to link people. The majority of those who survive this transgression are women who are pursued by men, as well as children who are pursued by adult hunters and pedophiles. Digital stalkers thrive on inexperienced web users who aren't well-versed in netiquette and web safety standards. A digital stalker could be a stranger, but it could also be someone you know[135].

Cyber stalkers use email, chat rooms, websites, conversation meetings, and open distributing sites to harass their victims (for example websites). The availability of free email/site space, as well as the anonymity provided by chat rooms and gatherings, has contributed to the growth of digital following episodes. Everyone these days has an online profile, and it's really easy to do a Google search and find one's name, pseudonym, phone

[134]Available at https://www.geeksforgeeks.org/web-jacking/ accessed on 07th March 2021 at 4pm

[135]Available at https://www.kaspersky.com/resource-center/threats/cyberstalking accessed on 07th March 2021 at 4pm

number, and address, adding to the threat of digital following. As the internet becomes a more integral part of our personal and professional life, stalkers can take advantage of the ease with which we can communicate and the ease with which we can get personal information with just a few mouse clicks. Furthermore, the mysterious and non-violent nature of web exchanges eliminates any disincentives to digital following. Cyber stalking/digital following is carried out in two ways.

Web stalking: In this case, the stalker uses the internet to track down the victim. The most well acknowledged form of compromising someone is through email, and the stalker may even send nasty material and diseases via email. Infections and impromptu sales emails, however, are insufficient to build a digital following. If an email is sent more than once in an attempt to threaten the recipient, they may be seen as following. Web stalking isn't limited to email; stalkers can use the internet to harass their targets to a greater extent. Other digital wrongdoings that we've successfully discovered may add up to digital following if they're done with the intent to compromise, irritate, or defame the victim.

Computer Stalking: The stalkers who are more mechanically advanced use their PC skills to aid them in their investigation of the infraction. They deal with the victim's computer by abusing the web's and Windows' operating frameworks. Despite the fact that this is usually done by skilled and computer-savvy stalkers, instructions on the most efficient approach are readily available on the internet[136].

The practice of cyber stalking/digital following has now moved to one-on-one communication. Your profile, images, and announcements are all visible to the world thanks to the increased use of online media such as Facebook, Twitter, Flickr, and YouTube. Your online presence provides you with enough information to make you an expected follower survival without having to keep an eye on the threat. With the "registration," "life-occasions," programs that access your personal data, and the requirement to set up pretty much everything you do and where you do it, you don't forget anything for the stalkers to figure out. Informal communication technology provides a social and communitarian platform for web users to connect, express their opinions, and share almost everything about their lives. Despite the fact that it promotes individual sociability, it also contributes to the rise of web infringement[137]

[136]Available at https://cyberbullying.org/cyberstalking accessed on 07th March 2021 at 4pm
[137] Available https://us.norton.com/blog/how-to/what-is-cyberstalking accessed on 07th March 2021 at 4pm

2.3.27. Data diddling

Data tampering/ Information tampering is the unapproved altering of data prior to or during transmission into a computer system, and then reversing the process once the preparation is accomplished. The aggressor can change the normal yield with this method, and it's difficult to track. Overall, the first data to be entered is changed, either by the person entering the data, an infection that is modified to change the data, the developer of the data set or application, or any other person involved in the process of creating, recording, encoding, analyzing, checking, changing over, or communicating data.

Given that even a PC novice can accomplish it, this is likely the simplest approach for committing a PC-related violation. Despite the fact that this is a simple task, it might have negative consequences. For example, a person in charge of bookkeeping may alter facts about themselves or a friend or relative to give the impression that they are completely settled. They are prepared to withdraw from the project by altering or failing to enter the data. Manufacturing or fabricating reports, as well as selling large PC tapes or cards with pre-arranged substitutions, are all examples of different types. When private gatherings in India began automating their frameworks, power sheets were survivors of information tampering by PC hoodlums[138].

2.3.28. Identity theft and credit card fraud

Identity theft/fraud occurs when someone assumes your identity and pretends to be you in order to gain access to assets such as Visas, ledgers, and other benefits in your name. The imposter could even use your personality to commit various crimes. "Visa misrepresentation" is a broad phrase that encompasses a variety of wrongdoings, including fraud in which the criminal uses your Mastercard to fund his transactions. In its most basic structure, charge card misrepresentation is wholesale fraud. Your pre-supported card getting into the wrong hands is the most well-known example of Visa extortion.

He can use it to buy anything until you denounce him to the authorities and get your card revoked. On charge card purchases, the only safeguard is a mark on the receipt, which can be made without much difficulty. However, in some countries, the shipper may ask for identification or a PIN. Some Visa companies have software that assesses the possibility of deception. The guarantor may even phone you to double-check if an unusually large transaction occurs.

[138]Available at https://www.computerhope.com/jargon/d/data-diddling.htm accessed on 06 March 2021 at 3pm

When paying with Visa, people frequently forget to collect their duplicate of the Visa receipt after eating at restaurants or elsewhere. Your Mastercard number and mark are printed on these receipts for anybody to see and use. Someone can make purchases on the internet or over the phone using only this information. You won't know about it until you get your month-to-month explanation, which is why you should carefully consider your claims. When shopping on the internet, make sure the site is trustworthy and safe. Using phishing techniques, a few programmers may be able to reclaim some control over your credit card number. In rare situations, a little latch symbol appears in the left screen corner of your program's location bar, indicating a higher level of security for data transmission. If you click on it, it will also reveal the encryption software that it employs[139].

A more serious issue is the use of your personal information to open records (or, even worse, to obtain a loan in your name) using stolen or false records. These scumbags can glean your personal information from your letter box or garbage can (make sure to shred every single delicate archive). Consider all of the important details imprinted on those receipts, pay stubs, and various reports. You won't have a clue about anything unless the Visa public tracks you down and follows you till you complete your mission. You'll be fighting to get your credit restored and your name cleared for a long time after that.

With the rise in charge card fraud, many financial institutions have stepped in with programming solutions to screen your credit and protect your character. It is possible to recover lost wages and repair your credit by obtaining ID robbery protection. However, before you spend a fortune on these administrations, use the free, mind-body-strengthening procedures to prevent such misconduct.

2.3.29. Salami slicing attack

A "salami cutting assault" or "salami extortion" is a tactic in which digital criminals remove money or assets one piece at a time, with no discernible difference in overall size. The perpetrator steals these small bits from a variety of assets, amassing a large quantity over an unspecified period of time. The difficulty to distinguish the misappropriation is at the heart of this tactic. The "collect the-roundoff" strategy is the most exceptional methodology. Most estimations are done in a given currency and then adjusted up to the nearest number for a fraction of the time and down for the rest. There appears to be no overall loss to the structure

[139] Pradhan R.K. *Cyber Crime and Cyber Terrorism,* Mangalam Publications, Delhi, 2010.

if a software programmer chooses to collect these abundance bits of rupees to a different record. This is accomplished by carefully moving the assets into the record of the perpetrator[140].

Aggressors insert a program into the framework to carry out the task. Rationale bombs can also be used by disgruntled ravenous employees who abuse their knowledge of the company and have restricted access to the system. The criminal uses math adding machines to organically change information, such as interest estimates, in this method.

The most well-known application of the salami cutting approach is taking money electronically, although it isn't confined to unlawful tax avoidance. The salami technique can also be used to collect little quantities of data over an indefinite time period in order to form a general picture of an association. This display of dispersed data social event could be used against an individual or a group. Information can be obtained from websites, promotions, waste bin records, and other sources, allowing for the continual development of a full data set of factual intelligence about the goal.

We should be extra cautious because the measure of misappropriation is simply below the limit of insight. A careful examination of our resources, exchanges, and all other aspects of management, including the sharing of secret data with others, may help to reduce the chances of an attack using this technique.

2.3.30. Software piracy

The internet is to thank for this. You can find practically any film, programming, or melody from any era for free thanks to the internet and downpours. Web robbery is a common occurrence in our lives that we all contribute to, whether consciously or unconsciously. As a result, asset engineers' benefits are being reduced. It's not just about illegally using another person's protected idea; it's also about sharing it to your friends, reducing the amount of money they deserve.

Software piracy/robbery is the unlicensed usage and distribution of computer software. Robbery tests their ability to generate enough cash to support application advancement. Programming designers try to foster these initiatives, and robbery checks their capacity to make enough revenue to support application advancement. This has an impact on the entire global

[140] Sharma Vakul, *Information Technology Law and Practice*, 4 ed. Universal Law Publishing, 2015.

economy since assets are transferred from diverse fields, resulting in a decrease in interest in marketing and research. Programming robbery is defined as follows:

- Stacking unlicensed software on your computer
- Using single-authorized programming across multiple PCs
- To get around duplicate assurance, you can use a critical generator.
- Disconnectedly disseminating an approved or unauthorized ("broken") kind of content via the internet.

Another risk is "cloning." It occurs when someone steals your product's idea and rewrites it in his own code. This isn't strictly illegal because thoughts aren't continually duplicated across borders. A product "break" is an incorrectly obtained variety of the product that circumvents the encoded duplicate anticipation. Clients of stolen programming can use a critical generator to generate a "sequence" number that opens the product's assessment adaption, effectively crushing the duplicate insurance. Copyright infringement is demonstrated through programming breakage and the use of unauthorized keys. Using stolen materials comes with its own set of risks. Because privateers will constantly taint programming with noxious code, the pilfered programming may contain Trojans, viruses, worms, and other malware[141].

Clients of pilfered programming may face legal repercussions for unauthorized use of protected material. Furthermore, you will not receive product support from the developers. If you're a designer, you should use strong security measures to prevent your product from theft. A few websites sell programming that includes a "computerized unique finger impression," which aids in tracing stolen replicas back to their source. Equipment locking is another common strategy. The product permission is attached to a specific PC equipment using this method, to the point where it only runs on that PC. Regrettably, programmers continue to find ways to get around these restrictions.[142]

2.3.31. Social Media Hack & Spamming

Hacking into social media/web-based media is frequently done as a joke, as evidenced by the attack on Burger King's twitter account. Many hacked VIPs may go after people they wouldn't typically go after or place themselves in unusual circumstances with. Although it may be entertaining for the average person to see a celebrity or brand post unusual things, it is a

[141] Brenner S. W. (et al), Approaches to Cyber Crime, *Journal of High Technology Law*, Vol. IV, 2004
[142]Available at https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html accessed on 04th March 2021 at 9pm

security breach. However, a programmer can also spread inappropriate content that can be upsetting to those who see it, as well as cause your account to be accounted for and closed down. Spamming on social media occurs when a person creates a fake profile and becomes friends with or followed by regular people. This gives the phony account the ability to spam inboxes with mass notifications, which should be possible for malware distribution. Spamming can also spread harmful connections that are intended to harm, deceive, or harm a client or their device. By clicking on the pernicious link, which may be promoting a new iPhone or a weight-loss treatment, you risk downloading malware that can lead to the theft of personal information.

Another thorny aspect of online media is the potential for vengeful records to spam your yield by repeatedly responding with negative information. This is a type of scavenging. While you can certainly report such behavior to the online media platform, and they should remove the client, or you can prevent them from seeing your content, it's easy for people to create new bot accounts in minutes and resume their assault[143].

2.3.32. Electronic money laundering

Before it is spent or contributed, money created in large amounts illegally should be washed. A "wire move" is an electronic method of laundering funds that involves sending messages between banks. Because of the large number of exchanges that occur on a daily basis, it has recently appeared to be impossible to screen or screen wire transfers as they occur. In any case, banks are bracing for the issue and logging any suspicious activity[144]. The electronic money transfer is the easiest form of money transfer for terrorism financing and illegal form which is used by the criminal is the Hawala form of money transfer.

2.3.33. Cyber bullying

Cyberbullying is characterized by an ongoing barrage of insulting, aggressive, and disrespectful comments, much like cyber stalking. Cyberbullying can also take the form of online posts containing pornographic images and videos. Cyberbullying includes excluding someone online, creating fictitious personas to disseminate offensive or frightening content, and sending hurtful communications. Bullying is a widespread issue, but it is getting worse

[143] Pillai, K.N., *Principles of Criminology* 06 (T.L.L. 2013)
[144] Krzysztof, W. O. D. A. "Money laundering techniques with electronic payment systems." *International & Security. An International Journal* (2006): 27-47.

online, particularly on social networking sites, cyber bullying can take place in multiple forms the person can use videos, photos and sensitive information to bully the next person in order to gain advantage over him and his mind[145].

2.3.34. Child Soliciting & Abuse

Child Soliciting and Abuse on the Internet is a type of cybercrime in which criminals seek minors through online forums in exchange for pornographic enjoyment. It can also take the form of content that depicts or shows sexual abuse of children. A child is defined as a person under the age of sixteen. The authorities keep a close eye on this type of digital misbehavior. It is a threat to both businesses and individuals because the perpetrators may be seeking to create a new persona on the internet, Government around the world have also given the importance of combatting online child soliciting and child abuse[146].

2.3.35. Internet time theft

This suggests that someone else's Internet hours were used by an unapproved individual. The financial offenses branch of the IPR area misconduct portion of the Delhi police enlisted its first case in May 2000, which involved the robbery of Internet hours. For this reason, the accused, Mukesh Gupta, an engineer with Nicom System (p) Ltd., was dispatched to the complainant's residence to activate his Internet connection. However, the accused obtained Col. Bajwa's login name and secret phrase from several sources, resulting in an unauthorized loss of 100 hours for Col. Bajwa. The suspect in the burglary for Internet time was apprehended by Delhi police. On further investigation into the matter, it was discovered that Krishan Kumar, the son of an ex-military officer who works as a senior leader for M/s Highpoint Tours & Travels, had used Col Bajwa's login and passwords many times from his home and twice from his office. He stated that the login and secret word were given to him by Shashi Nagpal, from whom he had purchased a computer.

The cops couldn't believe that time could be snatched away from them. By any stretch of the imagination, they had no notion what time-burglary was. The report of Colonel Bajwa was discarded. He made the decision to relocate to New Delhi, to The Times of India. As a result, they delivered a report on the New Delhi Police's failure to act with digital violations. The Commissioner of Police, Delhi, took the case into his own hands at that moment, and the

[145] Marées, Nandoli & Petermann, Franz, *Cyberbullying: An increasing challenge for schools*. (School Psychology International. 33. 467-476. 10.1177/0143034312445241)
[146] Available at https://www.silverbug.it/2017/08/28/10-types-of-cybercrimes accessed on 06 Jan 2021 at 9am

police assaulted and apprehended Krishan Kumar under sections 379, 411, and 34 of the Indian Penal Code, as well as section 25 of the Indian Telegraph Act. In another case, the Delhi Police's Economic Offenses Wing apprehended a PC engineer who obtained the secret key of an Internet customer, gained access to the PC, and deducted 107 hours of Web time from the other person's record. In May of 2000, a Delhi court reserved him for the offence[147].

2.3.36. Cyber terrorism

Cyberterrorism is the union of psychological warfare and the internet. It is for the most part perceived to signify "unlawful assaults and dangers of assault against PCs, organizations, and the data put away in that when done to threaten or pressure an administration or its kin in promotion of political or social destinations" (Michael Knetzger, 2008). Furthermore, for an attack to be classified as cyberterrorism, it must result in brutality against people or property, or perhaps cause enough harm to instill fear. Assaults that result in death or serious injury, explosions, plane crashes, tainted water, or significant financial ruin would be examples. Depending on the impact, genuine attacks against basic infrastructure could be considered cyberterrorism. Assaults that disrupt minor administrations or are primarily a source of annoyance would not be tolerated. This is an exhaustive list of cyber-crimes and how its committed to gain advantage on the general public or individual or organization as they are fruitful for the cybercrimes as well as for cybercriminals. Let's get the understanding of cyber-crimes on the Society[148].

Cyber terrorism is the unique method adopted in the 21st century by the cyber criminals in order to gain advantage towards the uneducated individuals to lure them and make them more dangerous mentally by gaining their trust through various internet things and electronic devices which is available easily in the cyberspace. This gives an advantage to the cybercriminals to have a upper hand in relation to crime committed on the internet with outmost secrecy and no online prints of any identity which is very difficult to be traced if one wants to find the cybercriminals in the real world.

[147] Mali Prashant, *Electronic Evidence and Cyber law*, (CSI Communications 2012)
[148] Conway M, *what is Cyberterrorism Current History* 36 (Vol. 2, 2000)

2.4 CYBER CRIME AND ITS CHALLENGES TO THE SOCIETY

A single cyber-attack/digital assault can have far-reaching implications, including as financial losses, theft of protected inventions, and loss of customer confidence and trust. It is believed that the annual economic impact of digital misbehavior on society and government is in the billions of dollars. Crooks profit from invention in a variety of ways. The Internet, in particular, is a terrific tool for con artists and other thieves since it allows them to do their business while remaining anonymous online. Misbehavior on the internet has a wide range of consequences for society, both online and offline[149].

2.4.1. Impact of cybercrime on identity theft/privacy

Cybercrime affects both a virtual and physical body, although the effects on each are different. Because of the deceit, this miracle is most obvious. People in the United States, for example, do not have an authority character card but do have a Social Security number, which has long served as a true identifying proof number. Every resident's Social Security number is used to collect assessments, and many private organizations use it to track their representatives, understudies, and patients.Access to a person's Social Security number controls the cost of the opportunity to amass all of the records associated with that person's citizenship—that is, to seize his identity. Even stolen credit card information can be used to change a person's personality. When hoodlums steal an organization's Mastercard records, they have two distinct outcomes. First and foremost, they collect advanced data on people that is useful from a variety of angles.

For example, they may use Mastercard data to add to massive invoices, causing massive losses for charge card companies, or they could sell the data to others who could use it in the same way. Second, they might use unique Mastercard names and numbers to create new personalities for various criminals. A burglar, for example, could contact the bank that issued a stolen Mastercard and modify the postal information on the record. The perpetrator may then obtain an identification card or a driver's license bearing his own image but bearing the name of the victim. With a driver's license, the criminal can easily obtain another Social Security card, allowing them to create financial accounts and obtain loans using the victim's credit history and foundation. The first cardholder may be completely unaware of this until the obligation becomes so significant that the bank notifies the record holder. It is at this point

[149] Iqbal, Juneed, and Bilal Maqbool Beigh. "Cybercrime in India: trends and challenges." *International Journal of Innovations & Advancement in Computer Science* 6.12 (2017): 187-196.

when the data fraud becomes apparent. Despite the fact that wholesale fraud occurs in many countries, analysts and law enforcement agencies are plagued by a lack of data and information about the crime all over the world. Regardless, cybercrime is clearly a global concern[150].

2.4.2. Impact of cybercrime on Economy

The prospect of a global town has become a reality in the twentieth century, as modern innovation has interconnected and enmeshed the world's economies, societies, and populations. India is no special case, with more than 560 million web clients starting at 2020, making it the second-biggest web populace on the planet. While more noteworthy network through the World Wide Web (www) guarantees huge scope progress, it additionally leaves our computerized social orders open to new weaknesses. "The expense of working together in the computerized age is to ensure your IT frameworks and ventures, and the monetary effect of digital wrongdoing ought to be quite possibly the main things organizations are zeroing in on in light of the fact that inability to secure their protected innovation [IP], monetary data and IT networks has a financial effect." Cyber violations know no lines and develop at a speed at standard with arising advancements.

As indicated by specialists, an excessive amount of consideration is paid to which country or digital wrongdoing bunch is behind assaults to distinguish who is at fault, though the more significant spotlight ought to be on the financial effect, how that can be diminished and the profit from interest in digital guards "Actually digital wrongdoing is only a development of conventional wrongdoing and straightforwardly affects financial development, occupations, advancement and speculation," he said. "Organizations need to comprehend that in this day and age, digital danger is business hazard." IP burglary alone records for at any rate 25% of the expense of digital wrongdoing and undermines public safety when it includes military innovation, the report said. "IP robbery and loss of chance are two spaces of digital wrongdoing sway that are incredibly hard to gauge, however we have seen that IP burglary and lost freedoms can be lethal for organizations, particularly for little and medium-sized organizations," said business chief. Digital assaults in the nation made monetary harms the tune of about According to a review, USD 500,000 has been given to India-based groups in the last 12 and a half years.

[150] https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy

The following are the types of digital misconduct that have the largest financial impact:

- The deficiency of IP and business-secret data.
- Online extortion and financial crimes are typically the result of identifiable data being obtained.
- Coordinated financial control for firms that are traded on an open market.
- Reduced trust in online workouts due to opportunity costs, recalling interruption for creation or advantages.
- The cost of setting up networks, purchasing digital security, and paying for digital attack recovery. * The cost of reputational damage and liability risk to the impacted firm and its image.

"Digital assaults can strike financial blows, derail India's intended economic path, and damage relations with our neighbors, triggering a state of insurgency," according to a recent assessment. The paper stated that the rise in advanced installments and expanded development of India's computerized economy to $1 trillion in the next 5-7 years from $270 billion presently is opening up flaws that can be exploited by foes[151].

2.4.3. Impact of cybercrime on Piracy

The web and other advanced methods for correspondence and distribution have taken the greatest jump among every one of the mechanical improvements saw in the previous twenty years. With about 566 million web users, India has risen to become the world's second largest online market, with 251 million in rural India. Cell phones are used by 97 percent of the Indian population, with an average monthly data usage of 9.8 GB per client.

Roughly 900 satellite TV stations, 6,000 multi-framework administrators, 60,000 neighborhood link administrators and seven Direct-to-Home (DTH) specialist co-ops are as of now working in the country. The media and media outlet in India has developed at a Compound Annual Growth Rate (CAGR) of 10.9% from monetary year 2017-18.

Media utilization has developed at a CAGR of 9% during 2012-18, right around multiple times that of the USA and multiple times that of China. From April 2000 to December 2018, unfamiliar direct speculation inflows in the data and broadcasting area arrived at USD7.5 billion. In any case, corresponding to the acceleration in the utilization of advanced media and

[151] https://www.dailyexcelsior.com/impact-of-cyber-crimes-on-indian-economy

extension of related ventures, theft has expanded quickly, bringing about a decrease in the products of work for copyright proprietors

Piracy alludes to the unapproved replicating, appropriation and selling of protected works. Before the appearance of internet web-based stages in India, Netflix, Amazon Prime, Amazon Music, Wynk, and other unlicensed sites and deluges were popular among film and television fans who had the 'no-cost' option. elective for downloading/streaming such substance. At the point when it came to music and sound accounts, downloading music from unapproved sites was gone in as the typical direction for a wide scope of crowds who were not even mindful that such conveyance of music was unlawful and unapproved.

Piracy has not just influenced the due benefits of legitimate copyright proprietors yet has given a significant hit to the general condition of the economy, which has seen a deficiency of occupations and income. What makes advanced theft so inclined to chance and hard to check is the failure of copyright proprietors to recognize the infringers because of the ubiquitous idea of computerized media and the resultant outstanding number of privateers.

The public authority of India (GOI) and different offices thereunder have been aware of this mechanical danger, and different drives have been taken at primary and strategy levels to battle something very similar. The ceaseless and ceaseless upgrades alongside the broad and far-located changes at the authoritative and managerial levels have brought about reinforcing the organization, the executives and authorization of licensed innovation rights (IPRs)[152].

2.4.4. Impact of cybercrime on social life

Despite the fact that a crime-free society is a myth, that misbehavior is an all-encompassing marvel, and that it is an indistinguishable component of social presence, one may be bothered by the question, 'Why is there such a fuss about crime?' No one can deny that wrongdoing is a social marvel; it is unavoidable; and there is something familiar in wrongdoing because it is one of the hallmark highlights of all social orders that have existed up to this point, whether enlightened or savage; and it is one of the fundamental senses of all human conduct! Nonetheless, It is critical to understand that society concern for the horror rate stems from the potential negative impact it may have on the larger population, not from its propensity. Furthermore, a few persons have been direct victims of misconduct. Victims of misconduct

[152] Combating Copyright Online Piracy in India: Government's Initiatives And Judicial Enforcement March 2020

may lose any assets they have. Security, harmony, money, and property may be essential characteristics since they contribute to the overall disposition of numerous desires[153].

2.4.5. Impact of cybercrime over Socio-Eco-Political provision.

In theory, misbehavior is a living and relative marvel, exposed to the relative socio-political and practical changes occurring in the current social structure. As a result, neither an all-encompassing definition encompassing all aspects of 'wrongdoing' at any point in time is conceivable, nor can a single definition be made relevant to multiple societies. Its dynamism is influenced by the changes that occur in the connected marvel and worth structure generated by these changes.

Unexpectedly financial wrongdoing is on its pinnacle. This plainly mirrors that wrongdoing has its interdependence with other social wonder, financial frameworks and political apparatuses. Additionally, the populace is one of the significant elements affecting rates of wrongdoings. It has been discovered that there is a positive correlation between the increase in the frequency of misbehavior and the population of the country. Other factors influencing wrongdoing include the location of the wrongdoing, the rate of urbanization, the movement of people from neighboring areas, joblessness, pay disparities, PC education in the case of cyber wrongdoing, and so on. At the same time, the monetary wrongdoings are influenced by the financial design of the give society. Because each regulating framework for wrongdoing has a lot to do with the political framework, which recommends standards, makes laws, and implements preventative measures, the political structure and framework also influence wrongdoing in a given society. This clearly demonstrates that any definition of wrongdoing is linked to socio-conservative and political elements[154].

2.4.6. Impact of cybercrime on youngsters

Cyberbullying is a prevalent phobia among today's youngsters. According to a report, it has been more common in the last five years, with youngsters under the age of eighteen being the most vulnerable and feared victims. In our general public, it's becoming a troubling pattern. According to an analysis of data, the most egregious fear of digital misconduct is among young females. When an individual receives threats, nasty words, negative photographs, or unpleasant remarks from another individual, it is known as digital bullying. This is accomplished entirely

[153] Fatima Talat. *Cyber Crimes* 62 (Ed., Eastern Book Company, Lucknow, 2016)
[154] Das, Sumanjit, and Tapaswini Nayak. "Impact of cybercrime: Issues and challenges." International journal of engineering sciences & Emerging technologies 6.2 (2013): 142-153

through the above-mentioned center developments, primarily through the use of the internet. Where sites like Facebook, Orkut, and Twitter clients are more influenced by Cyber Bullying, Digital Bullying should be achievable through visiting, texting, and so on. According to my research, a feared individual can reach a limit of misery, embarrassment, and undermines. Through this analysis, we discovered that if someone is bullied online, they may become disheartened to the point of self-harm.[155]

2.4.7. Impact of cybercrime and national security.

A server storing enormous backups of financial records, dozens of police reports revealing victims' data, incredibly sensitive government systems, and other vital information holding databases was breached by a team of ethical hackers known as Sakura Samurai.

The team analyzed their initial discoveries to identify further potential areas of weakness, which led to the discovery of over 13,000 exposed Personally Identifiable Information (PII) of government personnel and residents. Robert Willis, one of the security researchers, uncovered an application that allows hackers to examine the country's Police Department's forensic reports and tooling, as well as other sensitive police documents.

"These exposed records, coupled with additional SQL server dumps and Rob's [Robert] Police Record Exposure, are enough to constitute a data breach without even entering into any of the servers," said John Jackson, the Sakura Samurai team's lead researcher.They informed the US Department of Defense Cyber Crime Center (DC3), which contacted India's National Critical Infrastructure Information Protection Centre (NCIIPC). On February 8, the security team shared its 34-page threat report with NCIIPC.Despite putting in place a responsible vulnerability disclosure method, the country's nodal agency has yet to give any information on remedial activities or breach reporting processes two weeks later and after many follow-ups (RVDP).

Patching delays, the delay in patching the weakness could deepen the risk as a lot of citizen’s data isn’t being secured properly.

“Their citizens information can be stolen and used on their behalf, resulting in the loss of their accounts, private information sold on the darknet, or used in further campaigns for

[155] Ashok Vardhan, *Digital Crime and its Impact in Present Society* 04 (International Journal of Engineering Research & Technology (IJERT), Digital Crime Vol 1 2020)

social engineering attacks which may result in the loss of money, or other assets," Jackson told The Hindu

The weaknesses in the cyber defense system exposed by Sakura Samurai "needs to be patched in a month, far less if they can manage it," Jackson added.

Usually, fixing exposed credentials and files can be a fast process, but remote code execution weaknesses may take longer to fix as the application needs to be upgraded to its latest version.[156]

The following are the impact of cybercrime on society and it poses a huge challenge to cater that. The most impressive one is the threat to national security of any country. India was vulnerable and was exposed by hackers similarly the cyber security policy was not that good to cater such a large attack.

[156]Available at https://www.thehindu.com/sci-tech/technology/indias-cyber-defenses-breached-and-reported-govt-yet-to-fix-it/article33888110.ece India's cyber defenses breached and reported accessed on 20th Feb 2021 at 6pm.

CHAPTER III

Legal Framework Governing Cyber Security in India

3.1 INTRODUCTION TO CYBER SECURITY

India is rapidly ascending the digital ladder, with “560 million” internet users this year, making it the world's second-largest country. The pandemic is expected to increase this number in 2021, with forecasts of at least 600 million users. These unequivocal findings, on the other hand, emphasize the need for a strong national cybersecurity infrastructure. With India's rapid digitization and data explosion, it's vital to arm yourself with the resources you'll need, including rigorous training, to secure data security and privacy. Furthermore, with a $6.7 billion cybersecurity industry in India, rigorous and stringent cyber regulation is becoming increasingly necessary.

Cybercrime is currently dominating major media headlines worldwide, causing devastation on businesses and individuals alike. Among the most common types of cyber theft include data breaches, identity theft, money theft, and online time theft. Despite the fact that cybersecurity is improving on a daily basis, hackers are constantly refining their game and discovering new ways to sneak into new systems. This highlights the significance of not only improved cybersecurity technology, but also effective cyber regulation. Furthermore, in order to limit cybercrime and fraudsters' efforts, policymakers must be aware of any cybersecurity holes and correct them in real time. Consistent efforts and awareness are essential to control the country's developing risks[157].

The "Information Technology Act of 2000" (the "IT Act") protects against unauthorised use of information, equipment, devices, computer resources, communication devices, and any information stored on them. Cybercrime is any criminal activity that makes use of a computer, device, or network to carry out or facilitate a crime. The Indian courts defined "cybercrime" as an offence committed against individuals or groups of individuals with the criminal intent to intentionally harm another's reputation in “Jaydeep Vrujlal Depani v. State of Gujarat.” Utilizing current telecommunications networks, such as the Internet (including chat rooms,

[157] Available at https://www.appknox.com/blog/cybersecurity-laws-in-india accessed on 10th April 2021

emails, bulletin boards, and groups) and mobile phones (Bluetooth/SMS/MMS), the victim or indirectly cause the victim to suffer physical or emotional harm or loss.[158]

India was one of the first countries to embrace the digital revolution. The country is now gradually implementing the shift to make the society cashless. Apart from eliminating cash transactions, India is also digitising many other aspects. Whether it's for security, traffic management, or commodities manufacturing, the Indian economy is reaping the benefits of digitalization in various disciplines and industries. However, there is always a bitter side to every wonderful thing, and in the case of India, there are plenty. Some of the hazards associated with the digital revolution include breaching, interrupting, manipulating, and tampering with technology or digital platforms. These threats motivate India to develop a strong cyber security system. An anti-cybercrime agency is required in the country to mitigate the risks of a breach[159].

We keep fighting cyberwars to defend our nation's sovereignty, legal authority, and right to privacy against invasive and unidentified attacks. Last year's pandemic prompted a greater reliance on technology and greater usage of networked gadgets and hybrid work environments. As a result, we are more technologically susceptible than we have ever been. In 2020, the Indian government registered 1.16 million cyber security cases, a 3x increase over the previous year. Cyber-attacks in India, like in other countries, risk national security by gaining access to key government infrastructure. Hackers took down the Indian government's two-factor authentication system used to secure its email network three times last month, compromising the emails of several government personnel. Unfortunately, the attack's perpetrators and their operation methods are yet unknown. Every month, we hear about data breaches. Thousands of Indian residents' COVID-19 lab test results were leaked on government websites at the start of 2021. In May of this year, a cyberattack on the networks of an airline data service provider exposed the personal information of 4.5 million airline passengers. “190,000 candidates” in 2020 Common Admission Test participants had their Personally Identifiable Information and test results leaked and sold in the same month. A million credit card records and the details of 180 million pizza orders, including customer names, phone numbers, and email addresses, were hacked in April of this year.

[158] Available at https://www.mondaq.com/Guides/Results/16/100/all/1/India-Cybersecurity-Legal-framework accessed on 10th April 2021
[159] Available at https://www.jigsawacademy.com/cyber-security-in-india-are-we-doing-it-right accessed on 10th April 2021

While cyber threats are well-known, we still lack a national framework that outlines how to deal with them. No essential formal framework is in place to secure critical information infrastructure and other national assets, and no reaction mechanism is in place if either is attacked.

In 2013, the Indian government issued the National Cyber Security Policy (NCSP), which listed numerous strategies for addressing cyber-security threats. Despite the passage of eight years, only a small percentage of the plan has been carried out, and our country remains one of the most targeted. The lack of a comprehensive cybersecurity strategy/policy exposes the firm to higher risk.

For India, there appears to be a ray of hope at the end of the tunnel. The Department of Electronics and Information Technology would have presented India with a National Cybersecurity Policy before we entered 2022 (DeitY).

The government has already expressed its goal of maintaining a safe, secure, resilient, lively, and trusted cyber environment through a new strategy that will serve as a framework for managing data as a national resource, building indigenous capabilities, and performing cyber audits.

However, to attain stability and security, India must design and implement a collaborative strategy in the area of cybersecurity. Three critical aspects should be addressed in the updated Cybersecurity Policy for 2021:

1. Legal Framework - Although India has no separate cybersecurity law, the Information Technology (IT) Act of 2000 covers cybersecurity and associated offenses. Both “the Companies (Management and Administration) Rules 2014,” adopted under the Companies Act 2013, and “the Indian Penal Code, 1860” (which punishes offences, including those committed in online), have cybersecurity provisions. Furthermore, agencies such as the RBI, the IRDA Act of 1999, and others, the DOT, and the SEBI have adopted sector-specific laws that require their regulated firms – banks, insurance companies, telecom service providers, and listed entities – to maintain cybersecurity requirements. However, a lot has changed regarding how businesses work and how crimes are perpetrated online. Take, for example, the rise of digital payments, which has resulted in a considerable increase in sophisticated cybercrime involving digital payment transactions. Lending firms provide consumers with rapid, frictionless payment experiences, leaving banks and other institutions in the payment ecosystem

with little time to identify and respond to cyber threats. As a result, "the Information Technology Act of 2000," as revised in 2008, will need to be changed, with cybersecurity criteria aligned with the kind of information assets managed by specific companies.

2. Cyber Response Entity - Any national organization in charge of cyberspace management should have a clear line of authority to use all available resources to their full potential. Unfortunately, no such framework exists. In India, several government entities deal with various elements of cyber security. Cyber experts are assigned to each of our defence services, and even state police have cyber detectives. Experts operating under different government ministries and divisions must work together urgently to achieve a unified aim. A National Cyber Command, for example, might be formed by the government.
3. Data Protection - Data is a valuable national resource, most of which is traded in cyberspace. Most governments and residents in nations using the internet for everyday operations have implemented data protection legislation. The European Union is governed by the GDPR, while the California Consumer Privacy Act governs the United States. Even though numerous Indians have lost data (as widely publicized in the media), the Data Protection Bill was submitted to the Indian Parliament in 2019[160].

No one can deny corporate India's and the government's commitment to modernizing India's cybersecurity standards. Given the rising number of digital financial transactions and the current cyber-attack pace in India, the private sector must improve its interaction with the government.

3.2 HISTORY OF CYBER SECURITY IN INDIA

In the twentieth century, India had a rise in information technology (IT) and a tremendous expansion in e-commerce. Both industries operate in cyberspace and rely on electronic transactions, software, services, devices, and networks, all susceptible to cybercrime. As a result, cybersecurity has emerged as one of the country's main priorities to ensure its safety. The "National Cyber Security Policy of the Department of Electronics and Information Technology" is a policy framework (DeitY). Its goal is to protect public and private

[160]Available at https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053 accessed on 10th April 2021

infrastructure from cyber-attacks. It also intends to protect sensitive data such as personal information, financial and banking information, and data on sovereign nations.

Prior to 2013, India did not have a cyber-security policy. Using papers revealed by "NSA whistleblower Edward Snowden," a major daily newspaper reported in 2013 that the National Security Agency focused much of its eavesdropping on India's domestic politics and its strategic and commercial interests. The public was furious, and the government replied on July 2nd, 2013, by publishing a National Cyber Security Policy 2013[161].

2013 National Cybersecurity Policy

The Cyber Security Policy 2013 provides a clear plan to defend critical infrastructure and give citizens, industry, and government a secure cyberspace. The policy also seeks to avoid any economic volatility caused by cyber-attacks. The top 10 highlights of the 2013 National Cyber Security Policy are as follows.:

1. Establish a National Critical Information Infrastructure Protection Centre (NCIIPC) that is open 24 hours a day, seven days a week to collect strategic information about ICT infrastructure threats and to develop scenarios for response, resolution, and crisis management through effective predictive, preventive, protective, response, and recovery actions.
2. Over the next five years, create a task force of 500,000 cyber security experts through capacity creation, skill development, and training.
3. Create fiscal structures and incentives to incentivize businesses to establish, strengthen, and upgrade cyber security-related information infrastructure.
4. CERT-In is recognized as the national nodal entity for cyber security issues, with appropriate collaboration from local (state) CERT organizations.
5. Every organization should have a chief information security officer (CISO) and a security budget. Open standards are used in cybersecurity.
6. Establishment of a flexible legal framework to address cybersecurity concerns.
7. Increased reliance on Public Key Infrastructure (PKI) in government services Using information security professionals and organisations to assist with e-government projects, as well as to build Centers of Excellence and cyber security concept labs for

[161] Available at https://www.appknox.com/blog/a-glance-at-indias-cybersecurity-laws accessed on 10th April 2021

awareness and skill development via PPP - this is a common thread that runs through all of the policy's efforts..

8. The strategy regularly mentions developing an infrastructure for analysing and certifying reliable ICT security products, as well as the unifying concept of PPP throughout all cyber security activities[162].

The number of crimes employing electronic gadgets is projected to climb as our society becomes more reliant on technology. The Cyber Security Policy starts in the right direction but does not ensure complete freedom from crime. In order to strengthen security, private and public enterprises will have to share responsibility for safeguarding the protection of their customers' information and other sensitive data.

3.3 CHALLENGES IN CYBER SECURITY

Individuals, organizations, and governments all have concerns about cyber security. Keeping our data safe in a world where everything is on the internet, from lovely kitten videos to our vacation journals to our credit card information, is one of the most difficult tasks of Cyber Security. Ransomware, phishing assaults, malware attacks, and other cyber security issues are examples. India ranks 11th globally regarding local cyber-attacks, with 2,299,682 instances reported in the first quarter of 2020.[163]

Various cyber-security dangers and issues in India:

1. Cyber terrorism is a planned, political attack on information, computer systems, computer programmes, and data that results in violence.
2. The Danger of Digital Data Thieves has been more motivated to steal data as internet transactions have grown. Businesses also develop intellectual property, which is an attractive target in and of itself, in addition to mining data (customer information, results of product surveys, and generic market information).
3. Cyber warfare is described as a nation-state or international organisation attacking and attempting to damage another nation's computers or information networks. Concerns about cyber infrastructure number four.
4. Like any other connected system, most equipment and technical systems are subject to cyber-attacks. The government has yet to identify and implement critical information

[162] Ashok Vardhan, *National cyber security policy* 24, (2013)
[163] Available at https://www.jigsawacademy.com/blogs/cyber-security/challenges-of-cyber-security accessed on 10th April 2021

infrastructure protection measures, despite establishing the National Critical Information Infrastructure Protection Centre (NCIIPC).

5. Specialists are in short supply: India is the world's second-largest Internet user after China. India has a modest number of cyber-security experts as compared to the number of internet users.
6. India's approach to cyber security has been haphazard and unsystematic thus far due to a lack of robust law enforcement measures. Despite numerous agencies, policies, and initiatives, their implementation has been inadequate.
7. Inadequate Coordination: Due to too many agencies with overlapping functions, coordination between agencies in the field of cyber security is weak.
8. Cyber-security is critical in today's world of ever-increasing connectivity. Despite the government's numerous proactive steps, much more might be done to strengthen cyber-security in the country. Creating a strong policy and putting it in place correctly is vital.[164]

3.4 CYBERSECURITY IN INDIA: AN EVOLVING CONCERN FOR NATIONAL SECURITY

A huge cyberattack has harmed the Colonial Pipeline, which transfers roughly 45 percent of all fuel consumed on the East Coast of the United States. Fuel supply have been affected, and gas prices have risen in some sections of the country as a result of the ransomware assault. Darkside, a Russian-based criminal organization, has been blamed by US authorities for the attack, although the Russian government has been ruled out so far.

Traffic systems, banks and digital payment systems, electricity grids, oil pipelines, and nuclear reactors are examples of critical infrastructure facilities that must be operating at all times. Security experts have been speculating about the prospect of damaging key infrastructure functions for years. Assertive nations looking to settle geopolitical scores have shown that such disruptions are no longer a pipe dream. Several states have utilized rogue non-state actors as proxies to carry out these destructive cyberattacks in order to avoid being detected.

[164]Available at https://blog.forumias.com/answereddiscuss-various-threats-and-challenges-to-cyber-security-in-india-what-initiatives-are-being-taken-by-the-government-to-enhance-cyber-security-in-india accessed on 10th April 2021

In 2010, the Stuxnet worm, allegedly produced by the US and Israel, illustrated how such disruption may function in practice for the first time. The software was designed to attack Iran's Natanz reactor, a significant nuclear power plant. It caused centrifuges to malfunction, effectively halting the Iranian nuclear program's progress. However, the malware infected over 100,000 computers in 115 countries, causing severe disruptions outside of Iran. In December 2015, suspected Russian hackers broke into power grids in sections of Ukraine during the peak of the winter season, disrupting electricity supplies. The incident followed a standoff between Russia and Ukraine over the disputed territory of Crimea[165].

A debilitating cyberattack on key infrastructure by adversary nations and rogue non-state actors is a clear and present concern for India as well. According to a New York Times story, after the Galwan Valley clashes in June 2020, the Chinese allegedly bombarded the Indian power infrastructure with malware. Recorded Future, a cyber security firm, provided this information. According to the article, the attack was carried out by a hacking organization, ' RedEcho,' backed by the Chinese government. Power Systems Corporation Limited, National Thermal Power Corporation Limited, National Load Despatch Centre (NLDC), RLDCs and SLDCs, the Delhi State Load Despatch Centre, and the Kudgi Power Plant in Karnataka were among those targeted.

"Although the NYT piece does not prove that the attack was carried out by Chinese hackers, the supposition is based on substantial circumstantial evidence because large Chinese malware transmission was noticed towards Indian companies from October to November," Gupta added. No one wants to say this on the record because it would destabilize the India-China relationship, which had just begun to improve following meetings between Foreign Minister S. Jaishankar and his Chinese counterpart Wang Yi, according to Gupta. "However, if the Chinese did it, and it appears they did," he continued, "then this was like firing a shot across the bow."

According to Gupta, the Chinese demonstrated what they could do using malware delivered to Indian power distribution networks, meaning that if they could do it to our commercial capital for an hour, they could do it to the entire country[166].

[165] Available at https://www.gatewayhouse.in/cyber-attacks-on-critical-infrastructure-is-india-ready accessed on 10th April 2021

[166] Available at https://theprint.in/opinion/how-chinese-cyber-attacks-mumbai-blackout-depict-a-new-era-of-low-cost-high-tech-warfare/614892 accessed on 10th April 2021

3.4.1 On Monday, March 1, Maharashtra Energy Minister Nitin Raut said that a New York Times (NYT) report stating that the catastrophic power outage in Mumbai last year i.e. 2021 could have been caused by a cyber-attack from China was correct.

In support of the NYT's assertions, Raut stated that the state government has "established three committees to investigate the problem," and that "we will have a thorough report from the cyber department this evening."

From the start, the Maharashtra cyber agency had suspected a malware attack was to blame for the city's power outage in October of last year i.e. 2021.

Trains were suspended, while stock exchanges and hospitals were closed for hours due to the power outage. For about 10 to 12 hours, several neighborhoods in suburban central Mumbai were without power.

It discovered that the majority of the malware was never used. This suggests that only a small percentage of malware was responsible for the Mumbai power outage.

The malware may have been installed in India's main power plants by the China-linked threat activity group RedEcho, according to the research.

"RedEcho has been shown to methodically use advanced cyber intrusion techniques to discreetly build a foothold in almost a dozen important nodes across the Indian power production and transmission infrastructure," according to Stuart Solomon, Recorded Future's chief operating officer.

It discovered that the majority of the malware was never used. This suggests that only a small percentage of malware was responsible for the Mumbai power outage.

The malware may have been installed in India's main power plants by the China-linked threat activity group RedEcho, according to the research.

"RedEcho has been shown to methodically use advanced cyber intrusion techniques to discreetly build a foothold in almost a dozen important nodes across the Indian power production and transmission infrastructure," according to Stuart Solomon, Recorded Future's chief operating officer[167].

[167] Available at www.businesstoday.in/latest/economy-politics/story/cyber-attack-from-china-behind-mumbai-power-outage-in-2020-289648-2021-03-01 accessed on 10th April 2021

3.4.2 The UIDAI Aadhaar Software has been hacked.

One of the largest data breaches of 2018 occurred when 1.1 billion Indian Aadhaar card details were stolen.

The UIDAI issued an official notification on the data breach, stating that around 210 Indian government websites had been hacked.

Anonymous sellers selling Aadhaar information for Rs. 500 on Whatsapp after the Aadhaar software was hacked, exposing users' Aadhar, PAN, bank account IFSC codes, and other sensitive information. Printouts of Aadhaar cards are also available for Rs.300.

3.4.3 Cyberattack against Cosmos Bank in Pune

During a recent breach in India, hackers stole Rs. 94.42 crores from Cosmos bank. The following is a summary of cyberattacks concerning the economy.

How did they manage it? Hackers accessed the bank's ATM server, taking all card details and erasing cash from 28 countries before withdrawing the funds as soon as they were notified[168].

3.4.4 CERT-In alerts to over 700 entities: Govt in Lok Sabha

On Wednesday, IT Minister Ashwini Vaishnaw informed the Lok Sabha that the Indian Computer Emergency Response Team (CERT-IN) had issued alerts to over 700 firms from various sectors in order to allow active cyber-threat prevention.

CERT-In, India's major cyber security agency, publishes alerts and advisories regarding the most recent cyber threats or vulnerabilities, as well as activities to protect computers and networks, on a daily basis. The risk and intensity of cyber-attacks in India have escalated in recent years.

In a written reply, Vaishnaw shared this information with the Lok Sabha. According to the IT ministry, the government has drafted a draft National Cyber Security Strategy 2021 (NCSS2021), which comprehensively looks at national cyberspace security challenges[169].

[168] Available at https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector accessed on 10th April 2021
[169] Available at https://www.indiatoday.in/india/story/cyber-attacks-rising-in-india-cert-in-alerts-to-over-700-entities-govt-in-lok-sabha-1833783-2021-07-28 accessed on 10th April 2021

3.4.5 Union Bank of India was the target of a cyberattack.

Another terrifying cyberattacks occurred in July 2017, alerting everyone. The attack was directed at the Union Bank of India, one of India's largest banks. The attack began when one of the employees opened an email attachment. This email attachment included malware. It gave the hackers access to the bank's computer system and allowed them to steal data. The email attachment was a fake of a central bank email. The employee disregarded the warnings and trusted the email, allowing the hackers access to the bank's data and Union Bank's access passwords for the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT is used for international transactions.

3.4.6 Kudankulam Nuclear Power Plant was hacked by malware (KKNPP)

On October 20, 2019, authorities acknowledged that the nuclear power plant in Kudankulam had been hacked. Lazarus, a North Korean cyber outfit, launched the attack. This attack was carried out in order to obtain information on thorium-based reactors, which are an alternative to uranium-based reactors. Initially, the National Power Corporation of India (NPCI) denied the cyber-attack, but later admitted that one of its systems had been compromised. They utilized a malware called 'Dtrack' to get access to the company's computer system by exploiting a couple of security flaws[170].

3.4.7 Israeli malware spies on Indian journalists and activists Pegasus

Another major cyberattacks occurred in India in 2019, when the Israeli spyware Pegasus was used to eavesdrop on academics, attorneys, activists, and journalists.

NSO Group utilized Israeli malware dubbed Pegasus to gain access to passwords and text messages on messaging platforms like WhatsApp, according to WhatsApp. Pegasus exploited security flaws in the servers. It allowed government spies to access the personal information of approximately 1,400 users. Pegasus permitted remote hacking and access to anything on the user's (victims') phones. WhatsApp has also announced that it is updating its security features[171].

[170] Available at https://scroll.in/article/943954/what-happened-when-the-kudankulam-nuclear-plant-was-hacked-and-what-real-danger-did-it-pose accessed on 10th April 2021

[171] Available at https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones accessed on 10th April 2021

3.4.8 Attacks on the CoWIN app in India

During the epidemic, the CoWIN app was a beacon of hope for the people of India, assisting them and expediting the entire vaccination process for the vast country. However, this app proved to be appealing bait for hackers looking for easy targets. Hackers used the CoWin app to trick users into installing bogus apps. In January, a number of situations arose as a result of hackers creating fraudulent Aarogya Setu apps. It was used to infect end users' computers with malware. Many people were enticed to download the bogus CoWIN software by the desire to get vaccinated[172].

3.5 CYBER SECURITY FRAMEWORK IN INDIA

India approved the Information Technology Act, 2000 (the "IT Act") on June 9, 2000. The IT Act is based on the UNCITRAL model law for e-commerce. The IT Act's prologue states that the Act's objective is to provide legal legitimacy to electronic transactions. On the other hand, the IT Act's reach goes much beyond its prologue. It addresses various issues, including data protection and security, cybercrime, cyber-adjudication, government-mandated digital communication surveillance, and intermediary accountability.

The last amendment to the IT Act occurred in 2011. Despite a significant increase in cyber fraud, data breaches, and general cyber security threats, the IT Act has remained mostly unchanged for nearly a decade. The Ministry of Electronics and Information Technology ("MeitY") announced in February 2020 that the IT Act would be updated with a stronger emphasis on cyber security framework[173]. Emerging technology, the expansion of digital business models, and a significant increase in cybercrime incidents have prompted the government to expedite updating the IT Act[174].

[172] Available at https://www.republicworld.com/india-news/general-news/cowin-app-hacking-reports-rise-in-indore-madhya-pradesh-police-launches-probe.html https://economictimes.indiatimes.com/tech/ites/meity-seeks-ideas-on-it-act-revamp/articleshow/75017401.

[173] Available at https://economictimes.indiatimes.com/tech/ites/meity-seeks-ideas-on-it-act revamp/articles how/75017401. Hindu, 26 February 2020

[174] Available at https://economictimes.indiatimes.com/tech/ites/meity-seeks-ideas-on-it-act-revamp/articleshow/75017401. *Act revamp*, The Economic Times, 07 April 2020, 2020

3.5.1 INDIAN CONSTITUTION

The Indian Constitution, adopted on January 26, 1950, serves as the supreme law of the land, providing the framework for governance and protecting fundamental rights of its citizens. It is notable for its length, detail, and its commitment to democracy, secularism, and social justice.

Relevance to Cyber Laws in India:

Fundamental Rights: The Constitution guarantees certain fundamental rights, such as the right to freedom of speech and expression (Article 19), right to privacy (implied under Article 21), and right to equality (Article 14). These rights are particularly relevant in the context of cyber laws, ensuring that individuals have the freedom to express themselves online while also safeguarding their privacy and ensuring equal treatment under the law.

Directive Principles of State Policy: While not enforceable by courts, these principles (Article 36-51) provide guidelines for the government to establish a just and equitable society. They include principles related to social justice, economic welfare, and the protection of children and vulnerable groups, which can inform cyber laws aimed at promoting digital inclusion and protecting individuals from cybercrimes.

State Powers and Jurisdiction: The Constitution delineates powers between the central and state governments (Article 245-255). In the context of cyber laws, this allocation of powers affects the jurisdiction of laws related to cybercrimes and regulations governing cyberspace.

Amendment Procedures: The Constitution provides for its own amendment (Article 368). Amendments may be necessary to adapt the legal framework to rapidly evolving technologies and emerging cyber threats.

Judicial Review: The Constitution establishes the Supreme Court of India and empowers it to review laws for their constitutionality (Article 32). This provision allows the judiciary to ensure that cyber laws comply with constitutional principles and do not infringe upon fundamental rights.

Cyber laws in India, such as the Information Technology Act, 2000, and subsequent amendments, are designed to regulate various aspects of cyberspace, including electronic transactions, data protection, cybersecurity, and cybercrimes. These laws operate within the

framework provided by the Indian Constitution, ensuring that they align with constitutional principles and protect the rights of Indian citizens in the digital realm[175].

3.5.2 CRIMINAL LAWS

Criminal laws in India encompass a broad range of statutes and provisions aimed at maintaining public order, safety, and security, as well as ensuring justice for victims of crimes. In recent years, with the proliferation of digital technology and the internet, cyber laws have become an integral part of India's legal framework to address crimes committed in cyberspace. Here's a brief introduction to how criminal laws in India intersect with cyber laws:

Information Technology Act, 2000 (IT Act): This is the primary legislation governing cyber activities and offenses in India. It defines various cybercrimes such as hacking, identity theft, phishing, cyberstalking, cyberterrorism, and distribution of obscene content online. The IT Act also provides for penalties and punishments for these offenses.

Indian Penal Code (IPC): The IPC predates the IT Act and contains provisions that can be applied to cybercrimes. For example, sections related to fraud (Section 420), defamation (Section 499), and harassment (Section 509) can be invoked in cyber contexts. Additionally, provisions related to offenses against the state, such as sedition (Section 124A), may apply to cyber activities.

Evidence Act, 1872: The Indian Evidence Act governs the admissibility of electronic evidence in court proceedings. It establishes the legal framework for the collection, preservation, and presentation of digital evidence, ensuring its authenticity and reliability.

Criminal Procedure Code, 1973 (CrPC): The CrPC outlines the procedural aspects of criminal investigations and trials. It governs matters such as arrest, search and seizure, bail, and trial procedures. These provisions are relevant in the context of cybercrimes investigations and prosecutions.

Specialized Agencies and Authorities: India has established specialized agencies and authorities to investigate and prosecute cybercrimes effectively. This includes the Cyber Crime Investigation Cells (CCICs) at the state level, the Cyber Crime Investigation Unit (CCIUs) at the national level, and the National Cyber Crime Reporting Portal (NCRP) for reporting cybercrimes.

[175] Khosla, Madhav. The Indian Constitution. Oxford University Press, 2012.

International Cooperation: India also collaborates with international agencies and organizations to address transnational cybercrimes. Legal frameworks for extradition, mutual legal assistance treaties (MLATs), and international cooperation mechanisms play a crucial role in tackling cyber offenses with cross-border implications.

Overall, the intersection of criminal laws and cyber laws in India reflects the evolving nature of crime in the digital age. These laws aim to provide a comprehensive framework to investigate, prosecute, and deter cybercrimes while upholding principles of justice, fairness, and human rights in the digital realm[176].

3.5.3 INFORMATION TECHNOLOGY ACT, 2000

The Indian Ministry of Commerce was the first to write the E-Commerce Act of 1998. It was modified in 1999 as the Information Technology Bill, signed into law in May 2000. This arose due to the recommendations of the United Nations Commission on International Trade Law. To promote uniformity in national legislation, the United Nations Commission on International Trade Law (UNCITRAL) issued the Model Law on Electronic Commerce in 1996. After passing the Information Technology Act of 2000, India became the 12th country to pass cyber legislation. As a result of this act, other laws that did not deal with technology-related offences have been revised. The IT Act was updated in 2008.

The Information Technology Act of 2000 is divided into 13 chapters and four schedules (2 of which have been omitted). The legislation establishes legal recognition for digital and electronic signatures to verify electronic records and provisions for e-governance and e-records. It outlines how to protect electronic signatures. It then discusses the sanctions, compensation, and adjudication mechanism that will be used if a discrepancy occurs due to this act. The legislation also specifies the requirements for forming an appeal tribunal and the types of offences this act can investigate. It also contains several other provisions[177].

The Act's Objectives[178]

- The act attempts to legalize alternatives to traditional paper-based communication and data storage. This Act allows for electronic transactions, electronic communication, and

[176] Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber-crime and cyber laws of India." International Research Journal of Engineering and Technology (IRJET) 4.6 (2017): 1633-1640.
[177] Available at http://kanoon.nearlaw.com/2017/10/28/information-technology-act-2000 accessed on 11 May 2021
[178] Available ahttps://www.toppr.com/guides/business-laws-cs/cyber-laws/information-technology-act-2000 accessed on 11 May 2021

electronic submission of papers with government agencies.It acknowledges electronic signatures and digital signatures as valid methods of document authentication.

- Electronic data storage is legally permissible.
- Electronic cash transfers between banks and other financial entities are subject to legal sanctions.
- Allows bankers to keep their books of accounts in an electronic format according to the law.

Characteristics of the Act[179]

- Electronic contracts that are created over secure electronic means are legally binding.
- Legally, digital signatures are recognised.
- Also mentioned are methods for ensuring the security of digital documents and digital signatures.
- A procedure for appointing adjudicating officers to carry out this investigation is mentioned for the purpose of carrying out inquiries under this act.
- The legislation also provides for the establishment of a Cyber Regulatory Appellate Tribunal, which will consider appeals against the Controller's or Adjudicating Officer's judgments or directives.
- Giving the High Court the authority to consider appeals from the Tribunal's decisions.
- Providing for digital signatures

The Act's Applicability[180]

Section 1(2) of the Act stipulates that it applies to the entire country, including Jammu and Kashmir. Because Article 370 was in force at the time of enactment, the government used Article 253 to make the Act applicable to Jammu and Kashmir. Furthermore, when read in connection with Section 75, Section 1(2) specifies that the Act applies to anybody outside India who commits offences under it, as long as the nature of the offence includes a computer or a computer-based network in India. If such an offence is committed, the culprit, regardless of nationality, is subject to penalty under this statute.

[179] Available ahttps://www.vedantu.com/commerce/information-technology-act-2000 accessed on 11 May 2021
[180] https://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html

Except as expressly provided, the Act applies to any act or contravention committed outside India by any person. The Act has some particular exclusions (i.e., places where it does not apply), which are listed below in the First Schedule:

A negotiable document, other than a cheque, as defined by the Negotiable Instruments Act of 1881;

• A power-of-attorney, as specified in Section 1A of the Powers-of-Attorney Act of 1882.

• A trust is defined under Section 3 of the Indian Trusts Act of 1882.

• Any other testamentary disposition, as stated in paragraph (h) of Section 2 of the Indian Succession Act, 1925;

• Any contract for the sale or conveyance of real estate, or any interest in such real estate;

3.5.4 Amendments Brought in The Information Technology Act, 2000[181]

Sections 91-94 of the Information Technology Act of 2000 made changes to four statutes. Schedules 1-4 have been updated to reflect these changes.

The modifications to the Penal Code are listed in the first schedule. It has broadened the definition of the term "document" to include electronic documents.

The modifications to the India Evidence Act are dealt with in the second schedule. It has to do with electronic documents being included in the definition of evidence.

The Banker's Books Evidence Act is amended in the third schedule. The definition of "banker's book" has been changed as a result of this revision. Data from a floppy disk, a disc, a tape, or any other sort of electromagnetic data storage device is included in the printouts. The phrase "certified-copy" has also been changed to include such printouts in its definition.

The Reserve Bank of India Act is amended in the fourth schedule. It is concerned with the regulation of electronic fund transfers between banks or between banks and other financial institutions.

In 2008, a significant change was made. Section 66A(later on Supreme Court strucked down Section 66A of IT Act which allowed arrests for objectionable content online[182]) of the

[181] https://www.meity.gov.in/content/information-technology-act-2000
[182] https://timesofindia.indiatimes.com/india/supreme-court-strikes-down-section-66a-of-it-act-which-allowed-arrests-for-objectionable-content-online/articleshow/46672244

amendment was added, which made it illegal to send "offensive messages." It also included Section 69, which empowered authorities to "intercept, monitor, or decode any information through any computer resource." It also made child pornography, cyber terrorism, and voyeurism illegal. The amendment was enacted without debate in the Lok Sabha on December 22, 2008. The Rajya Sabha approved it the next day. On February 5, 2009, the then-President (Pratibha Patil) signed it.

3.5.5 Objectives of the Information Technology Amendment Act, 2008

- **Expression Freedom**

The first of these issues is the issue of child pornography. It's encouraging to note that the provision on child pornography (s.67B) has been carefully crafted. It exclusively refers to sexualized depictions of actual children and excludes imaginative play-acting by adults, for example. It's unclear from a cursory reading of the passage whether drawings featuring minors will be considered illegal as well. Regrettably, the clause applies to everyone who engages in the conducts listed in the section, including children. The age of "children" is specified in the explanation to section 67B as older than the age of sexual consent, which creates some discomfort. So, until the age of eighteen, a person who is legally capable of having sex may not videotape such conduct (even for private purposes).

Another issue is that the term "transmit" has only been defined in the context of section 66E. In sections 67, 67A, and 67B, the word "causes to be communicated" is used. On the surface, that statement appears to contain both the recipient who begins a transfer and the person whose server the data is delivered from. The individual charged with obscenity in India, on the other hand, is usually the one who develops and distributes the obscene material, not the one who consumes it. This new amendment may cause that position to shift.

Section 66A[183], which punishes people for sending harmful comments, is far too wide and clearly violates our Constitution's Art. 19(1)(a). The fact that some information is "grossly offensive" (s.66A(a)) or causes "annoyance" or "inconvenience" (s.66A(c)) while being known to be false cannot be used to limit freedom of speech unless it is directly related to decency or morality, public order, or defamation (or any of the four other grounds listed in Art. 19(2)). Many feel that John Stuart Mill's harm principle, rather than Joel Feinberg's offence principle, provides a superior framework for freedom of expression. The second half of s.66A(c), which

[183] https://www.drishtiias.com/daily-updates/daily-news-analysis/section-66a-of-the-it-act

deals with deceit, is enough to combat spam and phishing, hence the first half, which deals with irritation or inconvenience, is unnecessary. It would also be good if an explanation could be added to s.66A(c) to clarify what "origin" in that section means. Because s.66A(c) can unintentionally prevent organizations from using proxy servers and a person from using a sender envelope other than the "from" address in an e-mail depending on how the word is constructed (a feature that many e-mail providers like Gmail implement to allow people to send mails from their work account while being logged in to their personal account). It may also impede the use of remailers, tunneling, and other methods of online anonymity. This does not appear to be what the legislature intended, yet the section could end up having that impact. As a result, this should be clarified.

The Central Government has the authority under Section 69A to "give orders for limiting public access to any information through any computer resource." In English, this means that the government has the authority to restrict any website. No rules have been established, despite the fact that necessity or expediency in terms of specific restricted interests has been specified. According to s.69A (2), those recommendations "must be such as may be imposed." Before any censorship powers are provided to any authority, it must be assured that they are prescribed beforehand. Any law in India that grants an administrative power unguided discretion to implement censorship is clearly unjustifiable (In re Venugopal, AIR 1954 Mad 901[184]).

- **Liability of the Intermediary[185]**

While the adjustment to the intermediary liability clause (s.79) is a step in the right direction in that it attempts to hold only the law's genuine violators accountable, it is still insufficient. This exemption needs to be stated widely in order to encourage innovation and allow for corporate and public content sharing programs, including through peer-to-peer technologies.

For starters, the demand that content be taken down after receiving "real knowledge" is far too onerous for intermediaries. As a result of this necessity, the intermediary, rather than the authorized authority, is forced to make choices (which often is the judiciary). Because deciding whether a Gauguin painting of Tahitian women is obscene or not requires judicial

[184] https://indiankanoon.org/doc/1280775/
[185] https://www.mondaq.com/india/telecoms-mobile-cable-communications/225328/intermediaries-under-the-information-technology-amendment-act-2008

application of mind, the intermediary is in no position to do so. Second, that requirement violates natural justice and free speech principles by allowing a communication and news medium to be silenced without giving it, or the party communicating through it, a fair hearing. Our courts have ruled that a restriction that denies affected people the right to be heard is procedurally unjust (Virendra v. State of Punjab, AIR 1957 SC 896).

The act's protection is withdrawn if the intermediary (a) initiates the transfer, (b) picks the receiver of the transmission, and (c) selects or modifies the information. The first two are required in order to be considered "intermediaries," while the third is extremely broad. An intermediate, for example, may automatically inject advertising into all transmissions, but this alteration has no bearing on the transmission's essential functionality or makes it liable in any way. Similarly, the intermediary may create a code of conduct and limit transmissions based on explicit language (which is easier to judge), but it would be unable to determine whether copyrighted materials are being used fairly. As a result, because copyright infringement may be forbidden by the intermediary's terms and conditions of use, that form of "option" should not hold the intermediary accountable.

- **Surveillance and Privacy[186]**

While the potential of cyber-terrorism is very real, blanket traffic monitoring is not the way to go if you want to obtain results, and it will almost certainly backfire. A needle is considerably easier to find in a little bale of hay than in a haystack. As a result, it must be assured that the powers given by those provisions are not exercised until the procedures and safeguards described in sub-sections 69(2) and 69B(2) are drafted. Instead of receiving information overload from unchanneled monitoring of massive amounts of data, Small-scale, focused monitoring of metadata (dubbed "traffic data" in the Bill) is a far more appropriate strategy for achieving results. If such safeguards are not in place, the constitutionality of the powers may be questioned due to the lack of supervised execution of such powers.

Importantly, the government must follow up on these authority by being transparent about the kind of monitoring it conducts to ensure that our Constitution's civil and human rights are always maintained.

[186] https://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy

- **Other Penal Provisions[187]**

The definition of "cyberterrorism" in Section 66F(1)(B) is far too broad, and covers unauthorised access to material on a computer with the belief that the information could be used to harm decency, morals, or even defamation. While there is no universally acknowledged definition of cyberterrorism, it is difficult to imagine defamation being considered a terrorist act.

S.43, which refers to "diminishing its worth or utility" while referring to information stored on a computer, is also excessively broad and unguided by the statute. The act of reducing the value of information stored on a computer could be accomplished in a variety of ways; for example, a conscientious whistleblower copying unpublished data could fall under this provision. While the statutory interpretation concept of noscitur a socii (that the word must be understood by the company it maintains) could be used, it doesn't provide much guidance in this circumstance.

While all offenses punishable by more than three years in jail have been rendered cognizable, they have also been made bailable and lesser offenses compoundable. This is a welcome change, especially considering the genuine potential of erroneous imprisonments (as in the Airtel case) and the number of false cases being filed (Orkut obscenity cases).

Personation cheating isn't defined, and it's unclear whether it relates to cheating as defined by the Indian Penal Code when done using communication devices, or if it's a new category of crime. In the latter case, it is unclear whether the court will give those words a narrower meaning, such that only phishing will be punished, or whether other forms of anonymous communication or disputes in virtual worlds (such as Second Life) will be brought under the definition of "personation" and "cheating."

While it is important to remember that additional law is not always the answer to dealing with problems, whether online or off, it is encouraging to see the government attempting to address the emerging issues that have evolved as a result of newer technologies. However, both the court and law enforcement officials must be trained in order to reduce the chance of innocent persons being harassed.

[187] https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008

3.5.6 Bharatiya Nyaya Sanhita 2023 (BNS)

The Bharatiya Nyaya Sanhita Bill of 2023, presented in the Lok Sabha on August 11, 2023, aims to overhaul the existing legal framework, including the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872. This bill proposes significant changes to the Indian Penal Code, with a focus on modernizing and streamlining its provisions. One of the primary goals of the Bharatiya Nyaya Sanhita Bill is to condense the Indian Penal Code, reducing its length from 511 sections to 358 sections. This restructuring aims to make the legal framework more concise and accessible while addressing contemporary issues.

The bill introduces new offenses such as hate speech and terrorism, reflecting the evolving nature of criminal activities. Additionally, it redefines sedition, categorizing it as acts that endanger the sovereignty, unity, and integrity of India.A key aspect of the proposed changes is the consolidation of offenses against women, children, and murder into dedicated chapters. This reorganization enhances clarity and efficiency in addressing legal matters related to offenses against individuals.Furthermore, the Bharatiya Nyaya Sanhita Bill introduces uniformity in terminology, replacing expressions like 'minor' and 'child under the age of eighteen years' with the term 'child' throughout the legislation. This simplification aims to provide consistency and ease of interpretation.

Notably, the bill introduces community service as a punishment for certain offenses, marking a departure from traditional forms of punishment. This innovative approach aims to reform offenders and encourage positive contributions to society, reflecting a commitment to fairness and rehabilitation.Overall, the Bharatiya Nyaya Sanhita Bill of 2023 represents a comprehensive effort to modernize and streamline the legal framework, addressing contemporary challenges while promoting fairness and accountability in society[188].

The Bharatiya Nyaya Sanhita (BNS), 2023, introduces extensive amendments to the Indian legal framework, with notable changes aimed at modernizing and addressing contemporary challenges. Here's a summary of the key provisions:

[188] https://www.legalserviceindia.com/legal/article-14910-bharatiya-nyaya-sanhita-2023-transformative-revisions-and-noteworthy-additions.html

The Bharatiya Nyaya Sanhita (BNS), 2023, marks a significant milestone in India's legal landscape with its expansive reforms aimed at modernizing the legal framework. One notable aspect is the expanded jurisdiction outlined in Section 48, which holds individuals accountable outside India for planning and facilitating crimes within its borders. This provision strengthens India's ability to combat transnational crimes and ensure justice for its citizens regardless of where the offenses originate. Moreover, the inclusion of new offenses such as 'snatching' under Section 304 addresses gaps in previous legislation, reflecting a proactive approach to addressing emerging societal challenges.

In line with efforts to protect women's rights, Section 69 introduces an offense for engaging in sexual activity based on false promises, emphasizing the importance of genuine consent. Additionally, Section 70(2) eliminates age-based punishments for gang rape, mandating rigorous penalties regardless of the victim's age, thus ensuring equal justice for all victims. Gender neutrality is also prioritized through Sections 76 and 77, which make offenses like assault and voyeurism gender-neutral, reinforcing the principle of equal protection under the law[189].

The BNS, 2023, underscores the protection of vulnerable groups, including minors and individuals with disabilities. Section 95 penalizes involving children in criminal activities, prioritizing their well-being and safeguarding their future. Furthermore, Section 117(3) mandates rigorous imprisonment for offenses resulting in severe disability, reflecting a commitment to ensuring appropriate consequences for actions that cause lasting harm. The inclusion of provisions addressing organized crime, terrorism, and national security concerns, such as Sections 111, 113, and 197(1)(d), demonstrates the legislation's holistic approach to ensuring public safety and upholding national integrity[190].

In addition to substantive reforms, the BNS, 2023, emphasizes modernization and clarity in legal language, reflecting a commitment to accessibility and transparency in the legal system. By eliminating derogatory terms and colonial remnants, the legislation promotes inclusivity and respect for all individuals. Rationalization of penalties, enhanced terms of imprisonment, and mandatory minimum punishments for certain offenses reflect a calibrated approach to aligning penalties with the severity of crimes and societal standards. Overall, the Bharatiya Nyaya Sanhita (BNS), 2023, represents a comprehensive overhaul of the legal

[189] https://www.azbpartners.com/bank/overview-of-the-bharatiya-nyaya-sanhita-2023-penal-code
[190] https://prsindia.org/billtrack/the-bharatiya-nyaya-second-sanhita-2023

framework, aimed at addressing contemporary challenges, protecting vulnerable groups, and ensuring justice and fairness in society.

3.5.7 Important advancements in India's cyber security framework-

The Indian Computer Emergency Response Team (ICERT) –

The MeitY appointed the Indian Computer Emergency Response Team ("CERT-In") as the authority to issue instructions for blocking websites under the IT Act to combat online obscenity on February 23, 2003[191]. CERT-In was later named the national agency in charge of responding to cyber-security issues in 2009[192]. The CERT-In is currently responsible for the following tasks[193]:

a. Gathering, analysing, and sharing information on cyber occurrences;

b. Increasing citizen knowledge of cyber security;

c. Issuing information security policies, procedures, prevention, response, and reporting of cyber incidents guidelines, advisories, and vulnerability notices. For example, in December 2019, the CERT-In issued a vulnerability note on the StrandHogg[194] vulnerability in the Android operating system.

A.Establishment of a committee of experts to examine the IT Act-

In 2005, the former Ministry of Communications and Information Technology established a committee of experts to study the IT Act. The committee recommended that the framework for computer-related offences be strengthened in their report. It also advocated developing a strong system to address data protection and privacy issues.

As a result, the following significant adjustments were proposed[195]

a. Computer offences are prosecuted differently- Section 43 of the IT Act provides for compensation in a variety of situations, including unlawful access to a computer system, data theft, and virus transmission via a computer system. Hacking a computer

[191] Procedure for blocking of websites under the Information Technology Act 2000, MeitY, https://meity.gov.in/content/it-act-notification-no-181
[192] Instituted by section 36 of the Information Technology (Amendment) Act 2008 (10 of 2009), w.e.f. 27 October 2009, http://164.100.47.193/BillsPDFFiles/Notification/2006-96-gaz.pdf
[193] Functions of CERT-In, CERT-In, https://www.cert-in.org.in/s2cMainServlet?pageid=CHARTMISSION
[194] StrandHogg vulnerability in Google Android, CERT-In, 09 December 2019, https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2019-0037
[195] Report of the committee of experts on Amendments to IT Act 2000, 2005, https://meity.gov.in/content/report-expert-committee-amendments-it-act-2000

system is a crime under Section 66 of the IT Act. The committee proposed replacing Section 66 with a new section that dealt more thoroughly with computer-related offences. Section 66, which punished computer crimes committed "fraudulently" or "dishonestly," was reworded to be consistent with section 43 of the former IT Act[196].

b. Data protection - To safeguard data security and information protection against unauthorized damage, the committee proposed that any company that processes, deals with, or handles sensitive personal data in a computer resource be held accountable for failing to comply and maintain reasonable security procedures and measures[197].
c. Tougher cybercrime measures – Stricter sanctions have been proposed to combat the issue of child pornography and video voyeurism[198].
d. Based on the recommendations of the Inter-Ministerial Working Group on Cyber Laws and Cyber Forensics, broad powers of monitoring, interception, and decryption of any information via any computer resource were proposed to be transferred from the Controller of Certifying Authority to the central government.

The set of revisions proposed by these suggestions cleared the path for the government to take data protection and cyber security into account in its later attempts to reform the IT Act.

B. Recommendations of the Standing Committee on Information Technology on the Information Technology (Amendment) Bill 2006-

The government introduced the IT (Amendment) Bill, 2006 ("Amendment Bill") in December 2006, based on the committee of experts' recommendations. It was later forwarded to the standing committee on information technology for assessment. The government's approach of revising the existing IT Act rather than establishing new and unique legislation for managing information technology was criticized by the standing committee on IT in its 50th report released in 2007[199]. In its report, the standing committee on IT emphasised the following points:

[196] The committee of experts proposed to substitute the provision under section 66 pertaining to hacking of computer system with a provision that comprehensively dealt with offences related to damages to computer system.
[197] The committee of experts proposed to insert a new section, viz. 43(2) in the then Information Technology Act, 2000.
[198] The committee of experts proposed to insert a new section, viz. 67(2) in the then Information Technology Act, 2000
[199] Report of the standing committee on IT, September 2007, https://www.prsindia.org/sites/default/files/bill_files/scr1198750551_Information_Technology.pdf

a. Specific cybercrime and cyber terrorism issues– The committee emphasised the Amendment Bill's weakness in dealing with cybercrime, especially cyber terrorism. It was pointed out that cyber terrorism was not mentioned in the proposed IT Act revisions. The committee highlighted reservations about the government's intention to amend the IT Act to match it with the Indian Penal Code ("IPC"). According to the research, the IPC is an outdated statute that is ill-equipped to deal with a wide range of cybercrimes, including cyber terrorism. To properly deal with such offences, the committee proposed that adequate, stringent, precise, and self-enabling regulations be incorporated into the IT Act itself.
b. Cross-border cybercrime– According to the committee, entering into Mutual Legal Assistance Treaties with one country at a time to deal with cross-border cybercrime provides a 'piecemeal' solution. As a result, the committee suggested that the government develop a plan to join an omnibus international treaty on cybercrime in order to effectively handle the problem.
c. Child pornography– The committee suggested including clear measures in the Amendment Bill to address child pornography. This would bring it in line with the legislation of other developed countries, as well as Article 9 of the Council of Europe Convention on Cybercrime.
d. Interception powers - The committee questioned why the central government should have the authority to issue orders for the interception or surveillance of any information through any computer resource. It was noted that because 'public order' and 'police' are state issues under the Indian Constitution[200], state governments should have the authority to intercept any information. The proposed law will also be in line with the powers of interception granted to state governments under the Indian Telegraph Act of 1885[201].
e. CERT-In Status– The committee observed in its report that, despite the fact that CERT-In has been designated as the national agency for cyber security, the body's status has yet to be defined. As a result, the committee recommended that the agency be defined as a government body in order to eliminate any uncertainty about its position. This will give international investors' confidence that the government has a legitimate legal structure in place.

[200] Entries 1 and 2, List II, Seventh Schedule, Constitution of India.
[201] Section 5(2), Indian Telegraph Act, 1855.

C. The data Technology (Amendment) Act, 2008-

The IT (Amendment) Act 2008 ("Amendment Act") was passed by Parliament in the Gregorian calendar month of 2008. The following notable adjustments were made as a result of the change Act:

a. Laptop-related offenses– The new law made it illegal to send unpleasant messages or information for the purpose of causing irritation, inconvenience, or other harm to another person using a laptop resource and communication service. However, the Supreme Court of India later struck down this provision in the Shreya Singhal case.[202].

b. In support with the commission's recommendations, the Change Act empowered both the federal and state governments to issue orders for the interception/monitoring of any information under Section 609. The scope of the data intercepted was expanded to include transmission, generation, and storage, as opposed to just transfer under the original clause. The modified section also made such interception orders subject to additional safeguards imposed by the Data Technology (Procedure and Safeguards for Interception, Observance, and Cryptography of Information) Rules, 2009 ("Interception Rules").

c. crucial info infrastructure– The amendment legislation coined the phrase "critical information infrastructure" ("CII") to describe a resource whose loss could have a significant impact on national security, public health and safety, and the economy. Further, any pc resource facilitating such CII was selected as a protected system. consequently, the govt. was sceptred to exercise management over such protected systems, additionally to prescribing info security practices and procedures for such a system[203].

d. Nodal agency for CII– In January 2014, the National crucial info Infrastructure Protection Centre ("NCIIPC") was designated[204] because the national nodal agency underneath the provisions of the modification Act[22]. The NCIIPC is to blame for endeavor all measures to shield CII from unauthorized access, modification, use or disclosure.

[202] Shreya Singhal vs. Union of India, (2015) 5 SCC 1, https://meity.gov.in/writereaddata/files/Honorable-Supreme-Court-order-dated-24th-March%202015.pdf
[203] Section 35 of Information Technology (Amendment) Act, 2008, w.e.f. 27 October 2010, http://164.100.47.193/BillsPDFFiles/Notification/2006-96-gaz.pdf
[204] Designation of National Critical Information Infrastructure Protection Centre as the nodal agency in respect of Critical Information Infrastructure, 16 January 2014, https://meity.gov.in/writereaddata/files/S_O_18%28E%29_0.pdf

D. Bill on administrative unit reforms-

Shri Manish Tewari introduced the Intelligence Services (Powers and Regulation) Bill, 2011 ("Intelligence Bill") as a non-public member's bill in March 2011. He is a Lok Sabha Member of Parliament and a member of the Joint Parliamentary Committee studying the Draft Personal Information Protection Bill, 2019. The Intelligence Bill seeks to monitor the operations of three significant Indian intelligence agencies: the Analysis and Analysis Wing ("RAW"), the Intelligence Bureau ("IB"), and the National Technical Analysis Organisation ("NTAO") ("NTRO"). The Bill asserted that such intelligence agencies' police work operations violate people's right to privacy. It proposed a National Intelligence and Security Oversight Committee ("NISOC") to prevent intelligence services from abusing their police work authorities. The NISOC was sceptred to hunt any info that these agencies possessed. to boot, the Intelligence Bill provided for a National Intelligence court to carry these agencies responsible. The court was sceptred to analyze complaints filed by anyone for action taken against her or her property by these agencies. However, the Intelligence Bill, like most personal member bills, ne'er came up for discussion.

E. National Cyber Security Policy, 2013-

The National Cyber Security Policy ("NCSP") was announced in July 2013 by the former Ministry of Communication and Data Technology.)[205]. supported the objectives unreal within the NCSP 2013, the subsequent strategies/initiatives were introduced by the Indian government:

a. Designation of the NCIIPC because the nodal agency to undertake measures to secure the country's CII.

b. Cyber Swachhta Kendra initiative underneath the CERT-In to combat and analyse any malicious infections/attacks that injury laptop systems. The initiative is geared toward securing the cyber scheme by preventing such attacks from going down and cleanup the systems that have already been infected[206].

c. Development of quadripartite relationships within the space of cyber security. In 2016, Asian nation partnered with the United States of America for coordinative best practices in relevancy

[205] https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf National Cyber Security Policy, 2013 , 02July
[206] Cyber Swachhta Kendra, https://www.cyberswachhtakendra.gov.in/

cyber security and exchanging info in real time concerning malicious cyberattacks, among different things[207].

d. putting in of the National Cyber Coordination Centre ("NCCC") to make situational awareness concerning cyber security threats and modify timely info sharing for preventive action by individual entities[208].

F. Standing committee on IT report on 'Cyber Crime, Cyber Security and Right to Privacy-

In February 2014, the commission on that created the subsequent recommendations in its report on law-breaking, security and privacy[209]

a. The committee ascertained that their square measure twenty totally different styles of cybercrimes. Recognizing the impact of cyber threats on important sectors (such as power, nuclear energy, space, aviation, etc.), it counselled establishing a national protection centre to shield the CII within the country.

b. In managing problems relating cyber frauds, the govt. might have to be compelled to coordinate with multiple establishments, like the bank of Republic of India and also the SEBI. consequently, the committee counselled to make a centralized agency to affect all the cases of cybercrimes.

c. Multiple organizations, including the Ministry of Defence ("MoD"), Ministry of Home Affairs ("MHA"), IB, NTRO, NCIIPC, and others, are concerned about securing the Indian computer network, according to the committee. It further stated that the National Security Council Secretariat ("NSCS") has been tasked with overseeing compliance with cyber security regulations in order to reduce overlap in tasks amongst such entities. However, this might act as a hindrance in combatting cyber threats at the earliest, given the multiple agencies concerned. Recognising the requirement for a cooperative effort between the govt. and also the business to deal with this issue, the committee recommended to implement the recommendations created by a Joint unit ("JWG") that was established below the Deputy

[207] FACT SHEET: Framework for the U.S.-India Cyber Relationship, 07 June 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship

[208] Cyber Security, Press Information Bureau, Government of India, December 2018, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474

[209] 52nd Report of the standing committee on IT on Cybercrime, Cyber security and Right to Privacy, February 2014,

National Security adviser during this regard. The JWG counseled fixing place a permanent mechanism for a Public Personal Partnership ("PPP") on cyber security as an answer, among alternative things.

d. The committee acknowledged that despite the price blessings in hosting servers outside Republic of India, the incidental to technical and legal security considerations posed to the state and citizen's privacy have to be compelled to be due thought. consequently, the committee counseled that government ought to take all steps to confirm that as way as doable, the servers ought to be hosted domestically.

G. Surveillance order issued by MHA–

In Gregorian calendar month 2018, the MHA issued an order under the Interception Rules authorizing 10 security and intelligence agencies to intercept/monitor/decrypt any data transferred, generated, received, or stored on any computer resource. These organizations include the IB, the Narcotics Management Bureau, the Social Control Board of Directors, the Central Board of Direct Taxes, the Central Bureau of Investigation, and the City Police. The decree was extensively condemned and challenged before the Supreme Court on the grounds that it violated the fundamental right to privacy, as outlined in the Puttaswamy case.[210]. The central government defended the order by claiming that it's been passed to pursue a legitimate state aim. what is more, for approved agencies to intercept any info, the govt has submitted that they're going to need to look for the permission of the competent authority[211]. The matter is presently unfinished before the Supreme Court.

H. National Cyber Security Strategy 2020-

In another one among its tries to handle the problems referring to cyber threats and information vulnerabilities, the Indian government has planned to come back out with the National Cyber Security Strategy ("NCSS") 2020. The NCSS intends to examine a variety of issues of cyber security under three pillars: protecting national cyberspace, enhancing structures, people, processes, and capabilities, and synchronizing resources as well as cooperation and collaboration. By the tenth of January 2020, the government had requested

[210] *MHA's snooping order challenged in Supreme Court,* The Economic Times, 24 December 2018, https://economictimes.indiatimes.com/news/politics-and-nation/mhas-snooping-order-challenged-in-supreme-court/articleshow/67232730.cms?from=mdr

[211] *C to hear after four weeks pleas against MHA surveillance notification*, Business Standard, 08 March 2019, https://www.business-standard.com/article/news-ani/sc-to-hear-after-four-weeks-pleas-against-mha-surveillance-notification-119030800545_1.html

opinions and ideas on several parts of the NCSS and is now in the process of defining the policy.[212].

3.5.8 Key Issues on cyber security–

A. Surveillance and privacy-

a) The Secretary of the Union Ministry of Home Affairs/Home Department of a government ("Home Secretary") is designated as the "competent authority" for granting knowledge surveillance/monitoring requests under the IT Act by the Interception Rules. In addition, the Interception Rules provide for a review committee to oversee the responsible authority's orders to intercept/monitor such data. Per the Interception Rules, the review committee is remitted to fulfill at least once in 2 months. Similarly, a committee headed by the cabinet minister reviews state governments' directions.
b) This means that the central government must first consult with the House Secretary before issuing any orders to intercept or monitor any data communication. However, given the large number of interception/monitoring requests generated by the government, the Home Secretary can't analyze each request objectively. As a result, the House Secretary becomes little more than a rubber stamp for government interception demands.
c) Apparently, the Srikrishna Committee report mentioned that AN application filed below the RTI Act discovered that the review committee contains a task of reviewing fifteen,000-18,000 interception orders in each meeting[213]. This chimerical target poses a threat to safety and security of non-public knowledge of people. The committee noted that police investigation mustn't be dispensed while not a degree of transparency which will pass the Puttaswamy check unavoidably, quotient and due process[214].

B. Institutional Diversity –

In its 52nd report, the Standing Committee on IT raised the issue of institutional diversity in cyber security agencies. Because several institutions are tasked with securing cyberspace, there is a lack of cooperation among them. In its 17th report in 2015, the standing committee

[212] National Cyber Security Strategy 2020, https://ncss2020.nic.in/
[213] Pg. 125, Justice Srikrishna Committee Report on data protection: Security of the State, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf
[214] Pg. 124, Justice Srikrishna Committee Report on data protection: Security of the State, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf

on IT presented the government's response to the JWG's proposals to address the issue of several cyber security agencies. According to the report, the government had set the objectives to enhance the overall cooperative framework for a PPP on cyber security in July 2014. However, there was no plan in place to put these recommendations into reality. The issue as such appears to be unresolved with the following agencies dealing presently with the issue of cyber security:

a) MHA's Cyber and Information Security Division: The MHA's Cyber and Information Security Division is in charge of cyber security and cybercrime issues.
b) CERT-In: CERT-In is a MeitY-affiliated organization. Responding to cyber-security issues and publishing security guidelines, advisories, and alerts are among its key responsibilities.
c) NCIIPC: It serves as India's national nodal agency for CII protection.
d) NCCC: It is responsible for providing situational awareness regarding current and potential cyber security threats, as well as enabling fast information sharing for individual entities to take "proactive, preventative, and protective" steps.
e) The Indian Cyber Crime Coordination Centre (I4C) is a non-profit organization that works to combat cybercrime in India. The I4C plan is made up of seven components that the MHA will roll out over the course of 2018-2020. The scheme is made up of seven parts.[215], The National Cybercrime Threat Analytics Unit, the National Cybercrime Forensic Laboratory Ecosystem, and the National Cyber Research and Innovation Centre are among the initiatives.
f) National Cyber Security Coordinator ("NCSC"): The National Cyber Security Coordinator (NCSC) is a position under the Department of Homeland Security It was established as the nodal agency for cyber security under the NSCS. For cyber security issues, the NCSC collaborates with a variety of national agencies.[216]
g) Defense Cyber Agency: The Defense Cyber Agency was established to solve military cyber security and cyber warfare challenges. The Defence Intelligence Agency, which is part of the Ministry of Defense, is in charge of it.[217]

[215] Indian Cyber Crime Coordination Centre (I4C) – A 7-Pronged Scheme to Fight Cyber Crime, Press Information Bureau, Government of India, July 2019, https://pib.gov.in/newsite/PrintRelease.aspx?relid=191878
[216] Cyber Security, Press Information Bureau, Government of India, December 2018, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474
[217] *India's new Defence Cyber Agency*, Medianama, 15 May 2019, https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud

3.6 WORK OF ENFORCEMENT AGENCIES

Enforcement agencies play a critical role in upholding cyber laws in India by investigating cybercrimes, gathering evidence, and prosecuting offenders. Several agencies at the national and state levels are tasked with enforcing cyber laws and ensuring cybersecurity. Here's a detailed overview of some of the key enforcement agencies and their responsibilities:

Cyber Crime Investigation Cells (CCICs): CCICs are established at the state level and are responsible for investigating cybercrimes within their respective jurisdictions. They handle a wide range of cyber offenses, including hacking, online fraud, cyberbullying, cyberstalking, and identity theft. CCICs typically consist of trained personnel with expertise in digital forensics, computer science, and cyber law.

Cyber Crime Investigation Unit (CCIUs): CCIU is the national-level agency responsible for coordinating cybercrime investigations across India. It operates under the Central Bureau of Investigation (CBI), which is India's premier investigating agency. CCIU assists state CCICs in complex cybercrime cases, provides technical expertise, and coordinates with international law enforcement agencies when necessary.

National Cyber Crime Reporting Portal (NCRP): NCRP is an online platform launched by the Ministry of Home Affairs for reporting cybercrimes. It serves as a centralized mechanism for citizens to report cyber incidents and seek assistance from law enforcement agencies. NCRP forwards complaints to the relevant CCICs or other appropriate agencies for further action.

National Investigation Agency (NIA): NIA is a federal agency responsible for investigating and prosecuting offenses with national and international ramifications, including terrorism and organized crime. It has jurisdiction over certain cybercrimes, particularly those with links to national security threats or terrorist activities.

State Police Departments: State police departments are frontline agencies responsible for maintaining law and order within their respective states.

They often have dedicated cybercrime divisions or cells tasked with investigating cyber offenses. State police collaborate with CCICs and other national agencies to address cybercrimes effectively.

Computer Emergency Response Team-India (CERT-In): CERT-In is India's nodal agency for responding to cybersecurity incidents and emergencies. While not primarily an enforcement agency, CERT-In plays a crucial role in coordinating incident response, providing technical assistance, and disseminating cybersecurity alerts and advisories.

Financial Intelligence Unit-India (FIU-IND): FIU-IND is responsible for combating money laundering and terrorist financing activities. It collaborates with law enforcement agencies to investigate financial cybercrimes, such as online fraud, phishing, and money laundering schemes[218].

3.7 VARIOUS COMMITTEES/REPORTS/POLICIES ON CYBERLAWS

3.7.1 National Cyber Security Policy -2013

The National Cyber Security Policy (NCSP) of India, introduced in 2013, aimed to fortify the nation's cyberspace against emerging threats while fostering a secure environment for citizens, businesses, and government entities. It focused on safeguarding information infrastructure, enhancing readiness to counter cyber threats, and nurturing the growth of the digital economy. Additionally, the policy stressed the importance of legal frameworks to address cybercrime, data protection, and privacy issues, proposing both strengthening existing laws and enacting new legislation where necessary.

The NCSP outlined the establishment of institutional mechanisms such as the National Cyber Security Coordination Centre (NCSCC) to coordinate, monitor, and implement cybersecurity initiatives at the national level. Recognizing the pivotal role of human resources, the policy emphasized capacity-building initiatives through training programs, skill development, and education for cybersecurity professionals, law enforcement agencies, and other stakeholders[219].

International cooperation emerged as a key aspect, with the policy emphasizing collaboration with other countries, international organizations, and industry partners to exchange best practices, share information, and develop joint initiatives to bolster cybersecurity globally. Furthermore, the NCSP outlined strategies for effective cyber incident response,

[218] Ajayi, Emmanuel Femi Gbenga. "Challenges to enforcement of cyber-crimes laws and policy." *Journal of Internet and Information Systems* 6.1 (2016): 1-12.
[219] https://www.geeksforgeeks.org/the-national-cyber-security-policy-2013

including the establishment of incident response teams, development of protocols, and regular drills to test response capabilities.

To stay ahead of evolving cyber threats, the policy underscored the importance of research and development (R&D) in cybersecurity. It proposed initiatives to promote innovation, foster collaboration between academia, industry, and government, and support the development of indigenous cybersecurity technologies and solutions. Public awareness and education were also prioritized, with initiatives aimed at educating citizens, businesses, and government employees about cyber threats, best practices, and preventive measures.

The protection of critical information infrastructure (CII) received special attention, with the NCSP proposing measures to identify and classify critical infrastructure, assess risks, and implement security measures to safeguard against cyber-attacks. Finally, the policy stressed the adoption of cybersecurity standards and best practices across sectors, encouraging organizations to implement robust cybersecurity measures, conduct regular audits, assessments, and comply with relevant standards and regulations. Overall, the NCSP provided a comprehensive framework to address cybersecurity challenges and bolster the resilience of India's cyberspace ecosystem[220].

3.7.2 Justice BN Srikrishna Committee on Data Protection

The Justice BN Srikrishna Committee on Data Protection was constituted by the Government of India in 2017 to draft a comprehensive data protection framework for the country. The committee was led by Justice BN Srikrishna, a retired judge of the Supreme Court of India. Its primary objective was to recommend measures for ensuring the protection of personal data and formulating a robust data protection law in line with global standards.

The committee conducted extensive consultations with various stakeholders, including government agencies, industry experts, civil society organizations, and the general public, to gather inputs and insights on data protection issues. It reviewed existing data protection frameworks and laws from around the world to formulate a set of principles and recommendations tailored to India's unique socio-economic and technological landscape[221].

[220] https://www.india.gov.in/national-cyber-security-policy-2013?page=7
[221] https://prsindia.org/policy/report-summaries/free-and-fair-digital-economy

The committee's report, commonly known as the Srikrishna Report, was submitted to the Ministry of Electronics and Information Technology (MeitY) in July 2018. The report proposed a draft Personal Data Protection Bill, which aimed to regulate the processing of personal data by government agencies as well as private entities. The bill incorporated principles such as data minimization, purpose limitation, consent, transparency, and accountability to safeguard individuals' privacy rights.

Key highlights of the Srikrishna Report and the proposed Personal Data Protection Bill included the establishment of a Data Protection Authority of India (DPA) to oversee compliance with data protection laws, the categorization of certain data as sensitive personal data requiring higher levels of protection, provisions for cross-border data transfers, and mechanisms for grievance redressal and enforcement.

The recommendations of the Justice BN Srikrishna Committee and the draft Personal Data Protection Bill generated significant public discourse and scrutiny. Subsequently, the bill underwent several revisions and amendments based on feedback from stakeholders and parliamentary committees. As of my last update in January 2022, the bill was pending approval and enactment by the Indian Parliament, with ongoing discussions and debates on various aspects of the proposed data protection framework[222].

3.7.3 TK Vishwanathan committee on Cyber security

The TK Vishwanathan Committee on Cybersecurity was established by the Reserve Bank of India (RBI) in 2016 to review the existing framework of cybersecurity in banks and financial institutions. TK Vishwanathan, a former Secretary-General of the Lok Sabha, chaired the committee, which comprised experts from various fields including banking, finance, and cybersecurity.

The primary objective of the committee was to assess the current state of cybersecurity infrastructure and practices within the Indian banking sector and to recommend measures to enhance resilience against cyber threats. The committee conducted a comprehensive review of the cybersecurity landscape, analyzing emerging threats, vulnerabilities, and best practices in the financial industry.

The committee's report outlined various recommendations to strengthen cybersecurity in banks and financial institutions, including the establishment of robust cybersecurity

[222] https://pib.gov.in/newsite/PrintRelease.aspx?relid=169420

frameworks, enhancing collaboration between stakeholders, improving incident response capabilities, and promoting cybersecurity awareness and education among employees and customers[223].

Additionally, the TK Vishwanathan Committee emphasized the importance of implementing advanced technologies and tools such as threat intelligence, encryption, and secure authentication mechanisms to mitigate cyber risks effectively. It also stressed the need for regular audits, assessments, and cyber resilience testing to ensure the effectiveness of cybersecurity measures.

The recommendations of the TK Vishwanathan Committee played a crucial role in shaping the RBI's cybersecurity guidelines and regulations for banks and financial institutions. The committee's insights and proposals continue to inform efforts to enhance cybersecurity resilience across the Indian banking sector, reflecting the ongoing commitment to safeguarding financial systems against cyber threats[224].

3.7.4 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to online gaming

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introduced by the Government of India, aim to regulate digital content, social media, and online intermediaries to ensure accountability, transparency, and compliance with the law. Specifically focusing on online gaming platforms, these rules emphasize user privacy, content moderation, grievance redressal mechanisms, and overall compliance with regulations.

In terms of user privacy, the rules underscore the importance of protecting user personal data. Online gaming platforms are mandated to implement robust data protection measures and obtain explicit consent from users for collecting, storing, and processing their personal information. Additionally, adherence to data retention and sharing guidelines outlined in the rules is required to safeguard user privacy effectively[225].

Content moderation is another critical aspect addressed by the rules concerning online gaming platforms. These platforms are expected to actively moderate and remove content

[223] https://www.meity.gov.in/content/notification-cyber-regulation-advisory-committee
[224] https://beta.ficci.in/ficci-in-news-page.asp?nid=15276
[225] https://www.meity.gov.in/writereaddata/files/NOTICE-Public

deemed unlawful or objectionable, such as content inciting violence, promoting gambling, or violating copyright laws. To fulfill this requirement, platforms must deploy automated tools and human moderators for proactive monitoring and filtering of such content.

The rules further mandate the establishment of a grievance redressal mechanism by online gaming platforms. This mechanism aims to address user complaints and concerns promptly, ensuring a smooth process for users to report issues related to content, privacy, or other matters. Each platform must appoint a grievance officer responsible for receiving and resolving user grievances, and they must ensure easy access and timely resolution of complaints[226].

Compliance and enforcement play a vital role in the implementation of these rules. Online gaming platforms are obligated to comply with the IT rules and any other relevant laws and regulations. Failure to comply may result in penalties, including fines or legal action. The rules empower government authorities to monitor and enforce compliance to ensure the safety and integrity of online gaming platforms, promoting responsible conduct and protecting user rights in the digital space.

Overall, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, bring online gaming platforms under regulatory scrutiny to maintain a safe, ethical, and accountable online environment. Compliance with these rules is essential for online gaming platforms to operate lawfully and maintain trust among users and stakeholders, contributing to the overall integrity of the digital ecosystem.

3.7.5 SEBI- High Powered Steering Committee on cyber security (HPSC-CS) and Information Systems Security Committee (ISSC)

The Securities and Exchange Board of India (SEBI) has established two crucial bodies, the High Powered Steering Committee on Cyber Security (HPSC-CS) and the Information Systems Security Committee (ISSC), to tackle cybersecurity challenges within the Indian financial sector.

The HPSC-CS, formed by SEBI, concentrates on devising strategies and policies aimed at bolstering cybersecurity across Indian capital markets. Its core objective is to identify

[226] https://mib.gov.in/sites/default/files/IT%28Intermediary

potential cyber threats and vulnerabilities within the financial sector and formulate effective measures to mitigate these risks. Comprised of experts from diverse domains including cybersecurity, finance, technology, and regulation, the committee provides comprehensive insights and recommendations to address cybersecurity concerns.

Collaborating with regulatory authorities, government agencies, industry stakeholders, and cybersecurity experts, the HPSC-CS works diligently to develop robust cybersecurity frameworks and guidelines tailored to the unique needs of the securities market. Through its collaborative efforts, the committee endeavors to enhance the resilience of the financial sector against evolving cyber threats[227].

On the other hand, the ISSC operates within SEBI with a focus on overseeing the implementation of cybersecurity measures and ensuring compliance with regulatory requirements. It is primarily responsible for evaluating the cybersecurity posture of market intermediaries such as stock exchanges, brokers, depositories, and other entities operating within the capital markets.

To fulfill its mandate, the ISSC conducts regular assessments, audits, and inspections to monitor the effectiveness of cybersecurity controls and practices adopted by market participants. Moreover, the committee provides guidance and recommendations to market intermediaries to strengthen their cybersecurity infrastructure and respond effectively to emerging cyber threats.

Both the HPSC-CS and ISSC play pivotal roles in safeguarding the integrity, confidentiality, and availability of critical financial systems and information within the Indian capital markets. By contributing to the development of robust cybersecurity frameworks, policies, and practices, these committees mitigate cyber risks and ensure the stability and trustworthiness of the financial ecosystem, ultimately fostering a culture of cybersecurity awareness, resilience, and preparedness[228].

[227] https://www.sebi.gov.in/sebiweb/about/AboutAction.do?doMember
[228] https://www.business-standard.com/article/markets/sebi-expands-committees-on-cyber-security-and-information-security

3.7.6 Cyber Security Guidelines for Government Employees manual

The Cyber Security Guidelines for Government Employees manual provides comprehensive guidance and best practices to ensure the security of government information systems and networks. It emphasizes the critical importance of cybersecurity in protecting sensitive government data from cyber threats and breaches. The manual outlines various security measures and protocols that government employees should adhere to when accessing, handling, and transmitting sensitive information. This includes guidelines on password management, data encryption, and secure communication protocols to safeguard against unauthorized access and data breaches.

Additionally, the manual educates government employees on recognizing and mitigating common cyber threats such as phishing attacks, malware infections, and social engineering scams. It emphasizes the need for regular software updates, antivirus protection, and the use of secure browsing practices to minimize the risk of cyber incidents. The manual also emphasizes the importance of physical security measures to prevent unauthorized access to government IT infrastructure and devices. This includes guidelines on securing workstations, laptops, and mobile devices, as well as implementing access controls and surveillance measures in government facilities.

Furthermore, the manual provides guidance on incident response procedures, outlining the steps that government employees should take in the event of a cyber-incident or data breach. This includes reporting procedures, containment measures, and collaboration with cybersecurity teams to mitigate the impact of the incident and prevent further harm. Overall, the Cyber Security Guidelines for Government Employees manual serves as a comprehensive resource for promoting cybersecurity awareness and best practices among government employees. By following these guidelines, government agencies can enhance their cybersecurity posture and better protect sensitive information assets from evolving cyber threats[229].

3.7.7 Cyber hygiene for cyber space Manual Standing

The "Cyber Hygiene for Cyberspace" manual serves as a foundational document for promoting cybersecurity awareness and best practices among users operating within cyberspace. It outlines essential guidelines and protocols to maintain a secure and resilient

[229] https://infosecawareness.in/pdf/Cyber_Security_Guidelines_for_Govt_Employeesv1.4.pdf

cyber environment, emphasizing the importance of individual responsibility and proactive measures in combating cyber threats.At its core, the manual emphasizes the concept of "cyber hygiene," which refers to the routine practices and habits individuals can adopt to safeguard their digital assets and information. These practices include regular software updates, strong password management, and the use of antivirus software to protect against malware and other cyber threats[230].

One of the key aspects highlighted in the manual is the significance of user education and awareness in mitigating cyber risks. It provides clear and concise instructions on identifying common cyber threats such as phishing emails, malicious websites, and social engineering scams, empowering users to recognize and respond effectively to potential threats. The manual also emphasizes the importance of securing personal devices and networks to prevent unauthorized access and data breaches. This includes guidelines on configuring privacy settings, enabling firewalls, and implementing encryption protocols to safeguard sensitive information from cyber attackers.

Furthermore, the manual stresses the need for regular data backups as a crucial component of cyber hygiene. By regularly backing up important files and data, users can mitigate the impact of ransomware attacks, hardware failures, or other unforeseen incidents that may compromise data integrity. Overall, the "Cyber Hygiene for Cyberspace" manual serves as a practical resource for individuals seeking to enhance their cybersecurity posture and protect themselves against evolving cyber threats. By adopting the recommended practices and incorporating cyber hygiene principles into their daily routines, users can contribute to creating a safer and more secure cyberspace for all[231].

3.7.8 Committee Report on – cyber-crime, cyber security and Right to Privacy by Ministry of communication and Information technology

The Committee Report on Cyber-crime, Cybersecurity, and Right to Privacy by the Ministry of Communication and Information Technology provides valuable insights and recommendations to address the growing challenges posed by cyber threats while safeguarding the fundamental right to privacy in India's digital landscape. This comprehensive report examines the evolving nature of cyber-crime and cybersecurity threats and their implications

[230] https://i4c.mha.gov.in/newsletter-manual.aspx
[231]https://www.researchgate.net/publication/342069141_Cyberhygiene_The_key_Concept_for_Cyber_Security_in_Cyberspace

for individuals, organizations, and the nation as a whole. It highlights the need for robust cybersecurity measures to protect critical infrastructure, sensitive data, and personal information from malicious actors operating in cyberspace.

Moreover, the report underscores the importance of upholding the right to privacy in the digital age, emphasizing the need for legislative frameworks and regulatory mechanisms to protect individuals' privacy rights while ensuring the legitimate use of data by government agencies and private entities. One of the key focus areas of the report is the development of proactive strategies to combat cyber-crime effectively. This includes recommendations for enhancing cybersecurity infrastructure, capacity building initiatives for law enforcement agencies and cybersecurity professionals, and fostering collaboration between government, industry, and academia to address emerging cyber threats[232].

Furthermore, the report advocates for the implementation of robust data protection laws and privacy regulations to safeguard individuals' personal information from unauthorized access, misuse, and exploitation. It calls for the establishment of comprehensive data protection frameworks that strike a balance between privacy rights and legitimate data processing activities. In addition to preventive measures, the report emphasizes the importance of effective incident response and crisis management mechanisms to mitigate the impact of cyber incidents and ensure swift recovery from cyber-attacks. It recommends the development of incident response plans, training programs for stakeholders, and coordination mechanisms to facilitate timely and coordinated responses to cyber incidents.

Overall, the Committee Report on Cyber-crime, Cybersecurity, and Right to Privacy provides a roadmap for addressing the complex challenges posed by cyber threats while upholding the right to privacy in India's digital ecosystem. By implementing the recommendations outlined in the report, policymakers, industry stakeholders, and citizens can work together to create a safer, more secure, and privacy-respecting cyberspace for all[233].

3.7.9 Cyber security Association of India

The Cyber Security Association of India (CSAI) is a prominent organization dedicated to promoting cybersecurity awareness, education, and collaboration within India's digital landscape. Founded with the aim of addressing the increasing cyber threats and vulnerabilities

[232] https://eparlib.nic.in/bitstream/123456789/64330/1/15_Information_Technology_52.pdf
[233] https://prsindia.org/policy/report-summaries/cyber-crime-cyber-security-and-right-to-privacy

faced by individuals, businesses, and government entities, CSAI plays a crucial role in fostering a safer and more secure cyberspace. At its core, CSAI serves as a platform for cybersecurity professionals, researchers, policymakers, and industry stakeholders to come together and exchange knowledge, best practices, and expertise in combating cyber threats. Through its various initiatives and programs, CSAI facilitates networking opportunities, skill development workshops, and collaborative projects to enhance cybersecurity capabilities across different sectors.

CSAI is actively involved in raising awareness about cybersecurity issues and promoting cyber hygiene practices among individuals and organizations. It conducts seminars, webinars, and training sessions on topics such as threat intelligence, risk management, and incident response to empower stakeholders with the knowledge and skills needed to protect themselves against cyber-attacks. Moreover, CSAI engages in advocacy efforts to influence policy development and regulatory frameworks related to cybersecurity in India. By providing input and expertise to policymakers, CSAI contributes to the formulation of effective cybersecurity policies and initiatives aimed at addressing emerging cyber threats and ensuring a resilient cyber ecosystem[234].

In addition to its advocacy and awareness activities, CSAI fosters collaboration and information sharing among its members to strengthen cyber defense capabilities and promote innovation in cybersecurity technologies and solutions. By facilitating partnerships between academia, industry, and government, CSAI encourages the development and adoption of cutting-edge cybersecurity tools and practices. Overall, the Cyber Security Association of India plays a pivotal role in advancing cybersecurity efforts in the country by promoting collaboration, awareness, and advocacy. Through its initiatives and partnerships, CSAI contributes to building a safer and more secure digital environment for all stakeholders, ultimately enhancing India's cybersecurity resilience in the face of evolving cyber threats[235].

3.7.10 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 namely- IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 in relation to online gaming and fake or false information about Central Government business

[234] https://www.ncsai.in/
[235] https://cybersecurityventures.com/cybersecurity-associations/

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, underwent an amendment in 2023, known as the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023. These amendments introduced significant changes regarding online gaming platforms and the dissemination of fake or false information about Central Government business.

Regarding online gaming platforms, the amendments aimed to enhance regulatory oversight and ensure responsible conduct within the online gaming industry. It introduced stricter guidelines for online gaming platforms to adhere to, including measures related to age verification, parental controls, and the prevention of addiction among users, particularly minors. Additionally, the amendments mandated online gaming platforms to implement mechanisms for real-time monitoring and reporting of unlawful activities, such as gambling and betting, to regulatory authorities. Furthermore, the amendments addressed the issue of fake or false information concerning Central Government business disseminated through digital media platforms. In response to growing concerns about misinformation and disinformation, particularly on social media and messaging platforms, the amendments introduced measures to combat the spread of false information related to government affairs. Online intermediaries were required to take proactive steps to identify and remove fake or false content that could potentially mislead the public or undermine the integrity of governmental processes[236].

These amendments reflected the Government of India's commitment to promoting accountability, transparency, and ethical conduct in the digital sphere. By imposing stricter regulations on online gaming platforms and combating the dissemination of fake news about Central Government business, the amendments aimed to foster a safer, more trustworthy digital environment for users while upholding the integrity of governmental institutions. Compliance with these rules was crucial for online platforms to operate lawfully and maintain the trust of users and stakeholders[237].

3.7.11 Report of the Joint committee on the Personal Data Protection Bill 2019

The Report of the Joint Committee on the Personal Data Protection Bill 2019 provides a comprehensive overview of the proposed legislation aimed at safeguarding individuals' personal data in India. The committee was tasked with examining the provisions of the bill and

[236]https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines

[237]https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1914358

making recommendations to strengthen data protection measures while balancing privacy concerns with the needs of businesses and government agencies. One of the key highlights of the report is its emphasis on ensuring robust data protection standards to protect individuals' privacy rights. The committee proposed several amendments to the bill to enhance transparency, accountability, and user consent requirements regarding the collection, processing, and sharing of personal data by both public and private entities.

Moreover, the report addressed concerns related to data localization requirements, cross-border data transfers, and the role of data protection authorities in enforcing compliance with the legislation. It recommended measures to facilitate the free flow of data while also ensuring adequate safeguards to protect sensitive personal information from unauthorized access or misuse. Additionally, the report underscored the importance of promoting innovation and economic growth while upholding data protection principles. It proposed provisions to support the responsible use of data for legitimate purposes such as research, innovation, and public interest activities, while also imposing strict penalties for violations of data protection laws[238].

Furthermore, the report highlighted the need for comprehensive data protection frameworks for sensitive personal data categories such as health data, biometric information, and children's data. It recommended additional safeguards and safeguards for these categories to mitigate the risks of potential misuse or abuse. Overall, the Report of the Joint Committee on the Personal Data Protection Bill 2019 provided valuable insights and recommendations to strengthen data protection measures in India. By addressing key concerns and proposing amendments to the bill, the committee aimed to create a robust legal framework that protects individuals' privacy rights while enabling responsible data use and innovation in the digital economy[239].

[238]https://eparlib.nic.in/bitstream/123456789/835465/1/17_Joint_Committee_on_the_Personal_Data_Protection_Bill_2019_1.pdf
[239] https://prsindia.org/parliamentary-committees/joint-committee-on-the-personal-data-protection-bill-2019

CHAPTER IV

Judicial Attitude Towards Cyber Crimes

4.1 Cyber Crime and Cyber Laws - Judicial Perspective

In India, there was no law governing Cyber Laws, including privacy, jurisdiction, intellectual property rights, and various other legal difficulties. Strict statutory rules are required in response to the growing misuse of technology in order to control criminal activity online and safeguard technology's original intent. The Indian Parliament passed the "INFORMATION TECHNOLOGY ACT, 2000" [ITA- 2000] to safeguard e-commerce, e-governance, and e-banking and provide sanctions and punishments for cybercrimes. The IT Amendment Act, 2008 (ITAA-2008) was passed to update the prior Act.[240]

Applicability and scope

The revision to ITA-2000 in 2008 broadened the scope and applicability of the standard. The term 'communication devices' was broadly defined, including cell phones, personal digital assistants, and any device that transmits text, video, or other data, such as the iPad or similar Wi-Fi and cellular gadgets. The term "electronic signature" was created and defined in the ITAA-2008 as a method of performing legally recognized signatures, despite the ITA-2000's definition of "digital signature" was insufficient to meet the needs of the time. Although one of the signature modes in this document is a digital signature, it also includes biometrics and other cutting-edge techniques for creating electronic signatures.

The power and processes for adjudication are covered in Sections 46 and beyond. A director in the Government of India or a state government may be chosen as an adjudicator by the Central Government under the Act. The Information Technology Secretary is often the designated Adjudicator for all civil claims resulting from data theft and related losses. Only a few applications—mostly from large cities—were submitted during the ITA's first ten years of operation. Nevertheless, the number of complaints made under the ITA is gradually rising.
The first judgement under this section was issued in a case involving ICICI Bank in Chennai, Tamil Nadu, in which the bank was directed to return the applicant for the amount incorrectly

[240] https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective

debited through Internet Banking, as well as expenses and damages. An appeals mechanism is in place as part of this process, and the composition of Furthermore, the Act creates a national Cyber Appellate Tribunal. Every adjudicating officer has civil court powers under the Code of Civil Procedure, and the Cyber Appellate Tribunal likewise has civil court powers.[241]

4.2 THE MAIN ACTS, WHICH GOT AMENDED AFTER THE ENACTMENT OF ITA

4.2.1 Apart from the penalties outlined in the Information Technology Act of 2000, certain offences are also covered by IPC regulations. The following is a list of the IPC provisions, the many cyber offences covered by each Section, and the associated penalties.

Although Section 292 of the IPC: was designed to deal with the sale of pornographic materials, it has evolved in the digital age to deal with several cybercrimes. This clause also controls the electronic publication and transmission of obscene content, sexually explicit activities, exploitation acts involving children, and other similar acts. Even though the offences described above appear identical, the IT Act and the IPC recognise them as separate offences. The punishment for engaging in such behaviour is up to two years in prison and a fine of Rs. 2000. Each of the offences as mentioned earlier could result in a term of up to 5 years in jail and a fine of up to Rs. 5000 if they are committed again.

Cybercrime under Section 354C of the IPC involves taking or disseminating a picture of a woman's private parts or activities without her consent. This section focuses solely on the crime of 'voyeurism,' which includes observing a woman perform sexual actions. If the fundamental requirements of this section (such as gender) are not met, Section 292 of the IPC and Section 66E of the IT Act, 2000, are broad enough to cover similar offenses. First-time offenders face a sentence of 1 to 3 years in jail, while repeat offenders face a sentence of 3 to 7 years in prison.

This part of the IPC defines and punishes ‘stalking,' including physical and cyberstalking. Cyber-stalking occurs when a woman is monitored through electronic communication, the internet, or email, or when she is compelled to communicate or contact someone despite her indifference. The punishment for this offense, according to the latter part of the Section, is imprisonment for up to 3 years for the first offense and up to 5 years for the

[241] https://indiankanoon.org/doc/1076139

second offense, as well as a fine in both cases. The victim in "Kalandi Charan Lenka v. State of Odisha"' got vulgar messages from an unknown number that were detrimental to her reputation. Furthermore, the accused wrote emails and constructed a false Facebook account with modified photographs of the victim. As a result, the High Court found the accused prima facie guilty of cyberstalking under different provisions of the IT Act and Section 354D of the IPC.

Section 379 of the IPC: If a mobile phone, its data, or computer hardware is stolen, Section 379 applies, and the penalty for such a crime can range from 3 years in prison to a fine or both. However, it is important to note that these rules will not apply if the special law, namely the IT Act of 2000, is invoked. In the case of Gagan Harsh Sharma v. The State of Maharashtra, one of the employers discovered that the software and data had been stolen and that someone had broken into the computers and given the employees access to critical information. The employer informed the police, who then filed a case under the IPC's Sections 379, 408, and 420 and other IT Act regulations. The court must decide whether the police can launch a case under the IPC. The court ruled that the matter could not be brought under the IPC since the IT Act had precedence.

Section 411 of the IPC: This is a crime that occurs after the offenses committed and punished under Section 379. Anyone who receives a stolen phone, computer, or data shall be prosecuted under Section 411 of the Indian Penal Code. The material does not have to be in the thief's possession. This provision will be attractive even if it is held by a third party who is aware that it belongs to others. The penalty can be enforced as imprisonment for up to three years, a fine, or both.

Sections 419 and 420 of the IPC: These provisions are connected since they both deal with fraud. These two sections of the IPC deal extensively with crimes such as password theft to achieve fraudulent purposes, the construction of phony websites, and the commission of cyber scams. Email phishing, on the other hand, only violates Section 419 of the IPC when it entails impersonating someone and requesting a password. The severity of the penalties under these statutes is determined by the seriousness of the cybercrime committed. Section 419 provides a maximum punishment of three years in prison or a fine, while Section 420 carries a maximum penalty of seven years in prison or a fine.

Section 465 of the Indian Penal Code: This section mostly addresses the penalties for forgery. Under this Part, crimes, including email spoofing and the production of false documents online are dealt with and punished, carrying a sentence of up to two years in prison, a fine, or both. In the case of Anil Kumar Srivastava v. MHFW, the petitioner digitally forged the AD's signature before bringing a claim alleging false accusations against the same person. Because the petitioner tried to pass it off as a genuine document, he was found responsible under Sections 465 and 471 of the IPC.

Section 468 of the IPC, which carries a punishment of seven years in jail or a fine or both, comes into play if the offences of email spoofing or online forgery are committed to commit other serious offences, such cheating.

Section 469 of the IPC: Anyone who commits forgery exclusively for the aim of discrediting a particular individual or knowing that such forgery hurts a person's reputation, whether in the form of a physical document or through online, electronic forms, can face up to three years in prison and a fine.

Defamation of any individual is punishable under Section 500 of the Indian Penal Code. Anybody who sends abusive or defamatory messages via email will be subject to prosecution under Section 500 of the IPC, which deals with cybercrime. The maximum penalty for violating this clause is two years in prison plus a fine.

Section 504 of the Indian Penal Code: Whenever someone threatens, insults, or attempts to provoke another person by email or electronic to promote peace, it is a crime under Section 504 of the Indian Criminal Code. Up to two years in prison, a fine may be imposed as a punishment for this offence.

Section 506 of the IPC: A person will be charged with an offence under Section 506 of the IPC, which carries a maximum sentence of seven years in prison, a fine, or both, if they attempt to criminally intimidate another person, either physically or through electronic means, regarding a person's life, property destruction through the fire, or a woman's chastity.

Section 509 of the IPC deals with the crime of speaking, gesturing, or acting in a way that would be offensive to a woman's modesty. Invasion of a woman's privacy also includes

sounds made and actions taken. A maximum of a year in jail, a dn a fine, or a combination of both is a possible punishment for this if it is done physically or electronically, according to Section 509 of the law.[242]

4.2.2 India: Use of Electronic Evidence in Judicial Proceedings

The growth of computers and digitalization has been one of humanity's greatest and most transformative inventions. Like other human life, cyberspace has not been immune to threats and criminal activity. This results from the wide range of content and information offered and its accessibility and reach. However, as cyberspace has grown in popularity, there has been a significant surge in its misuse. E-documents' legitimacy has long been contested due to how quickly they may be altered. For law enforcement officials, the admissibility of such electronic evidence is becoming more and more of a challenge. The procedure used to look into and assess material saved on or recovered from electronic media to submit in a court of law is significant because, unlike conventional or traditional evidence, electronic evidence requires specialised and professional cyberspace expertise.

The Evidence Act of 1872 and the Information Technology Act of 2000

The Information Technology Act of 2000 ("IT Act"), as well as associated modifications to the Evidence Act of 1872 ("Evidence Act") and the Indian Penal Code, 1860, established the idea of "electronic evidence" ("IPC"). The model Law on Electronic Commerce created by the United Nations Commission on International Trade Law served as the foundation for the IT Act and subsequent revisions ("UNCITRAL"). The term "electronic record" is defined under Section 2(1)(t) of the IT Act as "data, record, or data generated," "picture or sound saved, received, or conveyed in an electronic form," or "micro-film or computer-generated micro fiche." The legality and usage of electronic records instead of traditional paper-based records is expressly recognized in Section 4 of the IT Act.

Section 92 of the IT Act amended the Evidence Act by expanding the definition of "evidence" to include "electronic record," making digital evidence acceptable. Sections 63 and 65 of the Evidence Act largely dealt with and specified the conditions for the admissibility of electronic evidence before its legal recognition. According to these laws, printed copies of electronic evidence were obtained using various methods. Cyber forensics were considered

[242] https://blog.ipleaders.in/punishments-cyber-crimes-ipc/

secondary evidence and required authentication by a qualified signatory who might be questioned under cross-examination over the certified document. The overriding clause in Section 65B, the exclusion of electronic records under Section 59 of the Evidence Act, and the absence of the term "Electronic Records" from the scheme of Sections 61 to 65 of the Evidence Act all make it clear that the legislature did not intend for those provisions to apply to electronic records.[243]

Electronic Records Admissibility

Section 65A of the Evidence Act states that the contents of electronic documents may be proven by Section 65B of the Evidence Act. As a result, only the method outlined in Section 65B of the Evidence Act can be utilized to establish any documented evidence as an electronic record. Any information contained in an electronic record, whether it be the contents of a document or communication printed on paper, or stored, recorded, or copied in optical or magnetic media produced by a computer, is deemed to be a document and is admissible in evidence without further proof of the original's production, subject to the conditions outlined in Section 65B of the Evidence Act.[244]

Technical and non-technical considerations

Section 65B of the Evidence Act allows for the admissibility of electronic evidence on both technical and non-technical grounds. Section 65B (2) of the Evidence Act specifies the technological conditions under which a duplicate copy (including a printout) of an original electronic record may be utilized. The following are some of them:

a) At the time of creation, the computer that created the electronic record was required to be in regular use;
b) The electronic record's contents must have been loaded into the computer regularly and routinely;
c) The computer was fully functional; and
d) The duplicate electronic document must be an identical original clone.

As can be deduced, the above conditions are related to the data's integrity. The conditions have a two-fold effect: I ensure that the data has not been misused, and ii) they ensure that the device is working properly, ensuring the accuracy and genuineness of the reproduced data.

[243] http:/www.advocatekhoj.com/library/bareacts/informationtechnology
[244] https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/

Suppose a user uses a networked device to store or process information. In that case, all connected devices will be treated as single, according to Section 65B(3) of the Evidence Act.

Authenticity Certificate

A certificate of authenticity is one of the non-technical requirements in Section 65B(4) of the Evidence Act. The objective of the certificate is to conform with the previous sub-section of Section 65B of the Evidence Act (2). The certificate must be executed/signed by a person in charge of the equipment that generated the data. The certificate must identify the electronic record containing the statement, describe how it was formed, and include any information about any device used to develop the electronic record required to verify that a computer created it. Any issues raised by the admissibility standards must be addressed in the certificate. The certificate's sole function is to prove the source's integrity and the data's authenticity so that the Court can trust it. This is critical because electronic data is more subject to tampering and modification.

Certificates are required by law:

In this context, one important question is whether a certificate under **Section 65B of the Evidence Act** is required. The Supreme Court has now answered this question in the affirmative in the case of **"Anwar PV v PK Basheer and Others [(2014) 10 SCC 473]."** This, however, was not the first point of view on the subject. Previously, in **"State (NCT of Delhi) v Navjot Sandhu Afzal Guru, [(2005) 11 SCC 600],"** the Supreme Court, for the first time dealing with the admissibility and evidentiary value of electronic evidence, decided that there is no restriction to adducing secondary evidence under other provisions of the Evidence Act, notably s. Furthermore, additional evidence may be offered in the conditions in the relevant parts of the Evidence Act, namely "**Sections 63 and 65**, even if a certificate containing the information outlined in sub-Section (4) of **Section 65B of the Evidence Act** is not filed. As a result, the Supreme Court did not accord **Section 65B of the Evidence Act**" the legal weight it merited. Despite enacting **"the Information Technology Act in 2000"** and changes to the Evidence Act, the Supreme Court in Anwar PV ruled for the first time that documentary evidence in the form of an electronic record can only be shown using the approach outlined in **Section 65B of the Evidence Act**. In this case, the Supreme Court fully acknowledged and appreciated the importance of **Section 65B of the Evidence Act.**

In that sense, the Supreme Court's finding in **Anwar PV** that a certificate under **Section 65B of the Evidence Act** is required for electronic evidence entry contradicted its earlier decision in Navjot Sandhu. The Supreme Court pointed out that **Section 65B of the Evidence Act** begins with a "non-obstante clause" that would override the Act's general secondary evidence regulations, which are found in **Sections 63 and 65. Section 65B of the Evidence Act** is a one-of-a-kind provision that deals with the proof of electronic records. When read in conjunction with **Sections 59 and 65B of the Evidence Act, Section 65A of the Evidence Act** is sufficient to hold that the specific provisions on evidence relating to electronic records are controlled by the method outlined in **Section 65B of the Evidence Act**. Because this is a whole code in and of itself, the general law under **Sections 63 and 65 of the Evidence Act** must yield to the maxim **"Generalia Specialibus Non-Derogant."**

Because of the Supreme Court's decision in Anwar PV, the duty to comply with the rules of Section 65B of the Evidence Act in cases where an electronic record is made by a party who does not have the device has been reduced. The Supreme Court held in a case involving a similar factual scenario that the procedural requirement for furnishing a certificate under Section 65B(4) of the Evidence Act applies only when electronic evidence is produced by a person who is in a position to produce a such certificate. At the same time, in control of the device, the Court may relax such requirement if the interest of justice so warrants. 1 A two-judge Supreme Court bench has sent the matter to a bigger bench to lay down the law with greater certainty, owing to the ruling as mentioned earlier's lack of confidence[245].

E-mail

Electronic mail, sometimes known as e-mail, is one of the most widely used electronic channels for information communication. Because most official communications between persons occur via e-mail, Indian courts have made such e-mails acceptable in evidence if a printout of the e-mails is filed with the certificate under "Section 65B of the Evidence Act."[246]

The certificate needed by "Section 65B of the Evidence" Act should say that the computer was in the person proving the e-lawful mail's control during the relevant period. That information was often input into the computer in the course of business. It's also worth noting that the

[245] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors 2019 SCC OnLine SC 1553
[246] Abdul Rahaman Kunji v. The State of West Bengal 2014 SCC OnLine Cal 18816

computer was operational, and the printed contents were derived from data fed into the computer during routine business activities.

E-mails can be read into evidence if they fit the criteria mentioned earlier. “Section 88A of the Evidence Act” gives the contents of an electronic message a presumption of validity unless it is conclusively refuted.[247]

This Section, on the other hand, makes no assumptions about the sender of the e-mail. As a result, a printout of an email cannot be given much weight unless and unless a party verifies who the sender was.[248]

WhatsApp and other SMS and instant messaging apps

In contrast to e-mails, which are normally used for formal communications, short messaging services (SMS) or instant messaging services such as WhatsApp are frequently utilised in official and informal talks. In contrast to traditional computers, a readily available mobile phone can be used as evidence. As a result, when the device carrying the message and instant message sent on WhatsApp or any other comparable application is submitted in court, there is no need to file a certificate under Section 65B of the Evidence Act. However, in such cases, ensuring no dispute over the device's ownership or any content changes is vital.

When comparing a computer to a mobile phone, the According to the Hon'ble High Court of Telangana, a mobile phone is a computer that is configured to execute, among other things, the function of receiving digital audio signals and should be understood as a computer under the IT Act's definition of computer and computer network.[249] When the mobile phone containing the Because an SMS or WhatsApp communication cannot be used as evidence, the person who received or transmitted it must file a certificate under Section 65B. While Indian courts have yet to rule on the admissibility of WhatsApp conversations as evidence, it is vital to show appropriate mobile phone possession. Because such messages would be subject to judicial scrutiny, ensuring that no data has been tampered with is vital, as this could compromise the messages' admissibility.

[247] M/s. Xact Studio International v M/s. Liwona SP. Z.O.O 2018 SCC OnLine Del 9469
[248] S. Karunakaran v Srileka 2019 SCC OnLine Mad 1402
[249] Syed Asifuddin v State of Andhra Pradesh 2005 SCC OnLine AP 1100

Records of Phone Calls

The majority of criminal cases start with a check of the accused's phone records. These phone logs are typically used as a jumping-off point for forming a conspiracy with others. Even though call records are stored on large servers that are difficult to move and produce in court, the Hon'ble Supreme Court has held that printouts taken from computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led in evidence through a witness who can identify the signatures of the certifying officer or otherwise speak of the facts based on his knowledge. Adducing additional evidence under Sections 63 and 65 of the Evidence Act is also an option that is not barred if the requirements of Section 65B of the Evidence Act are met.[250]

Photographs

In most cases, a digital camera is not supplied in court; thus, a party must rely on a printout or other storage media like CDs, USB drives, and other similar devices. As a result, the person in charge of handling the digital camera, capturing the photograph, and transferring it to the storage media must attest to how the printout or storage was accomplished. The Hon'ble Delhi High Court clarified this by holding that where a party deposes that he took the images himself, had them processed, and submitted them in the Court, the absence of negatives cannot be used to reject them, especially when the photographs in question are digital photographs.[251]

Use of electronic Media in other judicial proceedings

In addition to electronic records being used as evidence, the use of electronic media in court proceedings for other purposes has increased. While recognising the advantages of electronic media like as emails and WhatsApp messages, the Supreme Court has urged parties and their attorneys to serve the other party via e-mail in addition to traditional methods of service[252] in commercial litigation and litigation involving interim relief. The Hon'ble Bombay High Court[253] has reached a similar conclusion. The Hon'ble Delhi High Court and the Hon'ble Bombay High Court have recently recognized even service via WhatsApp.

The Bankers Book Evidence act 1891 and the Information Technology Act of 2000

[250] State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600
[251] Puneet Prakash v Suresh Kumar Singhal & Anr 2018 SCC OnLine Del 9857
[252] Central Electricity Regulatory Commission v National Hydroelectric Power Corporation Ltd. & Ors. (2010) 10 SCC 280
[253] Dr. Madhav Vishwanath Dawalbhakta v M/s. Bendale Brothers 2018 SCC OnLine Bom 2652

The keeping of records is a fundamental and necessary element of the banking industry. A customer, for example, wishes to deposit $10,000 in a bank. He makes a deposit with a bank, which is acknowledged with a receipt. The banker will next properly record the transaction in a ledger or account book. The customer then claims that he deposited $15,000 in the bank but only received $10,000. The banker will be able to verify it using suitable documentation in this case. The customer merely put down $10,000, according to the bank. If legal action is initiated against the bank, it can produce a certified copy of the record. The Bankers' Books Evidence Act of 1891 creates a legal foundation for bankers' books and verified bank documents.

The Information Technology Act of 2000 modified this Act in response to the introduction of computer systems, which are now used to store records in banking institutions rather than on paper.

The Bankers' Books Evidence Act of 1891 provides guidelines for banking institutions in legal actions involving banking records. This is a statute that was passed in order to alter the law of evidence in the area of banking records. Bookkeeping is done in bank books such as ledger books, registers, account books, and other books used in typical commercial activities. Any discrepancy in these banking records will be treated as a violation of the Act. If a legal action is launched against a banking institution or a firm that performs a banking function, they are required to comply with the provisions of this Act[254].

Amendments

The Bankers' Books Evidence Act of 1891 was amended by the Information Technology Act of 2000, which changed the definition of bankers' books. This Act brought about the following changes:

Previously, ledgers, daybooks, cash books, accounts books, and other books used in the ordinary course of business in a bank were included in the definition of bankers' books. It now covers records recorded on microfilm, magnetic tape, or any other mechanical or electronic data retrieval device after the modification.

[254]https://www.advocatekhoj.com/library/bareacts/bankersbook/index.php?Title=Bankers%20Book%20Evidence%20Act,%201891

Section 2(8)(b) of the Act: The definition of a certified copy was expanded to include a printout of any entry recorded on microfilm, magnetic tape, or any other mechanical or electronic data retrieval method that ensures the accuracy of the printout as a copy of the entry.

2A Section: This section was added to address the certification criteria for the printout form's acceptability of a certified copy. It specifies the certificates the person in charge of the computer system must have.

Recent decisions

"Central Bureau of Investigation v. Om Prakash:" "Section 65B of the Indian Evidence Act" was determined to be pari materia (on the same subject or matter) to Section 2A of the Bankers' Books Evidence Act in this case. As a result, they should be construed as a unit. Furthermore, it was stated in "Anvar P.V. v. P.K. Basheer and Ors"[255] that a special law will always prevail over general law. This means that, while The Indian Evidence Act (Section 65B) provides a provision for electronic records, while the Bankers' Books Evidence Act (Section 2A) contains a provision that deals especially with the admissibility of electronic banking data. Section 2A will be favoured over Section 65 B when dealing with electronic banking records, according to the principle of 'generalia specialibus.'

In "Sonu Amar v. State of Haryana",[256] it was held that If the fault in question could have been corrected at the time of marking the document and the party offering evidence could have used the ordinary mode of proof, the objection to the admission of banking records should be permitted.

"Safiya Bai v. Radheshyam G. Garg Ibrahim Lightwalla"[257]: When a bank agent signs a certificate validating a record as a true copy of the original, kept in the bank's custody in the ordinary course of business, the court should not focus on all of the conditions set out in Section 2(8) of the Act and take a hyper-technical approach, as was held in this case. Section 2(8) of the Act contains advisory rather than mandatory conditions.

4.3 LANDMARK CYBER LAW CASES IN INDIA

[255] https://indiankanoon.org/doc/187283766/
[256] https://indiankanoon.org/doc/25220929/
[257] https://www.lawyerservices.in/Radheshyam-G-Garg-Versus-Safiyabai-Ibrahim-Lightwalla-1987-01-19

As the name implies, Cyber Law is concerned with statutory regulations that govern cyberspace. There has been a significant increase in the number of cyber-crimes reported since the introduction of digitalization and AI (Artificial Intelligence). India recorded 50,035 cases of cyber-crime in 2020, with an 11.8 percent surge in such offences over the previous year, as 578 incidents of "fake news on social media" were also reported , official data showed on September 15 2021[258].The Information Technology Act of 2000 (hereafter referred to as the "IT Act") and the Rules promulgated under it establish India's legal foundation for cyber law. The IT Act is the main piece of legislation that governs various types of cybercrime, as well as the penalties that can be imposed, as well as compliance requirements for intermediaries.

The IT Act, on the other hand, does not cover the entirety of India's Cyber Law regime. There have been several court decisions that have significantly influenced India's cyber law regime. It is necessary to refer to the following landmark Cyber Law cases in India to comprehend the scope of the Cyber Law regime fully:

4.3.1. UOI v. Shreya Singhal[259]

The legality of Section 66A of the IT Act was questioned in this case before the Supreme Court.

Facts: Two women were arrested under Section 66A of the Information Technology Act for allegedly making derogatory and offensive comments on Facebook concerning Mumbai's complete closure following the death of a prominent leader. Section 66A of the IT Act makes it illegal to use a computer resource or communication to transmit content that is offensive, false, or causes irritation, discomfort, danger, insult, hostility, hurt, or ill will.

The women filed a petition challenging the constitutionality of Section 66A of the IT Act, saying that it violates their right to free speech and expression.

The Supreme Court's ruling was guided by three factors: debate, advocacy, and incitement. It was argued that just discussing or even campaigning for an idea, no matter how divisive, is at the essence of free speech and expression. Section 66A was found capable of prohibiting all types of communication, with no distinction made between basic advocacy or

[258] https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece
[259] (2013) 12 SCC 73

discussion on a particular subject that is unpopular with some and utterances that provoke public disruption, security, or health.

The Court declared that it condemns offensive comments that may irritate an individual but do not impair his reputation in response to the question of whether Section 66A intended to protect individuals against defamation.

However, the Court ruled that Section 66A of the IT Act did not violate Article 14 of the Indian Constitution because there was a discernible distinction between material sent via the internet and information communicated via other media. Furthermore, the Supreme Court did not evaluate the procedural unreasonableness issue because it is unconstitutional on substantive grounds.

Decision Overview[260]

The Supreme Court of India's opinion was delivered by Justices Chelameswar and Nariman.

The major question was whether Section 66A of the ITA infringed on Article 19(1)(a) of the Indian Constitution's right to freedom of expression. Article 19(2) allows the government to impose "reasonable restrictions... in the interests of India's sovereignty and integrity, the State's security, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation, or incitement to an offense" as an exception to the right.

Section 66A was deemed unconstitutional by the Petitioners because it was meant to protect people from irritation, discomfort, danger, obstruction, insult, injury, criminal intimidation, or malice (2). They further claimed that the law was unconstitutionally vague because the restrictions were not specified. They also claimed that the regulation has a "chilling impact" on free expression. [paragraph 5]

The government, on the other side, maintained that the legislature is best prepared to address people's needs and that courts should only intervene in the legislative process when "a statute clearly violates the citizen's rights granted under Part-III of the Constitution." [Part 6]

[260] https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/

According to the administration, the mere existence of abuse of a provision may not be enough to declare it unlawful. Furthermore, the government believed that the law's unclear language could not be used to strike it down because it dealt with fresh ways of infringing on people's rights via the internet. According to the government, "if the statute is otherwise legislatively competent and non-arbitrary," ambiguity cannot be used to find a statute unconstitutional. [paragraph 6]

The Court started by talking about three key ideas in comprehending freedom of expression: debate, advocacy, and incitement. "[m]ere discussion or even advocacy of a particular cause, however unpopular, is at the heart" of the right, according to the Court. [paragraph 13] And only when a discussion or advocacy amounts to incitement may the law restrict freedom. [paragraph 13]

As applied to the case at hand, the Court found that Section 66A has the potential to restrict all forms of internet communication because it makes no distinction “between mere discussion or advocacy of a particular point of view, which may be annoying, inconvenient, or grossly offensive to some, and incitement by which such words lead to an imminent causal connection with public disorder, security of the State, or other public safety concerns.” [paragraph 20]

The Court went on to conclude that the law does not have a clear proximate nexus to the safeguarding of public order. According to the Court, sending a message with the aim to irritate or offend someone is enough to violate Section 66A. As a result, the law makes no distinction between extensive distribution and transmission to a single person, and the message does not need to demonstrate a clear tendency to disrupt public order.

When assessing whether Section 66A was a reasonable attempt to protect individuals against defamatory statements made through internet communications, the Court noted that the basic ingredient of defamation is "harm to reputation The law was found to be ineffective in achieving this purpose because it also forbids offensive statements that may annoy or inconvenience an individual without endangering his reputation. [paragraph 43]

The government also failed to show that the law is intended to prevent communications that incite the commission of an offense because "merely causing annoyance, inconvenience,

danger, etc., or being grossly offensive or having a menacing character are not offences under the Penal Code at all," according to the Court. [paragraph 44]

In response to petitioners' claim of vagueness, the Court held that "where no reasonable standards are laid down to define guilt in a Section which creates an offense, and where no clear guidance is given to either law abiding citizens or authorities and courts, a Section which creates an offense and is vague must be struck down as arbitrary and unreasonable." [Section 52] Many wording in Section 66A is left open-ended and ambiguous, according to the Court, making the law unlawful due to its vagueness.

The Court also evaluated whether Section 66A could limit the right to freedom of expression. Because the provision does not define terms like discomfort or annoyance, it was determined that "a tremendous amount of protected and innocent expression" could be limited. [[paragraph 83]

The Supreme Court also stressed the distinction between content transmitted over the internet and other forms of expression, allowing the government to create new offenses for online communications. As a result, petitioners' allegation that Section 66A violated Article 14 of the Constitution, which bans discrimination, was dismissed by the Court. [[paragraph 98]

The Court declined to hear the Petitioners' argument of procedural unreasonableness because the statute had already been declared unconstitutional on substantive grounds. It also found that Section 118(d) of the Kerala Police Act was invalid when applied to Section 66A.

For the reasons stated above, the Court found Section 66A of the ITA illegal in its entirety, since it infringed on Article 19(1)(a) of the Indian Constitution's right to freedom of expression.

4.3.2. Shamsher Singh Verma v. Haryana State[261]

In this instance, the accused filed an appeal with the Supreme Court after the High Court denied his request to exhibit and have the Compact Disc presented in his defense verified by the Forensic Science Laboratory.

[261] 2015 SCC OnLine SC 1242

FACTS OF THE CASE[262]: On October 25, 2013, a report was filed at the Police Station against the appellant (accused), registering a FIR No. 232 in relation to an offence punishable under Section 354 of the Indian Penal Code (IPC) and another relating to the Protection of Children from Sexual Offences Act, 2015 (POCSO), in which complainant Munish Verma claimed that the appellant molested his minor niece. Following an investigation, it appears that a charge sheet was filed against the appellant, culminating in the filing of Sessions Case No. 33 of 2014. On the 28th of March 2014, Special Judge Kaithal framed charges in respect of offences punishable under Sections 354A and 376 IPC, as well as offences punishable under Sections 4/12 of POCSO, after hearing the parties. After the accused's statement was recorded under Section 313 of the Code of Criminal Procedure, 1973, prosecution witnesses were questioned (for short CrPC). The accused called four witnesses in his defense and requested that an alleged recording of a conversation between the victim's father and the accused's son and wife be played in court for the purpose of preserving a copy of the text contained therein for communication to the Forensic Science Laboratory for authentication under section 294 of the Criminal Procedure Code. It was also hoped that the victim's father's voice would be recorded by experts at the Forensic Science Laboratory and then matched with the previously recorded voice. The application was denied by the trial court, and the decision was upheld by the High Court. The appellant's learned counsel argued in front of the Supreme Court that the accused has the right to present evidence in his or her defense, and that the lower courts erred in law by denying that right. Because the accused/appellant was in custody, it was pointed out that he had no intention of prolonging the trial. The only thing that was considered was whether or not the accused had been denied the right to a lawyer, without expressing any opinion on the merits of the prosecution or defense case. The Hon'ble Court concluded that the lower courts erred in law by refusing to allow the defense to play the compact disc relating to the above-mentioned conversation about an alleged property dispute, based on the facts and circumstances.

According to the Supreme Court, a Compact Disc is also a document. It went on to say that personally obtaining admission or rejection of a document from the accused, the complainant, or the witness under Section 294 (1) of the CrPC is not required.

[262] https://advocatespedia.com/CASE_SUMMARY

R.M. Malkani vs. State of Maharashtra, (1973) 1 SCC 471: 1973 (2) SCR 417, the Court held that tape recorded conversation is admissible if the conversation is relevant to the issues at hand, the voice can be identified, and the accuracy of the tape-recorded conversation can be demonstrated by eliminating the possibility of erasing the tape record.

This Court held in Ziyauddin Barhanuddin Bukhari vs. Brijmohan Ramdass Mehra and others; (1976) 2 SCC 17: 1975 (Supp) SCR 281, that tape-recorded speeches were "documents," as defined by Section 3 of the Evidence Act, that stood on the same footing as photographs, and that they were admissible in evidence if the following conditions were met: (a) The voice of the person alleged to be (b) The maker of the record had to prove the accuracy of what was actually recorded, and there had to be sufficient evidence, direct or circumstantial, to rule out the possibility of tampering with the record. (c) The subject-matter recorded had to be shown to be relevant according to the Evidence Act's relevancy rules."

4.3.3. Syed Asifuddin and Others v. Andhra Pradesh State and Others[263]

Facts: Under the Dhirubhai Ambani Pioneer Scheme, the subscriber purchased a Reliance device and Reliance mobile services at the same time. The user was enticed by better tariff options offered by rival service providers and desired to switch to them. The Electronic Serial Number (hereafter referred to as "ESN") was hacked by the petitioners (TATA Indicom employees). Reliance phones' Mobile Identification Numbers (MIN) were irreversibly linked to ESN, and reprogramming ESN made the device valid only by Petitioner's service provider, not by Reliance Infocomm.

ii) Does tampering with an ESN loaded into a mobile handset constitute source code alteration under Section 65 of the IT Act?

Decision: I A "computer" is defined as any electronic, magnetic, optical, or other high-speed data processing device or system that performs logical, arithmetic, or memory functions through manipulations of electronic, magnetic, or optical impulses, as well as all input, output, processing, storage, computer software, or communication facilities that are connected or related, according to Section 2(1)(i) of the IT Act. As a result, a telephone handset falls within the definition of "computer" as stated in Section 2(1)(i) of the IT Act.

[263] 2005 CriLJ 4314

(ii) Changing the ESN allows other service providers, such as TATA Indicomm, to use previously exclusive devices. As a result, changing an ESN is a violation of Section 65 of the IT Act, because every service provider must keep track of its own SID code and assign a unique number to each instrument used to access the services. As a result, the applicants' convictions cannot be invalidated under Section 65 of the Information Technology Act.

4.3.4. Shankar v. State Rep[264]

Factual information: Under Section 482, CrPC, the petitioner filed a motion to suppress the charge sheet filed against him. The petitioner was charged under Sections 66, 70, and 72 of the IT Act with gaining illegal access to the protected system of the Directorate of Vigilance and Anti-Legal Corruption's Advisor (DVAC).

According to the Court, the charge sheet filed against the petitioner cannot be dismissed under the law of non-granting of sanction of prosecution under Section 72 of the IT Act.

4.3.5.Nakul Bajaj & Ors. v. Christian Louboutin SAS[265]

Facts[266]: The Delhi High Court laid forth certain requirements for an e-commerce intermediary to follow in order to claim safe harbor protection under Section 79 of the Information Technology Act, 2000 on November 2, 2018. The Delhi High Court upped the bar for e-commerce intermediaries to qualify for safe harbor protection under Section 79 of the Information Technology Act of 2000 with this decision. The Court specified 26 services that may be used to evaluate whether an intermediary was only acting as a conduit or as an active middleman.

The case began when the Petitioner, Christian Louboutin, a luxury goods brand, claimed that the defendant company, Darveys.com, was engaging in illegal sales of its items, in violation of the Trademarks Act of 1999.

[264] Crl. O.P. No. 6628 of 2010
[265] (2018) 253 DLT 728
[266] https://wilmap.stanford.edu/entries/christian-louboutin-sas-v-nakul-bajaj-and-or

The website charged visitors a membership fee to join the platform, hosted an article on Christian Louboutin products, used meta-tags, and displayed the firms' logos and product photos, among other things. Darvey.com actively participated in the trading process, according to the Court, as evidenced by the fact that it did not reveal information about the overseas vendors, guaranteed the products' validity, and charged a membership fee. As a result, under Section 79 of the Information Technology Act of 1999, it was not entitled to safe harbor protection.

The Court had to decide whether the offender's use of the petitioner's trademark, logos, and picture was protected under Section 79 of the Information Technology Act.

Because the website maintains entire control over the items supplied through its platform, the Court found that the defendant is more than an intermediary. It encourages third-party vendors to market their items by recognizing and promoting them. The Court also stated that an active involvement by an e-commerce platform would protect it from the rights afforded to intermediaries under Section 79 of the IT Act.

4.3.6.Avnish Bajaj v. Delhi State (NCT)[267]

Facts: Avnish Bajaj, the CEO of Bazee.com, was arrested under Section 67 of the IT Act for propagating computer pornography. Someone had previously used the bazee.com website to sell copies of a pornographic CD. A seventeen-year-old high school student filmed himself and a classmate engaging in a sexual act in 2004. (also a minor). For a long period, the movie was disseminated over mobile phones before being published for sale on Baazee.com. The 'DPS MMS Scandal' became known as a result of the occurrence[268].

Baazee.com was an eBay-owned website that, like eBay, acted as an online marketplace for sellers and buyers to transact. Avnish Bajaj, the Managing Director of the company that operated Baazee.com, and the person who advertised the film for sale online were both arrested.The first notable discussion of intermediary culpability by the Indian judiciary is seen in the judgements following from the latter's arrest.

[267] (2008) 150 DLT 769

[268] Indian Express, Sex scandal: Boy who shot MMS clip held, December 19, 2004, available at http://expressindia.indianexpress.com/news/fullstory.php?newsid=39787

According to the court, Mr. Bajaj was not involved in the broadcasting of pornographic content. On the Bazee.com website, the sexual material was similarly unavailable to access. Bazee.com, on the other hand, receives a commission from sales and money from advertisements placed on its website.

The evidence acquired demonstrates that the crime of cyber pornography was perpetrated by someone other than Bazee.com, according to the court. Mr. Bajaj was granted bail after submitting two sureties, each worth Rs. 1 lakh. The burden of proof is on the accused to show that he was merely a service provider and not a content creator.

4.3.7. Suhas Katti v. State of Tamil Nadu[269]

The current case represents a watershed moment in the Cyber Law regime because of the speed with which it was handled, resulting in a conviction within seven months of the FIR being filed.

Facts[270]: The accused was a close friend of the plaintiff's family. The accused sent the plaintiff harassing, slanderous, and obscene communications. On social networking networks and chat apps, the victim was a divorced woman. The accused utilized the Yahoo Messenger program to spread such rumors about the women. The primary issue here is that the accused is only interested in the women. He wanted to marry her as well, but she had already married another man. After her divorce, the accused tried to force her to marry him again, but she refused. After being rejected twice, he began posting derogatory statements about her on social media, as well as sharing her personal phone number.

Following then, mail was routed to the women with information about the accused. The culprit set up a bogus email account in the victim's name. As a result, the victim received a barrage of nasty and filthy phone calls. After being subjected to such slander as a result of the accused's acts, the women filed a complaint against him. Based on the women's accusation, the perpetrator was apprehended by police after a few days. On March 24, 2004, a charge sheet was filed under Section 67 of the IT Act 2000 and Section 469 of the IPC.

[269] CC No. 4680 of 2004
[270] https://lexpeeps.in/state-of-tamil-nadu-v-suhas-katti

Sections 67 of the IT Act, as well as Sections 469 and 509 of the Indian Penal Code, 1860, were utilized to charge the defendant.

The Additional Chief Metropolitan Magistrate in Egmore ruled the accused person guilty under Sections 469 and 509 of the Indian Penal Code, 1860, and Section 67 of the IT Act. Under Section 469 of the Indian Penal Code, the accused was sentenced to two years in prison and a fine of Rs. 500, one year in prison and a fine of Rs. 500 under Section 509 of the IPC, and two years in prison and a fine of Rs. 4,000 under Section 67 of the Information Technology Act.

4.3.8.Arif Azim v. CBI (Sony Sambandh case)[271]

Facts[272]: Sony India Ltd, which operates the website www.sony.sambandh.com, has filed a complaint. By making an online payment, NRIs can send Sony products to their friends and family in India. Someone signed onto the website under the name Barbara Campa. A Sony Color Television and a cordless headphone were also ordered. The user made his or her payment with a credit card. She requested that the product be sent to Arif Azim in Noida. The credit card company dutifully cleared the payment. After completing the relevant formalities, the products are delivered to Arif Azim. That are required for the record, such as taking photographs as proof of delivery acceptance.

That was the end of the transaction. However, the Credit Card agency notified the corporation after one and a half months. An unauthorized person carried out the transaction. Because the true owner declined to complete the purchase.

The corporation then filed a complaint with the CBI, which opened an investigation under Indian Penal Code Sections 418, 419, and 420. Following the investigation, it was discovered that Arif Azim was employed at a call center in Noida at the time of the incident. He gained access to the data of an American citizen's credit card number. As a result, he used to buy Sony things on the internet without permission.

The CBI recovered the Color Television and cordless headphones, and Arif Azim was arrested.

[271] https://www.lawyersclubindia.com/articles/landmark-judgments-on-cyber-law-14025
[272] https://bnwjournal.com/2020/07/17/analysis-cbi-v-arif-azim/

Arif Azim was found guilty, but the Court was lenient with him because he was a young guy and a first-time offender. The guilty offender was given a year of probation by the court. This was a significant case in cyber law because it revealed that the Indian Penal Code, 1860, may be a relevant statute to rely on when the IT Act isn't enough.

4.3.9.Pune Citibank Mphasis Call Cente r Fraud[273]

Facts: In 2005, $ 3,50,000 was unlawfully moved through the internet from four Citibank accounts in the United States to a few fictitious accounts. The staff acquired the customers' trust and collected their PINs under the guise of being able to help them deal with difficult problems. They were seeking for weaknesses in the MphasiS system rather than decoding encrypted software or breaking firewalls.

The defendants in this case, according to the court, are former MphasiS call centre employees. Every time an employee enters or exits the building, they are inspected. As a result, the employees' identification numbers were vividly memorised. SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, was used to transfer the funds. Gaining illegal access to the consumers' electronic accounts was used to commit the crime. As a result, this case has been designated as a "internet crime." The IT Act is wide enough to include these offences, and any IPC violation using electronic documents can be penalised on the same level as crimes involving written materials.

Analysis[274]

Ex-employees of MphasiS BFL's Call Center in Pune are the defendants in this case. They were taught to have a friendly conversation with Citiban's global customers who call for problems with their credit cards and bank accounts when they first joined the call center. The highest level of security is used in India's call centers. Employees are checked every time they come in and out to prevent them from copying down account numbers. As a result, in this case, the employees must have memorized the number and gone to the cyber café shortly after leaving the office to access Citibank customers' accounts.

[273] https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/
[274] https://bnwjournal.com/2020/07/17/pune-citibank-mphasis-call-center-fraud/

The money was then transferred into the accounts that had been opened in Pune. Customers later complained that their money had been transferred to accounts in Pune, and the criminals were tracked down. SWIFT, or Society for Worldwide Interbank Financial Telecommunication, was the service they used to transfer the funds. Fake email accounts were created at the same time as fake bank accounts in Pune. The original account holders never received the confirmations that would have been sent during the money transfer. The money was transferred to a dozen bank accounts in March 2005, with the assistance of two ICICI home loan agents whose job was to facilitate the illicit accounts. They were non-BPO employees, and they were also among those arrested. Citibank was completely unaware of the transactions until one of their customers complained.

Rajendra Bhagwat, the head of Citigroup Investigation Services in Mumbai, was alerted. The team confirmed the fraud by contacting the receiving banks. When the main accused went to the Rupee Co-operative Bank in Pune to check the transfer, the police detained the suspects and made a total of 16 arrests. The arrests were made under the supervision of Assistant Commissioner of Police Sanjay Jadhav.

This fraud raised a number of issues, including the role of "Data Protection." Unauthorized access to customers' electronic account spaces was used to commit this crime. As a result, we can conclude that this case falls under the category of "Cyber Crimes." The Information Technology Act of 2000 is broad enough to cover these aspects of crime that are not codified in the Act but are covered by other laws. Any offense committed with the use of electronic documents under the Indian Penal Code, 1860, can be charged at the same level as crimes committed with written documents.

As a result, trickery, breach of trust, and conspiracy are all applicable in this instance under the sections of the Information Technology Act of 2000. The offense is outlined in the Act's Sections 43(a) and 66. The adjudication process can also be used to establish who is liable for the damages owed to the victims.

The court determined that section 43(a) of the IT Act, 2000 applies because of the kind of unauthorised access that is involved in committing transactions. Sections 66 and 420 of the Information Technology Act of 2000, as well as sections 465,467, and 471 of the Indian Penal Code, were used to charge the defendants.

4.3.10. Jogesh Kwatra vs. SMC Pneumatics (India) Pvt. Ltd.[275]

Facts[276]: Obscene, vulgar, filthy, abusive, threatening, embarrassing, humiliating, and defamatory e-mails were sent to the plaintiff. With the help of a private computer specialist, Plaintiff was able to track down one of the e-mails sent on April 2, 2001. According to the inquiry, the e-mail was sent from a cybercafé in New Delhi. From a group shot taken during the investigation. The defendant was identified as the same person who sent the e-mail by the Cybercafe Attendant.

The e-mails were sent to senior executives at SMC's many subsidiaries throughout the world. They were sent through the sales department, namely to Australia, which is located in several nations, where he worked, and then forwarded to plaintiff No.2. Copies of e-mails were transmitted to the Managing Directors of the Group Companies; only through the Managing Directors of the Group Companies was plaintiff No.2 defamed. All of these people were sent copies of the email with the intent of poisoning their minds, destroying professional career chances, and destabilizing the plaintiff.

Since these emails were forwarded to the plaintiff, the complainant has come to obtain a copy of all of them. On May 11, 2001, the plaintiff filed a police complaint against the defendant. The plaintiff terminated the defendant's services on May 11, 2011, citing the defendant's sending of e-mails and hurting the plaintiff's reputation.

The plaintiffs are not entitled to the proposed perpetual injunction because the court did not qualify as certified evidence under section 65B of the Indian Evidence Act. Because there was no direct evidence indicating the defendant was the one who sent the emails, the court was unwilling to accept even the strongest evidence. The defendant was also prohibited from publishing or transmitting in cyberspace any information that was derogatory or abusive towards the plaintiffs.

Case analysis:

[275] CM APPL. No. 33474 of 2016
[276] https://bnwjournal.com/2020/07/17/analysis-smc-pneumatics-india-pvt-ltd-vs-shri-jogesh-kwatra/

The defense filed a written statement contending that the complainants have not come to court with clean hands and that the claims brought by the plaintiffs against the defendant are false and manufactured, as evidenced by the plaintiffs' woeful failure to:

Give the IP address of the server where each email was sent. When did each of the alleged emails go out? Details regarding the Internet connection of the email's author, such as the user name

The phone number used to connect to the originating server and the phone number phoned for connecting to the originating server if the original sender of emails utilized a leased line.

This page contains detailed information regarding a leased line. The plaintiffs filed a replication in which they rejected the claims made by the defendant in his written statement and restated and confirmed the contents of the plaint.

Six witnesses were called by the plaintiff's attorney. Plaintiff No. 2 himself, Director Operations for plaintiff No. 1, Dy. Divisional Manager (Accounts & Administration) for plaintiff No. 1, Computer Expert, and Forensic Expert/Handwriting Expert for plaintiff No. 1 Company.
One witness was called on behalf of the defendant's attorney. In his own right, he is a defendant.

The plaintiff is not entitled to perpetual injection under the Specific Relief Act if he has not come to court with clean hands. Only one of the e-mails received was traced. Cybercafe was identified as the sender of the e-mail. The identity of Cybercafe was used to send the e-mail, not the identity of the sender. The defendant was identified by the Cybercafe Attendant based on a photograph of a picnic, however that photograph was not included in the records.

The plaintiff counsel's argument was that the substance of the e-mails suggested that the source of the e-mail was defendant, because the stated issues were discussed orally by defendant with the management, particularly plaintiff no. 2.

After the interim order was issued, those types of e-mails stopped arriving save once, according to plaintiff counsel. According to the plaintiff's lawyer, the defendant was the one who was engaging in the conduct, and he was injuncted, so he stopped it so he wouldn't have to face the repercussions of disobeying the court.

4.3.11 The Punjab National Bank Phishing Scam

The Punjab National Bank (PNB) phishing case in India is one of the largest cybercrimes in the country's history. It involves fraudulent transactions worth millions of dollars through unauthorized access to the bank's systems. Here's a detailed explanation of the case[277]:

Background: In early 2018, Punjab National Bank, one of India's largest public sector banks, discovered unauthorized transactions worth approximately $2 billion (around ₹13,000 crores) at one of its branches in Mumbai. The transactions were carried out through the misuse of the bank's SWIFT (Society for Worldwide Interbank Financial Telecommunication) system, a messaging network used by financial institutions to securely transmit information and instructions for financial transactions.

Modus Operandi: The fraudulent transactions were facilitated by exploiting vulnerabilities in PNB's internal controls and procedures. The perpetrators, including bank employees and external actors, allegedly issued fraudulent Letters of Undertaking (LoUs) and Letters of Credit (LoCs) in favor of companies owned by billionaire jeweler Nirav Modi and his uncle Mehul Choksi, without proper collateral or due diligence.

Phishing and Social Engineering: The cybercriminals involved in the scam reportedly used sophisticated phishing techniques to obtain login credentials and passwords of authorized bank officials, allowing them unauthorized access to the SWIFT messaging system. Phishing involves sending deceptive emails or messages that appear to be from legitimate sources to trick recipients into disclosing sensitive information or clicking on malicious links.

Collusion and Complicity: The investigation revealed collusion between bank employees and the perpetrators, who exploited their insider knowledge and access to perpetrate the fraud. It was alleged that certain employees failed to follow prescribed procedures and controls, enabling the fraudulent transactions to go undetected for an extended period.

Impact: The PNB phishing case sent shockwaves across India's banking sector, leading to heightened scrutiny of internal controls, risk management practices, and regulatory oversight.

[277] Gupta, Ruchi, Shilpi Gupta, and Clement Chiahemba M. Ajekwe. "Electronic Banking Frauds: The Case of India." Theory and Practice of Illegitimate Finance. IGI Global, 2023. 166-183.

The incident not only tarnished PNB's reputation but also raised concerns about the vulnerability of India's banking infrastructure to cyber threats and financial frauds.

Investigation and Legal Proceedings: Following the discovery of the fraud, PNB reported the incident to law enforcement authorities and regulatory agencies, including the Central Bureau of Investigation (CBI) and the Reserve Bank of India (RBI). Multiple agencies, including the Enforcement Directorate (ED) and the Income Tax Department, launched investigations into the case.

Arrests and Charges: Several individuals, including PNB employees, Nirav Modi, Mehul Choksi, and their associates, were named as accused in the case. Arrest warrants were issued, and extradition proceedings were initiated against Modi and Choksi, who fled the country before the fraud came to light. The accused were charged with various offenses, including criminal conspiracy, cheating, forgery, and money laundering.

Lessons Learned and Reforms: The PNB phishing case underscored the need for banks to strengthen their cybersecurity infrastructure, enhance internal controls, and foster a culture of compliance and ethical conduct among employees. It also prompted regulatory reforms and policy measures aimed at mitigating the risks associated with fraudulent banking practices and cybercrimes.

In summary, the PNB phishing case stands as a stark reminder of the challenges posed by cyber threats to India's financial system and the imperative for robust cybersecurity measures, effective risk management frameworks, and vigilant regulatory oversight to safeguard the integrity and stability of the banking sector[278].

4.4 JUDICIAL REMEDIES AVAILABLE TO SAFEGUARD AGAINST CYBERCRIMES

These are a few cyber-crimes that occur across various sectors of cyberspace; nevertheless, there are many more that have yet to be found. The number of solved cases is

[278] Soni, R. R., and Soni Neena. "An investigative study of banking cyber frauds with special reference to private and public sector banks." Research Journal of Management Sciences

significantly fewer than the number of unsolved instances, and the crime rate is increasing daily in lockstep with internet usage and technological innovation.

There are legal remedies available to victims of cybercrime, which are overseen by the country's judicial system.

The Information Technology Act of 2000, later updated in 2008, was enacted to set limitations for these types of attackers when it came to committing Cyber-crimes. For laypeople, this is known as the Cyber-law. This Act imposes penalties and restitution for technology-related violations. When a person is the victim of a cyber-crime, he has the option of taking the perpetrator to court to seek legal redress.

Under section 43A of the Information Technology Act of 2000, the victim has the right to seek a court appeal for compensation for the wrong done to him, as this provision covers the punishments and compensations for offenses such as "damage to the computer, computer system, or computer networks, etc." Any company that interacts with sensitive data, information, or maintains it on its own or on behalf of others and carelessly compromises such data or information will be held accountable under this clause and may be forced to pay compensation at the discretion of the court.

"Whoever intentionally or knowingly conceals, destroys, or alters any computer source code used for a computer, computer program, computer system, or computer network, or who intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer program, computer system, or computer network, when the computer source code is required to be kept or maintained by law for the tampering with computer source documents," a law state.

The IT Act of 2008 still has some faults, as there are new and undiscovered cyber-crimes for which the law needs to expand its arms and tighten its grip.

Some offences, such as "cyber-defamation," are not covered by the IT Act because they are already covered by other laws, such as the Indian Penal Code, 1860. Because the impact of such an online violation is the same as it is offline, the term "defamation" and its punishment are defined in this Act; no additional definition is required elsewhere.

As society becomes increasingly reliant on technology, the number of crimes involving electronic devices is expected to rise. As a result of the inappropriate use and misuse of computers and the internet, cyber-crime is common and growing quickly. Crime is a significant impediment to a country's development, as it has a negative impact on society's members and slows the country's economic growth. The Information Technology Act is a lifesaver in the fight against cybercrime. This Act is a particular law designed to combat cybercrime, however computer-related offenses are covered by the Indian Penal Code and other laws in India. In the country, there is a lack of reporting of cybercrime.

Cybercrime is committed on a daily basis, yet only a small percentage of it is reported. As a result, cybercrime cases that make it to a court of law are rare. Collecting, maintaining, and appreciating Digital Evidence can be tricky. The Act has a long way to go before it can adequately safeguard cybercrime victims. To keep crime to a minimum, efforts by the nation's legal system should be done with the scope of fraudsters' crimes in mind. As a result, rulers and lawmakers should make ongoing efforts to guarantee that technology-related regulations cover every area and issue of cybercrime, and that they continue to expand in a healthy and consistent manner in order to keep a constant eye on and check on related crimes.

CHAPTER V
INTERNATIONAL LEGISLATIVE FRAMEWORK TO COMBAT CYBERCRIMES - A COMPARATIVE STUDY OF INDIA, ISRAEL AND USA

5.1 INTRODUCTION

Information societies rely heavily on the information technology available, which is proportional to cyberspace security.[279] A variety of state and non-state entities constantly threatens the availability of information technology. The cyber-attack on the available information technology straddles the border between cybercrime and cyberwar, which have disastrous consequences in the physical world. The recent revelation of 'cyber-attack vectors' such as Stuxnet, Duqu, Flame, Careto, Heart Bleed, and others only emphasizes the vulnerability of information technology resources' confidentiality, integrity, and availability.

The issue is complicated further by cyberspace, which manifests itself in anonymity in space and time, quickness of actions resulting in unequal results disproportionate to the resources used, non-attribution of activities, and the lack of international borders. Because of these characteristics, "the transnational dimension of cybercrime offence arises when an element or substantial effect of the offence, or where part of the modus operandi of the offence is in another territory," raising issues of "sovereignty, jurisdiction, transnational investigations, and extraterritorial evidence," necessitating international cooperation[280]. The effectiveness of multinational efforts to combat cybercrime will be examined in this chapter.

International cybercrime frequently puts domestic and international law, as well as law enforcement, to the test. Because many countries' present laws aren't designed to cope with cybercrime, criminals are increasingly turning to the Internet to avoid harsher sanctions or the difficulty of being tracked. Governments and industry in both emerging and developed countries have increasingly grasped the enormous hazards that cybercrime poses to economic and political security and public interests. However, the variety of types and forms of

[279] M. Gercke, "Understanding cybercrime: a guide for developing countries," International Telecommunication Union (Draft), vol. 89, p. 93, 2011.
[280] O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.

cybercrime makes it more difficult to combat. In this regard, combating cybercrime necessitates international collaboration. On a regional and international basis, various organizations and governments have previously collaborated to establish global laws and law enforcement standards. Because they are the top two source countries of cybercrime, the collaboration between China and the United States has been one of the most notable recent developments[281].

ICT (information and communication technology) is crucial to guaranteeing global standards-based interoperability and security. General countermeasures have been implemented to combat cybercrime, including legal measures to improve legislation and technical measures to track down crimes over the network, such as Internet content control, the use of public or private proxy servers, computer forensics, encryption, and plausible deniability, among others. Because law enforcement and technology countermeasures differ among countries, this essay will primarily focus on international cooperative legislative and regulatory efforts.[282]

5.2 INTERNATIONAL TREATIES, CONVENTIONS AND PROTOCOLS CONCERNING CYBERSPACE

The international treaties, conventions and protocols concerning the cyber-crime which is a part of the cyber space is immense as it provides for a regulatory framework for the relevant countries who are part of the treaty or conventions[283]. This will bind the countries to cater with the rules and regulations. The following treaties, conventions set a backdrop for the comparative study of the legislative framework for this chapter.

- The United Nations is the most well-known of all international organizations. The United Nations Commission on International Trade Law (UNCITRAL) is the organization in charge of harmonizing and unifying international trade law. UNCITRAL, based in Vienna, is a global legal organization that has specialized on commercial law reform for over 40 years. The mission of UNCITRAL is to modernize and harmonize international business rules.

[281] Devidas Ramachandra Tuljapurkar Vs the State of Maharashtra (2015) 6 SCC 1
[282] Apoorva Bhangla and Jahanvi Tuli , A Study on Cyber Crime and its Legal Framework in India, 4 (2) IJLMH Page 493 - 504 (2021), DOI: http://doi.one/10.1732/IJLMH.26089
[283] Firos vs State of Kerala on 24 May, 2006, AIR2006 KER 279

In 1996, the UNCITRAL issued a Model Law on Electronic Commerce in response to the expanding use of electronic commerce and advanced communications technologies in international trade. This was based on a resolution passed by the United Nations General Assembly in 19851 encouraging nations and international organisations to take steps to safeguard legal security in the context of the widespread use of automated data processing in international trade.

- A World Summit on the Information Society (WSIS) was conducted in two phases, one in Geneva from December 1 to 12, 2003, and the other in Tunis from November 16 to 18, 2005, under the auspices of the United Nations, with the International Telecommunication Union playing a prominent role. Realizing the enormous potential of information and communication technologies in human development, world leaders declared their "common desire and commitment to build a people-centered, inclusive, and development-oriented information society, where everyone can create, access, utilize, and share information and knowledge, enabling individuals, communities, and peoples to achieve their full potential in promoting their sustainable development" at the summit in Geneva in 2003. One of the goals of the WSIS was to alleviate the digital divide, or the unequal distribution of the advantages of the information technology revolution between developed and poor countries and within societies.
- The United Nations Commission on Trade and Development (UNCTAD) is the primary trade and development agency of the United Nations General Assembly. UNCTAD has been engaged in advocating for the role and importance of information and communication technologies in development since 1998 when the General Assembly allocated it a special grant to pursue and promote electronic commerce initiatives.
- The most thorough approach to cybercrime and international cyber law was taken at the European Convention on Cybercrime, which met in Budapest on November 23, 2001. It is one of the most important international electronic evidence and cybercrime agreements. The Council of Europe, Canada, Japan, South Africa, and the United States of America all contributed to the writing of the report. There are 48 articles in all, divided into four chapters, in this Convention. This Convention is a global treaty on criminal justice that provides States with Computer and internet-based criminalization of specific behaviors; procedural law for investigating cybercrime and admitting electronic evidence in any criminal case; and international collaboration between law enforcement and judicial authorities in the areas of cybercrime and electronic evidence.

India’s stand on the convention its status as non-member of the convention but india voted for a separate convention. Similarly, data sharing with foreign bodies is against the national sovereign of the country as termed by the Intelligence Bureau. Due to a lack of a strong legislative framework, India's data protection regulations are currently set with challenges and discontent. The legal framework consists of the following elements:

The Information Technology Act of 2000 (IT Act) comprises legislation relating to cyber and IT-related laws in India (for example, sections 43A and 72A)[284].

Compensation for data breaches under Section 43A.

Section 72A: Any knowingly and intentionally disclosing of information without the consent of the person concerned is punishable by imprisonment for up to three years.

However, these provisions do not, on the one hand, protect against data breaches and, on the other, do not impose a privacy framework based on rights[285].

- 67 countries have signed the Convention, and ten international organisations (the Commonwealth Secretariat, European Union, INTERPOL, International Telecommunication Union, Organization of American States, UN Office on Drugs and Crime, and others) are members or observers on the Cybercrime Convention Committee. The Committee is in charge of the Signatories' implementation of the Convention. However, because India has not signed the Convention on Cybercrime, it is not required to alter or implement domestic legislation following the Convention.
- Computer and Computer-Related Crimes Model LawThe Commonwealth Secretariat drafted a "Model Law on Computer and Computer-Related Crime" for the Commonwealth's 53 member countries in October 2002. The Model Law expanded the scope of criminal culpability for offenses involving the internet and computer systems, as well as the use of unauthorized computer-related devices and practices.

  In the context of cybercrime, the Model Law also introduced the idea of dual criminality. It indicates that if a person commits an infraction outside of his nation, the

[284] Firos vs State of Kerala on 24 May, 2006, AIR2006KER279

[285]https://www.drishtiias.com/daily-updates/daily-news-analysis/convention-on-global-cybercrime

offence is punishable if the person's acts would be punishable under any law of the country where the offence was done. This idea of dual criminality could lead to charges or extradition. The Model Law has been used to draft domestic cyber laws in some Commonwealth member countries[286].

- Members of the World Trade Organization (WTO) adopted a declaration on global electronic commerce on May 20, 1998, during their Second Ministerial Conference in Geneva, Switzerland, due to the growing importance of internet commerce in global trade. The WTO General Council was directed to prepare a thorough work programme to evaluate all trade-related concerns arising from electronic commerce, and to deliver a progress report to the WTO's Third Ministerial Conference, according to the Declaration.
- The Group of Eight consists of eight countries (G8)

  The Group of Eight (G8) was primarily focused on prosecuting high-tech criminals and supporting technical and legislative improvements to combat worldwide computer crimes at the Denver Summit in 1997[287].

- The Okinawa Charter on Global Information Society, adopted at the Okinawa Summit in 2000, adopted the concepts of international collaboration and harmonization for cybercrime. The Group of Eight agreed on the importance and principles of privacy protection, free flow of information, and transaction security.

- WIPO, the World Intellectual Property Organization, is situated in Geneva and has 179 member states. WIPO's mission is to "advance the protection of intellectual property around the world through international collaboration." (WIPO Convention, Article 3) WIPO is the custodian of 23 international treaties and serves as a platform for worldwide IP policy development and administration. Intellectual property migration to the digital realm is the order of the day, as IP is well-suited to digitalization. Because an infinite number of perfect copies may be generated and readily distributed across digital networks around the world, IP on the internet is insecure. As a result, it's

[286] R v Gold and Schifreen [1988] 2 WLR 984
[287] https://blog.ipleaders.in/regulatory-framework-for-cyber-crimes/

understandable that online content, such as information, music, software, films, business procedures, databases, and so on, needs to be protected[288].

- The United Nations Convention Against Transnational Organized Crime (UNCTOC) was adopted by the United Nations in 2000. The Palermo Convention requires state parties to create domestic criminal charges that target organised criminal groups, as well as new procedures for extradition, mutual legal assistance, and law enforcement cooperation. Despite the fact that the treaty does not specifically mention cybercrime, its provisions are extremely pertinent.

- Article 34 of the 1989 Convention on the Rights of the Child mandates that states protect children from all forms of sexual exploitation and abuse, including prostitution and pornography.

- Protocol to the Convention on the Rights of the Child (Optional Protocol) (2001) – The sale of children, child prostitution, and child pornography are all addressed in this protocol, which is based on the CRC Convention. The production, distribution, dissemination, sale, and possession of child pornography are all prohibited under Article 3(1)(c). The Internet is mentioned in the Preamble as a source of child pornography distribution. Article 2(3) contains a definition of child pornography that is wide enough to include virtual images of minors[289].

5.3 LEGISLATIVE FRAMEWORK OF CYBER LAW IN INDIA

5.3.1 India's Cyber Laws

In India, cyber laws are governed under the Information Technology Act, 2000 ("IT ACT"). The primary purpose of the act is to protect private data and personal information of individuals, which has become increasingly crucial in today's digital world as the number of IT-enabled services develops. In a larger sense, sensitive and crucial information critical to

[288] Apoorva Bhangla and Jahanvi Tuli , A Study on Cyber Crime and its Legal Framework in India, 4 (2) IJLMH Page 493 - 504 (2021), DOI: http://doi.one/10.1732/IJLMH.26089
[289] https://netlawgic.com/cyber-crime-conventions 07 Feb 2022 10am

national security must also be safeguarded. The IT Act establishes the infrastructure needed to build up a secure system and restrict access to confidential information[290].

The Model Law on Electronic Signatures was adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 2001. The recommendations of the general assembly recommended all states to incorporate the Model Law on Electronic Signatures into their own state laws. The provisions on digital signatures are included in the IT Law, which is in accordance with the UNICITRAL Model Law.

As information technology has advanced, crimes have also made their way into the digital arena. Hacking, voyeurism, identity theft, and other cybercrimes and e-commerce frauds are becoming a growing global concern. To deter these offences, the IT Act recognizes them and sets appropriate punishments.

The Act also provides provisions that allow service providers to establish, maintain, and improve computerized facilities while also collecting and retaining acceptable service costs if the State and Central Governments grant them authorization[291].

It encompasses a wide range of topics, including data protection, data security, digital transactions, electronic communication, freedom of expression, and online privacy, to name a few. Regulation Of Information Technology Regulation of Information Technology

The Information and Technology Act. It is based on the United Nations Model Law on Electronic Commerce (UNCITRAL Model), which was recommended by the United Nations General Assembly in a resolution dated January 30, 1997." In India, the legislation establishes a legal foundation for e-commerce. It focuses on and addresses digital crimes, sometimes known as cybercrime, as well as electronic trade. The legislation was passed in order to update some outdated laws and to give cybercrime jurisdiction. These laws have addressed issues such as electronic authentication, digital (electronic) signatures, cybercrime, and network service provider liability. In addition, the Information Technology Amendment Bill of 2008 amended

[290] Suhas Katti v. State of Tamil Nadu C No. 4680 of 2004

[291] https://www.lawyered.in/legal-disrupt/articles/diving-information-technology-act-2000-salient-features-and-2008-amendments-rashi-suri

the statute. The Indian Penal Code of 1860 and the Indian Evidence Act of 1872 were amended by the IT Act of 2000 to take into account the fast-changing technological landscape[292].

On October 17, 2000, the Cyber Law IT Act 2000 was enacted in India to address e-commerce and cybercrime. After the Indian Constitution was drafted, cyber legislation was enacted. As a result, it is a residuary topic managed by the Central Government that is not included in the three lists: Union, State, and Concurrent. The following is a list of characteristics of Cyber Law as defined by the act[293]:

- All electronic contracts entered into through secure electronic channels are legally binding.
- E-records and digital signatures are protected by security mechanisms.
- The Cyber Law Act establishes a procedure for appointing an adjudicating officer to conduct investigations.
- Digital signatures are legally recognized under the IT legislation act. The employment of an asymmetric cryptosystem and a hash function is also required for digital signatures.
- Without a warrant, top police officers and other officials are able to search any public case
- The act includes a provision to create a Cyber Regulation Appellate Tribunal. This tribunal hears appeals from the Adjudicating Officer's or the Controller's final orders. However, the only way to challenge the tribunal's decision is to go to the High Court.
- The act also establishes a Cyber Regulations Advisory Committee, which will advise the Controller and the Central Government.
- The Cyber Law Act's nature also applies to online crimes or offenses committed outside of India.
- There is also a provision for the Controller of Certifying Authorities to be established, which will license and regulate the Certifying Authorities' operations. In this situation, the Controller stores all of the digital signatures.
- Areas where cyber law is not applicable

[292] https://learn.lawdocs.in/analysis-of-indian-legal-framework-for-cyber-crimes
[293] https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence

- The Central Government has started a number of initiatives and papers.
- Financial and legal acts performed by a person who has been lawfully designated as a Power of Attorney.
- Contract for the sale or transfer of real estate

Some of the most important sections under Information Technology act 2000

Section 3 - Electronic record authentication

Section 4 - Electronic record legal recognition

Section 5 - Digital Signature Legal Recognition

Section 6 - Electronic records and digital signatures in government and government agencies

Section 17 - Appointment of certifying authority' controllers and other officials

Section 18 - Functions of certifying authorities' controllers

Section 43 - Penalty for computer and computer system damage, unauthorised access, data download, virus infection, denial of access, and so on.

Section 44 - Penalty for failing to provide information returns and other documents to the certifying authority

Section 48 - Creation of a Cyber Appellate Tribunal

Penalty for tampering with computer source materials under Section 65

Section 66 - Penalty for computer system hacking

Penalty for obtaining stolen computer or communication devices under Section 66B

Section 66C – Identity theft penalties

Section 66D - Penalty for personation cheating utilising computer resources

Section 66E - Penalty for capturing, transmitting, or publishing photos of another person without their consent

Section 66F - Cyberterrorism Penalty

Section 67 - Penalty for releasing obscene information in electronic form

Penalty for releasing images of sexual acts or conduct under Section 67A

Penalty for child pornography under Section 67B

Section 70 - Penalty for obtaining or attempting to obtain access to a protected system

Section 71 - Penalty for false statements

5.3.2 Recent development in Cyber law in India in the year 2021[294]

[294] https://www.jigsawacademy.com/blogs/cyber-security/what-is-cyber-law/

The government of India has introduced new guidelines to regulate social media and OTT (over-the-top) platforms, as social media has become a newfound arena for everyone to communicate and express their ideas[295]. It was set up to prevent hate speech from being used and spread. Another important motivation is to address people's grievances. They'll also track down the original sender of offensive remarks and tweets. This will be done either by the government or by a court order directed at that platform. The government has also stated that they will not support anything that could pose a threat to national security.

The requirement for social media and Over-the-Top (OTT) directions[296]

- Hate speech and defamation- Due to the unexpected surge in visibility on social media, it is critical to prevent hate speech and defamation, which can have serious consequences for the public.
- Misuse of content and misinformation- Misuse of personal content, including obscene content, on the same platforms is another important issue.
- Online Protection- There is a pressing need to safeguard women and men from sexual assaults that take place on online platforms.

There were no effective controls in place earlier to ensure that content on OTT Platforms was being watched by an appropriate age group. However, with the new rules and strong parental controls in place, content will now be sent to the appropriate audience.

As amendments where it had some drawbacks also

- Concerns about privacy- Any information can be exploited, and propaganda of any kind can harm digital publishers.
- Infringing on the Right to Freedom of Expression and Speech- This right, according to Article 19(a), empowers citizens to express any opinion through any means of communication, including speech and writing. Curbing and regulating social media is essentially depriving citizens of their First Amendment right to free speech and expression.
- Tracking problems- Personal data, such as WhatsApp communications, is essential for the government to trace hate speech and original originators of tweets. However,

[295] Janhit Manch & Ors. v. The Union of India PIL NO. 155 OF 2009

[296] https://www.livelaw.in/law-firms/law-firm-articles-/it-rules-2021-digital-media-ott-platforms-186065

given WhatsApp's encryption, it's unclear how they'll be able to extract such information[297].

The government periodically publishes sets of Information Technology Rules (the IT Rules) under various parts of the IT Act to widen its scope. These IT Rules are focused on and regulate specific areas of data collection, transfer, and processing, and include the following, most recently:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[298], which mandate that companies holding sensitive personal data or information of users adhere to particular security requirements;

- 2021 Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, which ban content of a particular sort on the internet and restrict the role of intermediates, particularly social media intermediaries, in keeping their customers' personal data safe online;

- The Information Technology (Guidelines for Cyber Cafe) Rules[299], which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage; and the Information Technology (Guidelines for Cyber Cafe) Rules, which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage.

- The government can specify that certain services, such as applications, certificates, and licenses, be delivered electronically under the Information Technology (Electronic Service Delivery) Rules[300], which allow the government to specify that certain services, such as applications, certificates, and licenses, be delivered electronically.

And the most important one the compliance regulators which look after the compliance part

[297] Emeka Fabian Vs State of Karnataka Crl.P. NO. 570/2016

[298] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
[299] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[300] meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf

5.3.3 CERT-In

The government established CERT-In under Section 70B of the IT (Amendment) Act 2008, which the Ministry of Electronics and Information Technology refers to as the "Indian Computer Emergency Response Team." CERT-In is a national nodal agency that handles computer security events as they happen. The following are the functions of the agency as defined by the Ministry of Electronics and Information Technology:

- Information about cybersecurity incidents is collected, analyzed, and disseminated.
- Cybersecurity incident forecasting and notifications;
- actions should be taken in the event of a cyber-attack;
- actions for cybersecurity incident response cooperation; and
- issuing guidelines, advisories, vulnerability notes, and white papers on information security practices, processes, cybersecurity incident prevention, response, and reporting[301].

5.3.4 Appellate Tribunal for Cyber Regulations (CRAT)

In October 2006, the Ministry of Electronics and Information Technology formed CRAT under Section 48(1) of the IT Act 2000. The Cyber Appellate Tribunal was renamed as a result of the IT (Amendment) Act 2008. (CRAT). Any individual who is aggrieved by an order made by the Controller of Certifying Authorities or an adjudicating officer under this Act may file an appeal with the CAT under the IT Act. According to Section 49 of the IT Act 2000, the CRAT is led by a chairperson who is selected by the central government by notification[302].

The chairperson was previously known as the presiding officer until the IT (Amendment) Act 2008. The modified Act specifies that the CRAT will consist of a chairperson and as many other members as the federal government may notify or appoint[303].

5.4 LEGISLATIVE FRAMEWORK OF CYBER LAW IN ISRAEL

The key statutory and regulatory provisions that address cyber issues under Israeli law are:

---

[301] www.cert-in.org.in.

[302] Adv R.Mahalakshmi vs Commissioner Of Police CRL.O.P.Nos.27389 of 2013

[303]https://www.meity.gov.in/writereaddata/files/The%20Cyber%20Appellate%20Tribunal%28Chairperson_Members%29%20Rules%2C%202009.pdf.

5.4.1 The Computer Law, 1995[304]

The main law that deals with cybercrimes is the Computer Law (1995). This Law forbids the illegal access to computer material (Article 4), data and system interference (Article 2) and the misuse of devices (Article 6) alongside other offences.
Some of the important sections in Computer Law 1995.

Section 4 – unlawful penetration into computer material -," A person who unlawfully penetrates computer material located in a computer, shall be liable to imprisonment for a period of three years; for this purpose, "penetration into computer material" - penetration by means of communication or connection with a computer"

Section 6 – computer virus- "(a) A person who composes a software program in a manner that enables it to cause damage to or disruption of a non-specific computer or computer material, in order to unlawfully cause damage to or disruption of a computer or computer material, whether specific or non-specific, shall be liable to imprisonment for a period of three years. (b) A person who transfers software program to another, or who infiltrates another's computer with, a software program that is capable of causing damage or disruption as aforesaid in Subsection (a), in order to unlawfully cause the aforesaid damage or disruption, shall be liable to imprisonment for a period of five years"

.

5.4.2 The Privacy Protection Regulations (Data Security), 2017 (based on the 1981 Privacy Protection Law)[305]

The regulations apply to both the private and public sectors, and they provide organizational procedures to ensure that data security is integrated into the management processes of all businesses that process personal data.

[304] https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/israel/
[305] https://www.gov.il/en/Departments/General/data_security

The rules are the result of a thorough examination of relevant legislation, standards, and related Israeli and international recommendations. The laws were put in place following thorough consultation with the Israeli people, particularly those who might be affected by them.

The regulations are projected to significantly improve Israel's data security since they are both flexible, concrete, and particular to the point where they provide enterprises with regulatory certainty and practical instruments that are easy to execute. With the legislation' implementation in May 2018, we anticipate a new age in which Israel's privacy protection will be greater than ever.

5.4.3 The Emergency Regulations, 2020 on the and processing of 'technological information' on Israeli citizens to stop the spread of COVID-19[306]

On March 15 and 17, 2020, Israel's transitional government, led by Prime Minister Binyamin Netanyahu, approved two separate emergency regulations that, among other things, allow the General Security Service (GSS) to use digital surveillance and give the Israel Police expanded search authority to combat the spread of the coronavirus. The GSS is in charge of "protecting state security... and promoting other critical state interests for the state's national security, all as stipulated by the government and according to legislation."

The Cyber Defence and National Cyber Directorate Bill, which is under negotiation in the Israeli Knesset (Parliament)[307]; andThe Israel National Cyber Directorate is responsible for all aspects of cyber defense in the civilian sphere, from formulating policy and building technological power to operational defense in cyberspace. We provide incident handling services and guidance for all civilian entities as well as all critical infrastructures in the Israeli economy, and works towards increasing the resilience of the civilian cyber space.

The Copyright Law, 2007 – Amendment 5 (2019) on the procedure for the disclosure of the identity of internet users under certain circumstances[308].The law acknowledges copyright as being applicable to original productions – literary, artistic, dramatic, or musical – as well as

[306] https://www.loc.gov/item/global-legal-monitor/2020-03-18/israel-emergency-regulations-authorize-digital-surveillance-of-coronavirus-patients-and-persons-subjected-to-home-isolation/
[307] https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page
[308] https://www.loc.gov/item/global-legal-monitor/2007-12-02/israel-new-copyright-law

recordings, as long as they have a connection to Israel or are protected by a decree issued by the Minister of Justice in compliance with an international convention.

The law broadens the range of uses that are either permitted or considered fair use. Use of a creation in legal or administrative proceedings; copying of a creation that is deposited by law for public review; indirect use of a creation by inclusion in another creation such as a photograph, a film, or a record; copying of computer software for backup or maintenance; and use of a creation for broadcast; as part of an educational activity; in libraries, and so on are among them. The law extends copyright protection to the creator's lifetime or, in the case of a joint creation, the last remaining creator's lifetime, to 70 years after his death. Anonymous creations are protected for 70 years, while records and creations owned by the state are protected for 50 years. The law also acknowledges moral rights, which include the creators' rights to name their creation and to be safeguarded from any change or action that could jeopardize the creator's dignity or reputation.

The 2017 Privacy Protection Regulations (Data Protection) outline the levels of security required for several types of information, based on the sensitivity of the data as specified by the regulations. They are divided into the following categories:

- databases that are subject to a basic level of security;
- databases with a medium level of security; and databases with a low level of security.
- databases that require a high level of security

Outsourcing is addressed in paragraph 15 of the Privacy Protection Regulations (Data Security) 2017, which stipulates the responsibility of the outsourced service provider in terms of cybersecurity. The regulations govern the agreement between an Israeli business and its outsourced service provider (which could be a non-Israeli entity) for databases that must be kept secure.

5.4.4 Enforcement and penalties under the cyber laws in Isreal[309]

The following criminal consequences for cybercrime are set out in the Israeli Computer Law of 1995. (eg, hacking, theft of trade secrets).

[309] https://www.mondaq.com/technology/1070854/cybersecurity-comparative-guide

Paragraph 3 stipulates a five-year prison sentence for anyone who:
write software, transfer software to or store software on a computer in such a way that its use will result in false information or false output, or operate a computer using such software; or transmit or store false information or act on information in a way that results in false information or false output; or write software, transfer software to or store software on a computer in such a way that its use will result in false information or false output.
In this context, 'false information' and 'false output' refer to data and output that, depending on their application, may be misleading.

Except if the unlawful entry of a computer or the illegal infiltration of material found on a computer is based on the Wiretap Act of 1979, illegal intrusion of a computer or illegal infiltration of material found on a computer is punishable by three years in prison under paragraph 4.Anyone who undertakes an act banned by Section 4 in order to commit an offence under any legislation would be punished to five years in prison, according to paragraph 5.
Anyone who alters software in such a way that it is capable of causing harm or disruption to a computer or content stored on a computer, whether stated or unspecified, is subject to paragraph 6 of the law. will be sentenced to three years in prison; and anyone who transfers or instals software capable of causing damage or disruption on another's computer in order to cause unlawful damage or disruption will be sentenced to five years in jail.

The Israeli Privacy Protection Authority is in charge of cyber-related civil matters including personal information and data security breaches (PPA). Any personal data breach must be reported to the PPA under the Privacy Protection Regulations (Data Security) of 2017. The PPA is empowered by law to enforce and supervise any organisation that is required by law to register its databases in Israel. Under the Privacy Protection Law and its regulations, the PPA has the legal authority and reason to apply administrative fines and entry and search orders, which it does in select situations. The PPA ensures that any database must be registered in accordance with the legislation. The applicant must provide all of the following information on the database registration application form:

- the data owner (equivalent to a data controller); and
- the registered database manager's personal information, who bears legal personal liability.

If the management fails to supervise the organization's data control, he or she is legally liable. Through the Israeli Cyber Emergency Response Team, the Israel National Cyber Directorate monitors national civil cyber threats in order to improve Israel's defence and build a shared basis of civil knowledge on data protection. The National Cyber Directorate is not authorized to enforce any laws. The Cyber Authority and other government entities are aggressively addressing and enforcing national and international cybersecurity issues. These organizations have unrestricted ability to take whatever actions are necessary to avoid national or international security threats.

The Israeli police force has developed a cybercrime central section to combat crimes such as pedophilia, drug trafficking, credit card fraud, and identity theft that occur on virtual platforms. The cybercrime unit is authorized to investigate and prosecute. Cyber-related guidelines and processes have been implemented by other government-supervised businesses, such as banks and insurers, to meet worldwide requirements. With the exception of homeland security problems, none of the aforementioned authorities or government entities have extraterritorial authority over firms that are not based in Israel and do not have a local presence (including subsidiaries and related companies).

5.5 LEGISLATIVE FRAMEWORK OF CYBER LAW IN USA[310]

5.5.1 Computer Fraud and Abuse Are Prohibited Under the Computer Fraud and Abuse Act (CFAA)

Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It's a piece of cyber-security legislation. It safeguards federal computers, bank computers, and Internet-connected systems. It protects them from trespassing, threats, vandalism, spying, and being exploited as fraud instruments by the corrupt. It is not a comprehensive provision; rather, it fills in the fractures and holes left by other federal criminal laws. This is a quick rundown of the CFAA and some of its federal statutory partners, including the Identity Theft Enforcement and Restitution Act, P.L. 110-326, 122 Stat. 3560, and its revisions (2008).

The seven provisions of subsection 1030(a) in their current form prohibit

18 U.S.C. 1030(a)(3); computer trespassing (e.g., hacking) in a federal computer;

[310] Available at https://www.everycrsreport.com/reports accessed on 05 May 2021 at 11am

18 U.S.C. 1030(a)(2); computer trespassing (e.g., hacking) resulting in exposure to certain governmental, credit, financial, or computer-stored information;
18 U.S.C. 1030(a)(5): destroying a government computer, a bank computer, or a computer used in, or influencing, interstate or foreign commerce (e.g., a worm, computer virus, Trojan horse, time bomb, denial of service attack, and other kinds of cyber-attack, cyber-crime, or cyber terrorism);
18 U.S.C. 1030(a)(4), perpetrating fraud that includes unauthorized access to a government computer, a bank computer, or a computer utilised in, or affecting, interstate or foreign commerce;
18 U.S.C. 1030(a)(7); threatening to harm a government computer, a bank computer, or a computer utilised in or affecting interstate or foreign commerce;
18 U.S.C. 1030(a)(6), for trafficking in passwords for a government computer or when the trafficking affects interstate or foreign commerce; and 18 U.S.C. 1030(a)(7), for trafficking in passwords for a government computer or when the trafficking affects interstate or overseas business.
18 U.S.C. 1030(a): Using a computer to commit espionage (1).
Attempting or conspiring to commit any of these actions is illegal under Section 1030(b). Subsection 1030(c) lists the penalty for committing crimes, which vary from a year in jail for ordinary cyberspace trespassing to a maximum of life in prison for intentional computer damage that results in death.

The Secret Service's investigation jurisdiction is preserved by Section 1030(d). Common definitions are provided in section 1030(e). Section 1030(f) does not apply to law enforcement efforts that are otherwise legal. Victims of these offences have a civil cause of action under Section 1030(g). The forfeiture of tainted property is allowed under Sections 1030(i) and (j).

5.5.2 Critical Infrastructure Information Act

The Critical Infrastructure Information Act of 2002 (CII Act) seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation’s vulnerability to terrorism. The Homeland Security Act of 2002 established a framework that allows individuals of the private sector and others to voluntarily submit sensitive information about the Nation's Critical information to Department of

Homeland security with the certainty that the information will be shielded from public exposure if it meets specific criteria[311].

5.5.3 Health Insurance Portability and Accountability Act of 1996 (HIPAA)[312]

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient. The HIPAA Privacy Rule was developed by the US Department of Health and Human Services (HHS) to implement HIPAA's provisions. A subset of information covered by the Privacy Rule is protected under the HIPAA Security Rule.

Individuals and organizations that fall under the following categories are considered covered entities under the Privacy Rule:

Every healthcare professional, regardless of practice size, who electronically communicates health information in connection with specific transactions is a healthcare provider. Claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has defined criteria under the HIPAA Transactions Rule are examples of these transactions.

Health plans are organizations that offer or pay for medical treatment. Health insurers, dental, vision, and prescription drug insurers; health maintenance organizations (HMOs); Medicare, Medicaid, Medicare Choice, and Medicare supplement insurers; and long-term care insurers are all examples of health plans (excluding nursing home fixed-indemnity policies). Employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans are all examples of health plans.

A covered entity is not a group health plan with less than 50 participants that is solely administered by the employer who established and maintains the plan.

[311] https://itlaw.fandom.com/wiki/Critical_Infrastructure_Information_Act_of_2002
[312] https://www.cdc.gov/phlp/publications/topic/hipaa.html

Entities that convert nonstandard information received from another entity into a standard (i.e., standard format or data content), or vice versa. Individually identifiable health information is often only received by healthcare clearinghouses when they are acting as a business associate for a health plan or a healthcare provider.

Individually identifiable health information is used or disclosed by business associates (other than members of a covered entity's workforce) to perform or provide operations, activities, or services for a covered entity. Claims processing, data analysis, usage review, and billing are examples of these functions, activities, or services.

5.5.4 Gramm-Leach-Bliley Act[313]

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

5.5.5 FISMA[314]

In December 2002, the Federal Information Security Management Act (FISMA) [FISMA 2002], which was enacted as part of the E-Government Act (Public Law 107-347) was signed into law. FISMA 2002 mandates that each federal agency create, document, and implement an agency-wide information security program for all information and systems that support the agency's operations and assets, including those provided or maintained by another agency, contractor, or other sources.

The Federal Information Security Modernization Act of 2014 modifies FISMA 2002 by making a number of changes to improve federal security practices in response to emerging security issues. These improvements result in less overall reporting, a stronger use of continuous monitoring in systems, a greater focus on agencies for compliance, and reporting that is more focused on security incident issues. FISMA 2014 also mandated that the Office of Management and Budget (OMB) amend/revise OMB Circular A-130 to minimize inefficient

[313] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act
[314] https://csrc.nist.gov/projects/risk-management/fisma-background

and unnecessary reporting, as well as to reflect changes in the law and technological advancements.

FISMA, like the Paperwork Reduction Act of 1995 and the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act), places a strong emphasis on risk-based security. The Office of Management and Budget (OMB), in support of and to reinforce FISMA, has issued Circular A-130, "Managing Federal Information as a Strategic Resource," which requires executive agencies within the federal government to:

- Make a security plan.
- Assign security duty to the relevant officials.
- Review the security controls in their systems on a regular basis.
- Authorize system processing before beginning operations and on a regular basis thereafter.

FISMA applies to Federal agencies, contractors, or other sources that provide information security for the information and information systems that support the operations and assets of the agency.

5.5.6 Electronic Communications Privacy Act of 1986 (ECPA)[315]

The Electronic Communications Privacy Act (ECPA) of 1986 combines the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. The ECPA revised the Federal Wiretap Act of 1968, which covered interception of conversations over "hard" telephone lines but not computer and other digital and electronic communications. Several following pieces of legislation, such as the USA PATRIOT Act, explain and update the ECPA in order to keep up with the growth of new communications technology and methods, including loosening restrictions on law enforcement access to stored communications in some situations.

General Provisions

The ECPA, as modified, safeguards wire, oral, and electronic communications while they are in use, in transit, and when they are stored on computers. Email, phone chats, and data saved electronically are all covered by the Act.

[315] https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

"The SCA's structure incorporates a number of classifications that reflect the drafters' assessments of which types of information pose higher or lesser privacy risks. The drafters, for example, identified a higher level of privacy concern in the content of retained emails than in subscriber account information. Similarly, the drafters considered that computing services that were 'open to the public' required more stringent [sic] regulation than services that were not... The [Act] provides varied degrees of legal protection based on the perceived relevance of the privacy interest at hand, in order to preserve the wide range of privacy interests outlined by its drafters. A subpoena can be used to collect some information from providers; other information requires a special court order; and still more information requires a search warrant. Furthermore, some legal processes need the subscriber to be notified, while others do not."
The Act follows a general policy of providing more privacy protection for content with higher privacy concerns.

5.6 COMPARATIVE STUDY OF INDIA, USA AND ISRAEL

INDIA	**ISRAEL**	**USA**
1.The Information Technology Act, 2000 ("IT ACT") governs cyber laws in India. The act's principal goal is to give electronic trade legal legitimacy and to make filing electronic records with the government easier	The main law that deals with cybercrimes is the Computer Law (1995). This Law forbids the illegal access to computer material (Article 4), data and system interference (Article 2) and the misuse of devices (Article 6) alongside other offences	Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It's a piece of cyber-security legislation. It safeguards federal computers, bank computers, and Internet-connected systems. It protects them from trespassing, threats, vandalism, spying, and being exploited as fraud instruments by the corrupt

2. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules[316], which mandate that companies holding sensitive personal data or information of users adhere to particular security requirements.	The Privacy Protection Regulations (Data Security), 2017 (based on the 1981 Privacy Protection Law) The regulations apply to both the private and public sectors, and they provide organizational procedures to ensure that data security is integrated into the management processes of all businesses that process personal data.	Critical Infrastructure Information Act The Critical Infrastructure Information Act of 2002 (CII Act) seeks to facilitate greater sharing of critical infrastructure information among the owners and operators of the critical infrastructures and government entities with infrastructure protection responsibilities, thereby reducing the nation's vulnerability to terrorism
3. Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) 2021	The Emergency Regulations, 2020 on the and processing of 'technological information' on Israeli citizens	Health Insurance Portability and Accountability Act of 1996 (HIPAA) The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that mandated the adoption of national standards to prevent sensitive patient health information from being revealed without the consent or knowledge of the patient
4. The Information Technology (Guidelines for	The Cyber Defence and National Cyber Directorate Bill, which is under	Gramm-Leach-Bliley Act The Gramm-Leach-Bliley Act requires financial

[316] meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf

Cyber Cafe) Rules[317], which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage; and the Information Technology (Guidelines for Cyber Cafe) Rules, which require cybercafés to register with a registration agency and keep a log of users' identities and internet usage.	negotiation in the Israeli Knesset (Parliament)	institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
5. The government can specify that certain services, such as applications, certificates, and licenses, be delivered electronically under the Information Technology (Electronic Service Delivery) Rules[318], which allow the government to specify that certain services, such as applications, certificates, and licenses, be delivered electronically.	The Copyright Law, 2007 – Amendment 5 (2019) on the procedure for the disclosure of the identity of internet users under certain circumstances	FISMA In December 2002, the Federal Information Security Management Act (FISMA) [FISMA 2002], which was enacted as part of the E-Government Act (Public Law 107-347) was signed into law. FISMA 2002 mandates that each federal agency create, document, and implement an agency-wide information security program for all information and systems that support the agency's operations and

[317] meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
[318] meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf

		assets, including those provided or maintained by another agency, contractor, or other sources
	5.The 2017 Privacy Protection Regulations (Data Protection) outline the levels of security required for several types of information, based on the sensitivity of the data as specified by the regulations. They are divided into the following categories: databases that are subject to a basic level of security; databases with a medium level of security; and databases with a low level of security. databases that require a high level of security	Electronic Communications Privacy Act of 1986 (ECPA) The Electronic Communications Privacy Act (ECPA) of 1986 combines the Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act. The ECPA revised the Federal Wiretap Act of 1968, which covered interception of conversations over "hard" telephone lines but not computer and other digital and electronic communications.

As we compare the legislative framework of the all the three countries it gives a clear picture that India is lacking way behind in relation to cyber legislation specially in relation to the Data protection as Israel and USA have separate legislation on the following topic. A strong legislative action is required from the makers of law in India.

The most important is the critical infrastructure Israel and Usa have there own legislations on the critical infrastructure of on the other hand India is lacking a legislation as the critical infrastructure is the most important of all. Any kind on the nuclear power plants or the grid lines of the nation or on the stock exchanges can cripple the economy for many months.

Privacy related laws are missing in India as compared to Israel and Usa as they have their own legislation on the privacy related issues in their respective country.

Cyber-crime related model that should be adopted by India to become one of the best countries to combat cybercrime

The model prevailing in Israel and USA makes them one of the best countries in relation to cybercrime. Similar model could be adopted by India to strengthen the cybercrime rin the country. They are as follows:

1. Advanced technology parks should be established in relation to crime related to internet and development of public authorities in digital production.
2. Digital production and network safety instruction should be imparted to the students from the school level. Specialization in Graduation should be brought in relation to cyber security/ web security in the curriculum of the students at college level.
3. Research organizations should be set up, if research organization come together, it can make India super power in digital protection.

CHAPTER VI
CYBERCRIME- AN EMERGING THREAT TO THE FINANCIAL SECTOR

6.1. INTRODUCTION

Communication and information Our daily lives have become increasingly reliant on technology. Almost everyone now has access to the internet, thanks to the low cost of broadband and smart phones, which connects millions of online users all over the world. The increased usage of cyberspace has rendered us more exposed to cybercrime. A simple lapse or omission in managing our digital lives might lead to cybercrime and, as a result, financial loss. As a result, whenever we connect digitally to the outside world, whether for financial transactions, social networking, gaming, or seeking for information on the internet, we must be watchful and cautious.

Banks in India have transferred transactions to payment cards (debit and credit cards) and electronic channels such as ATMs, Internet Banking, and Mobile Banking, and have migrated to core banking platforms. With the rapid expansion of computer and internet technologies, the banking industry has enjoyed the ride of emerging technology to undergo significant changes and has seen expansion of its services and strives to provide better customer facilities through technology. However, there have been risks associated with it as well. Technology risks affect a bank not only directly as operational risks, but they can also amplify other risks such as credit and market risks. Customers are increasingly relying on electronic delivery channels to perform transactions, so any security concerns are important issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks[319].

Electronic banking, often known as e-banking, is a system in which banking transactions are conducted utilizing information and computer technology rather than human resources. There is no actual interaction between the bank and the consumers with e-banking, unlike traditional banking services. E-banking is the distribution of bank information and services to consumers using a variety of delivery platforms that can be utilized with a variety of terminal

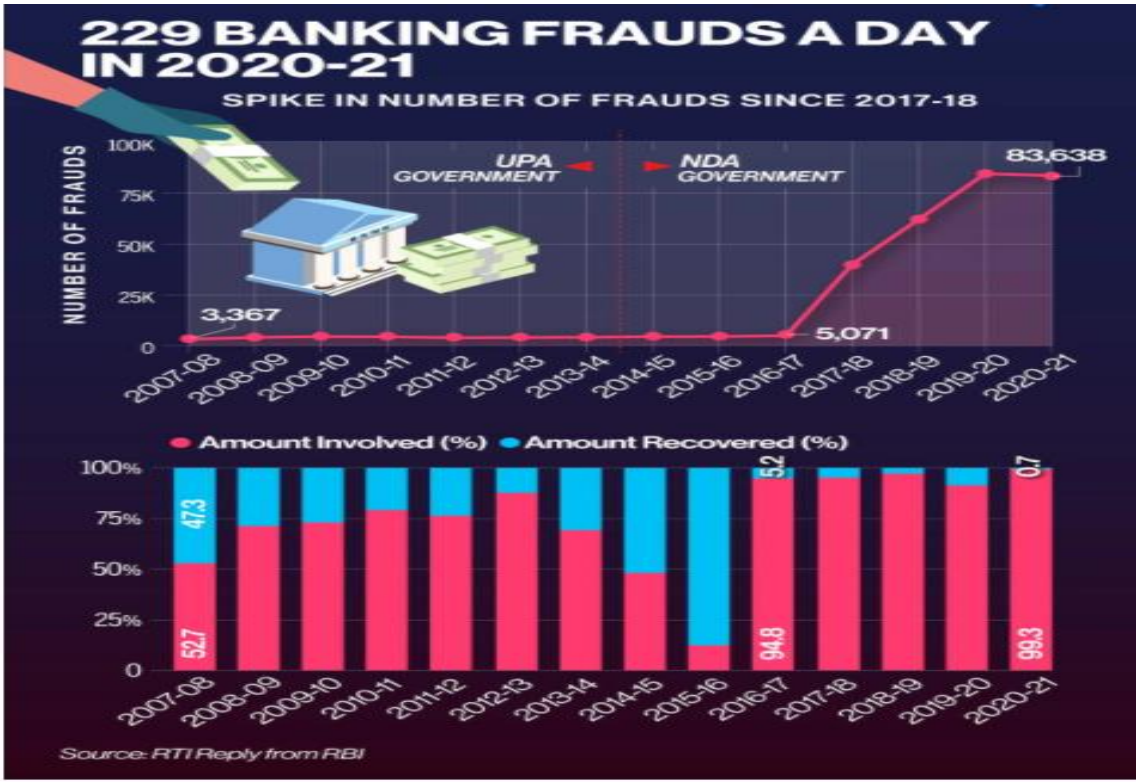
[319] State by Cybercrime Police vs. Abubakar Siddique C.C.No. 24836/2009

devices, including a personal computer and a mobile phone with browser or desktop software, a telephone, or a digital television[320].

The number of banking scams in the country has increased as the number of digital transactions has increased. According to Reserve Bank of India data, India had an average of 229 banking frauds each day in fiscal year 2020-21, with less than 1% of the total amount recovered.

In FY21, there were 83,638 cases of banking fraud in India, with a total value of Rs 1.38 lakh crore. According to data released by the RBI in response to a Right to Information request filed by India Today, only Rs 1,031.31 crore has been recovered thus far.

However, the figures for FY21 reflect a little improvement over FY20, when India had an average of 231 financial frauds each day. In 2016, there were 84,540 frauds reported in FY 20.



[320] S Kalpana," Cyber Crime: A Growing Threat To Indian E-Banking Sector" Journal of Emerging Technologies and Innovative Research (JETIR), December 2020, Volume 7, Issue 12,964-969

According to the data, the incidence of financial scams increased significantly after the government demonetized the Rs. 500 and Rs. 1,000 notes in November 2016. This surge was probably caused by the push towards digital in a cash-strapped system[321].

The number of fraud instances reported by scheduled commercial banks and select financial institutions increased from 5,071 in 2016-17 to 40,062 in 2017-18. The fraud's total value increased from Rs 23,927 crore in FY17 to Rs 41,231 crore in FY18.

Between FY15 and FY21, when the Narendra Modi-led NDA government was in office, 2.84 lakh cases of banking fraud involving a total of Rs 5.99 lakh crore were reported. A total of Rs 49,000 crore (or around 9.8%) has been recovered. During the seven years between FY08 and FY14, when the Manmohan Singh-led UPA administration was in power, there were 29,451 such cases involving Rs 31,674 crore.

During this time, Rs 7,493 crore, or 23.7 percent of the total cash involved, was recovered.

From FY08 to FY21, 3,14,270 incidences of financial fraud were registered, totaling Rs 5.31 lakh crore. Only Rs 56,502 crore has been recovered so far.

Crimes involving the use of a computer and a network[322] as a channel, source, instrument, target, or place of a crime are known as cyber-crimes. Economic crime has moved to the digital world as e-commerce and e-transactions have grown in popularity. Globally, cybercrime is on the rise, and India has seen a significant surge in cybercrime-related cases in recent years.

A report of cyber security ventures USA said that Cybercrime To Cost The World $10.5 Trillion Annually By 2025.[323]

However, such figures are simply approximations, and the true cost of cybercrime, including unreported damages, is impossible to calculate.

[321] Shagun and Ors vs Health W.P.(C) No.3193 of 2016

[322] Kharouni, L. (2012). Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit Feature (Rep.).

[323] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

6.2 OVERVIEW OF INTERNET BANKING IN INDIA

In order to understand the concept of internet banking and how it is used for that we must the basics of the internet banking and its functioning.

Following the demonetization in 2016, digital banking has grown at a faster rate. The bulk of Indian banks have built internet banking and mobile banking websites to provide users with online access to virtually all financial products. Internet banking has grown in popularity to access secure and convenient banking services[324].

Net-banking, also referred to as online banking or internet banking, is a payment system that enables bank or financial institution customers to conduct both financial and non-financial transactions online. Almost all financial services that were previously only accessible at a local branch, such as fund transfers, deposits, and online bill payments, are now available to customers through this service.[325]

Anyone who has signed up for online banking at their bank, has an active bank account, or works for a financial institution is eligible to utilise it. When a customer registers for online banking services, he or she does not need to visit the bank every time he or she need a financial service. It is not only convenient, but it is also a secure method of banking.

Some of the features of Internet Banking:[326]

- Access to both financial and non-financial banking services.
- At any time, you can check your bank balance.
- Pay bills and transfer money to other accounts.
- Keep an eye on your mortgages, loans, and bank-linked savings accounts.
- Banking in a safe and secure manner
- Protected with a one-of-a-kind ID and password
- Customers can apply for a chequebook to be issued.

[324] Sandip Harshadray Munjyasara vs State of Gujarat AIRONLINE 2018 GUJ 151

[325] https://www.paisabazaar.com/banking/internet-banking-e-banking/

[326] https://www.icicibank.com/Personal-Banking/insta-banking/internet-banking/online-banking-features.page

- Invest in general insurance.
- Automated recurring payments and standing orders can be set up or cancelled.
- Keep an eye on your bank account's investments.

And the other part of internet banking is the E- Banking which is more popular as compared to internet banking[327].

All financial services and online transactions are referred to as "e-banking" or "electronic banking" in this context. Individuals, organisations, and corporations can use a public or private network, such as the internet, to access their accounts, conduct business, or learn about different financial products and services.[328]

In India, the most common types of e-banking services are:

Internet banking is an electronic banking service that allows users to conduct various financial and non-financial activities over the internet. Customers can use the internet, often known as online banking or net-banking, to transfer money from one bank account to another, check account balances, read bank statements, pay utility bills, and much more.

Mobile Banking: This electronic banking system allows consumers to conduct financial and non-financial transactions using their mobile phones. Most banks have released mobile banking apps available on Google Play and Apple App Store. Customers can use the mobile application to access banking services like they can with the web-based site[329].

Automated Teller Machines are among the most frequent e-banking (ATM) types. Customers can withdraw money, deposit money, change their Debit Card PIN, and execute other banking transactions at ATMs. To use an ATM, a user must have a password. If a transaction is conducted from another bank's ATM, banks charge a small fee to customers who have surpassed the free transaction limit.

Debit Cards: Debit cards are carried by almost everyone. This card is linked to your bank account and allows you to go cashless. You can use your debit card for any transaction, and the amount is quickly deducted from your account.

---

[327] Sri Shakthi Institute of Engineering vs Anna University W.P.Nos.14136 & 16306 of 2021

[328] https://businessjargons.com/e-banking.html

[329] https://corporatefinanceinstitute.com/resources/knowledge/finance/mobile-banking/

Deposits and Withdrawals (Direct): This e-banking service allows customers to approve pay checks to be deposited into their accounts regularly. Customers can authorise the bank to deduct funds from their accounts to pay bills, instalments of any sort, insurance payments, and other expenses

Pay by Phone Systems: This service allows a consumer to call his or her bank and request a bill payment or a money transfer to another account.

Point-of-Sale Transfer Terminals: This service lets clients pay for their purchases instantly using a debit or credit card[330].

A slight difference between internet banking and e-banking, but both have a prominent place in the banking sector in India.

From the above, we learned about the banking system in India. The growing use of technology and the internet has led to an increase in the usage of facilities provided by the banks this has led to the increase in the cybercrime. The increase in the usage of debit and credit in daily life has changed how we shop or do transactions in our daily life. In order to under the usage of debit and credit we can see the following analysis[331] .

A recent report titled 'India Digital Payments Report' by Worldline has mentioned that, as of September, this year, the total number of cards in circulation stood at 985.35 million, which is a significant jump[332].

The expansion of debit and credit cards indicates two things: first, that Indians are placing greater demands on the economy, and second, that cashless transactions are rapidly increasing in the country. In the third quarter of 2021, 1.48 billion debit card transactions were processed, totalling Rs. 1.88 trillion. Although there was a 43 percent increase in volume, there was a minor 13 percent decrease in value when compared to Q3 2020.

[330] https://www.unionbankofindia.co.in/english/point-of-sales
[331] https://worldline.com/content/dam/worldline/documents/india/documents/worldline-india-digital-payments-report-q1-2021.pdf
[332] Prehari Cyber Security Facilities Pvt vs East Delhi Municipal Corporation W.P.(C) 5645/2021

In Q3 2021, the system received around 14.27 million debit cards and 2.21 million credit cards. Debit cards accounted for 93% of all cards in circulation, while credit cards accounted for 7%.

According to the data, "POS machines processed 607.42 million debit card transactions, while e-commerce transactions totalled 440.96 million. In terms of value, POS terminals processed Rs. 1.16 trillion, while e-commerce transactions processed Rs. 720.12 billion. POS terminals completed 284.64 million credit card transactions, while e-commerce transactions totaled 272.59 million. In terms of value, POS terminals processed Rs. 952.10 billion while e-commerce transactions processed Rs. 1.37 trillion." The most common use of debit and credit cards, according to these statistics, is for e-commerce transactions[333]

6.3 THE LEGAL STRUCTURE OF E-BANKING IN INDIA

E-Banking or Internet Banking has eliminated the need for paper and physical, financial instruments by making funds, money, and capital conveniently accessible and transferable to the beneficiary. As a result, challenges such as geographical boundaries, a lack of infrastructure, cost, trouble obtaining loans, and time consumption have been eliminated. As a result, understanding the current legal structure of e-banking as well as the difficulties that it brings, is crucial.

6.3.1 Reserve Bank of India's minimum standards on e-banking[334]

The Ministry of Information Technology published a notification on the 17th of October 2000, invoking its jurisdiction under the Information Technology Act of 2000. In response to this notice, the Reserve Bank of India (hereinafter referred to as "RBI") issued a notification on June 14, 2001, forming the S.R. Mittal Working Group Committee, and the previous notification on June 14, 2001 was amended by RBI notification on July 20, 2005, removing the need for RBI approval. The following were the minimum-security benchmarks established by the RBI.

[333] The Associated Chambers of Commerce and vs Cyber Security Integrators India Pvt O.M.P. (COMM) 390/2022.

[334] https://www.rbi.org.in/scripts/NotificationUser.aspx

- For authentication, highly encoded 128-bit Security Socket Layer-based digital signatures are used. Every bank should have a Security Officer who is entirely responsible for information technology and is responsible for enforcing the IT Act's provisions, which include requiring the Board of Directors to endorse the bank's security policy.
- Because login id, password, and biometric verification were new concepts at the time, banks were asked to adapt. For example, the bank must use a proxy server-based firewall to ensure that the Internet and Digital Banking System respects security and privacy. Before any form of Internet Banking service was available, all security structures were to be evaluated, and upgrades, bug removal, and other security software were judged required to be deployed.
- Any security breach that occurs during E-banking must be notified and addressed as soon as feasible, and future policies should be formulated with security breaches in mind. Meanwhile, it is the bank's responsibility to preserve both encoded and decoded records of all e-transaction transactions and messages.

6.3.2 Information Technology act 2000[335]

E-banking is primarily governed by the Banking Regulation Act, 1949, and the Reserve Bank of India Act, 1934, but the IT Act governs all types of cybercrime and electronic payment systems. The following are some of the key components of the IT Act to be aware of:

- The IT Act's legislative aim is to facilitate e-commerce and governance by recognising all electronic papers and digital signatures, which should be appropriately preserved and analysed by the bank because all contracts and electronic transactions are valid and enforceable under this Act[336].
- No e-banking transaction can survive if it does not comply with the provisions of the IT Act, because the protection of privacy and crypto function-based authentication of E-transactions can only take place under the protection of this Act, because data theft through unethical hacking, as well as the creation and spread of viruses, are all punishable under this Act. In fairness, the Act also gives protection to Internet Service

[335] https://www.legalindia.com/e-banking-system-in-the-banking-sector/
[336] Matispft Cyber Security Labs Private Vs the State of Andhra Pradesh W.P.No. 8860 of 2021

Providers and intermediaries to protect them from being harassed because of illicit activities on their networks.

E-banking is more practical when it comes to managing one's funds. Nonetheless, it still threatens one's financial security and right to privacy. Online banking has led to the compromise of many people's account information. Anyone considering it for financial transactions should be aware of the risks. He can take safeguards for a safer online banking experience now that he is aware of the hazards and challenges. Because it enables anyone to send money to anyone on the planet, the e-Banking system is well-liked in the United States and worldwide. Both bankers and bank customers profit from the e-banking system[337].

6.3.3 Data Protection Bill: Need of the hour in India

Data protection bill is hanging in the parliament since many years and the privacy issues related to data are increasing day by day for the instance Domino's data Leak mobi Kwik data Leak to name a few. There is urgent requirement to pass data protection bill at the earliest and keep the intermediary at check and held them liable for data Leak from the intermediary as they are required to keep them secured and away from hackers. As the data is sold in market at cheap cost. Data such as personal information, location access, residential address are readily available on the web. Data related to an individual's finances that is readily available on the web can cause huge loss to the individual. Data protection, individual privacy, and a clear articulation of the state's surveillance powers are all desperately needed, and the Bill's completion is a significant step in that direction[338].

The important components of the bill, which is now likely to be known as the Data Protection Bill, 2021, and is scheduled to be tabled in the coming days:

1. Exemption for the Government: The government and its agencies are excluded from the proposed law, according to section 35 of the bill. Section 12 allows the government to process non-personal data without obtaining consent, as long as parliamentary approval is obtained[339].

[337] J.B. Educational Society and 2 Others vs Jawaharlal Nehru Technological W.P.Nos.25815 2021

[338]https://economictimes.indiatimes.com/tech/technology/decoding-data protectionbill/articleshow/87952722.cms

[339] https://www.livemint.com/news/india/panel-recommends-govt-its-agencies-may-be-exempt-from-proposed-data-protection-law-11637595334541.html

2. Social media: The committee recommends that social media intermediaries be designated as publishers, making them liable for anything uploaded on their platform. This is because the "IT Act has not kept pace with the changing nature of the social media environment," according to the committee[340].
3. Inclusion of non-personal data: The committee considered a separate measure for non-personal data when the bill was first submitted in 2018. Both personal and non-personal data were confused in the final draught report. Information gathered by government agencies, non-profit organizations, and the corporate sector is considered non-personal data. The data is normally kept in a pseudonymous format[341].

6.4 PROMINENT CYBER CRIME IN THE FINANCIAL SECTOR

The many different varieties of cybercrime include cyberterrorism, cyberbullying, computer vandalism, software piracy, identity theft, online thefts and scams, email spam, and phishing, to name just a few. But, when it comes to electronically committed financial cybercrime, the following categories predominate:

Hacking: gaining unauthorised access to a computer or network in order to steal, corrupt, or see data. The phrase "hacking" refers to actions aimed at compromising digital devices such as computers, cell phones, tablets, and even entire networks. While hacking is not always for malicious purposes, most references to hacking and hackers now define it/them as illicit cybercriminal activity motivated by monetary gain, protest, information collection (spying), or even just the "pleasure" of the task[342]. Many people assume that a "hacker" is a self-taught genius or rogue programmer capable of modifying computer hardware or software so that it can be used in ways that the original designers never intended. However, this is a restricted viewpoint that does not begin to address the vast array of reasons why people turn to hacking[343].

Phishing: is a technique used to steal personal information such as usernames, passwords, and debit/credit card details by impersonating a trustworthy party in an internet communication and

[340] https://internetfreedom.in/privacyofthepeople-social-media-users/

[341] https://indianexpress.com/article/business/looking-at-bigger-umbrella-pdp-bill-likely-to-include-non-personal-data-7552240/

[342] https://www.malwarebytes.com/hacker

[343] Cyber Media (India) Ltd vs M/S Cyber Intelligent Security Pvt CS No. 159/11 Additional Senior Civil Judge (South), Saket Courts, New Delhi

subsequently reproducing the same information for malicious purposes. Phishing is a social engineering attack that is commonly used to gain sensitive information from individuals, such as login credentials and credit card information. When a hacker pretends as a trustworthy person and persuades a victim to open an email, instant message, or text message, this is what happens. Following that, the receiver is deceived into opening a malicious link, which can result in malware installation, system freeze as part of a ransomware attack, or the revealing of sensitive information[344]

An attack has the potential to be devastating. Unauthorized purchases, money theft, and identity theft are examples of this for individuals.

An organisation that falls victim to such an attack usually suffers significant financial losses as well as a loss of market share, reputation, and consumer trust. Depending on the extent, a phishing attempt could turn into a security disaster from which a company will struggle to recover.

Phishing example:

The following is an example of a common phishing scam:

- A mass email, purporting to be from myuniversity.edu, is sent to as many faculty members as possible.
- The user's password is due to expire, according to the email. Within 24 hours, they must go to myuniversity.edu/renewal and renew their password.

When you click the link, a variety of things can happen. Consider the following scenario:

- The user is sent to myuniversity.edurenewal.com, a fake page that looks identical to the real renewal page and asks for both new and old passwords. While watching the page, the attacker steals the original password and uses it to gain access to restricted sections of the university network.
- The user is forwarded to the password renewal page. While being routed, however, a malicious script runs in the background, stealing the user's session cookie. As a result

[344] Sheeli Goyal D/O Radhyashyam Goyal vs State of Gujarat R/CR.MA/6945/2021 In The High Court of Gujarat at Ahmedabad

of the mirrored XSS attack, the attacker now has privileged access to the university network[345].

E-mail spoofing: is a method of concealing an e-true mail's origin by forging the e-mail header to make it appear as though it came from a genuine source rather than the original sender. Spam and phishing attempts use email spoofing to fool people into thinking a message came from someone or something they know or can trust. The sender forges email headers in spoofing attacks so that client software shows the false sender address, which most users believe at face value. Users will not notice the counterfeit sender in a message until they examine the header more attentively. They are more likely to trust a name they are familiar with. As a result, they'll click harmful links, open virus attachments, send sensitive information, and even wire money to the company.

Antimalware software and recipient servers can help detect and filter fraudulent messages. Regrettably, not every email provider employs security measures. Users can still check the email headers included with each message to see if the sender address is forged.

Example of email spoofing:

- The purpose of email spoofing is to deceive people into thinking the email is from someone they know or can trust, which is usually a colleague, vendor, or brand. The attacker takes advantage of that trust by asking the victim to give information or do some other action.
- An attacker might create an email that seems like it came from PayPal as an example of email spoofing. The notification informs the user that if they do not click a link, authenticate on the site, and change their password, their account will be suspended. If the user is successfully duped and enters credentials, the attacker now has the credentials to get into the targeted person's PayPal account and potentially steal money.
- A faked email message appears real to the recipient, and many attackers include components from the official website to make the message more credible. Here's an example of email spoofing using a PayPal phishing attack:

[345] https://www.imperva.com/learn/application-security/phishing-attack-scam

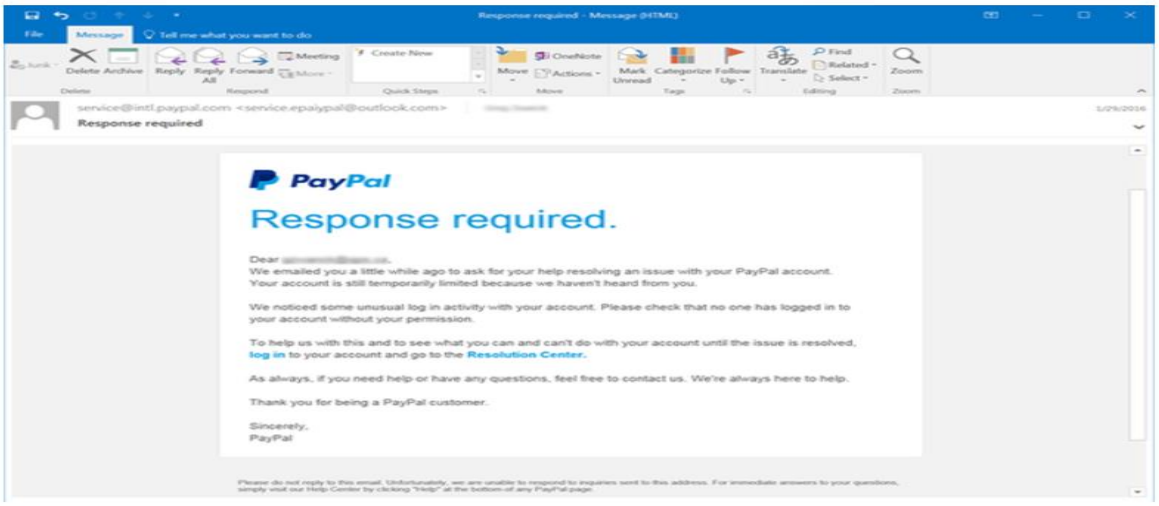


Image reference: Proofpoint.com

- The sender address is automatically input when a user sends a new email message using a standard email client (such as Microsoft Outlook). However, an attacker can send messages programmatically using basic scripts in any language that configure the sender address to a desired email address. Endpoints of the Email API allow a sender to specify a sender address regardless of whether or not that address exists. Outgoing email servers also cannot know if the sender's address is real.
- The Simple Mail Transfer Protocol retrieves and routes outgoing emails (SMTP). When a user selects "Send" in an email client, the message is initially sent to the client software's outbound SMTP server. The SMTP server identifies the recipient domain, which then sends the email to the domain's email server. The message is then routed to the correct user mailbox by the recipient's email server.
- The IP address of each server is logged and included in the email headers for each "hop" an email message takes as it travels across the internet from server to server. Many consumers do not check headers before connecting with an email sender, even though they reveal the genuine route and sender.

  The three major components of an email are:

  - The sender addresses
  - The recipient addresses

- The body of the email[346]

Spamming: Spam e-mails are unwanted and unsolicited e-mails that are sent in bulk in an attempt to force the message on persons who would not otherwise choose to receive it. Spamming, in layman's terms, is the act of flooding the Internet with uninvited or misleading messages. Spam is mostly used for commercial advertising, such as get-rich-quick schemes or the sale of fraudulent goods. However, this is not always the case.

Finally, rather than the product itself, the word refers to the aggressive methods used to advertise it. So don't fall into the trap of thinking that simply because the thing you're selling is legitimate, you can't be spamming.

True, email spamming is the most widespread form of spamming. Search engine spamming, on the other hand, is the most likely to harm your company's online presence.

Search engine spamming is the dishonest practise of altering HTML websites in order to enhance the likelihood of their being listed among the top search engine results.

Most search engine spammers are well aware that the content they promote is irrelevant and useless to internet users. Or, at the at least, they're aware that the methods they're doing to bring it to the top of search engine results are false[347].

Denial of Service: This attack is defined as an attempt by attackers to prevent legitimate users of a service from using that service by "flooding" a network to disallow legitimate network traffic, disrupting connections between two machines to prevent access to a service, or preventing a specific individual from accessing a service by "flooding" a network to disallow legitimate network traffic[348].

A Denial-of-Service (DoS) attack is one that attempts to bring a machine or network to a halt, rendering it unreachable to its intended users. DoS attacks work by inundating the target with traffic or delivering it information that causes it to crash. The DoS attack deprives genuine

[346] https://www.proofpoint.com/us/threat-reference/email-spoofing
[347] https://smallbiztrends.com/2017/02/what-is-spamming.html
[348] Net Losses: Estimating the Global Cost of Cybercrime (Rep.). (2019). Intel Security

users (workers, members, or account holders) of the service or resource they expected in both cases.

DoS assaults frequently target high-profile corporations such as banks, commerce, and media companies, as well as government and trade organisations' web servers. Despite the fact that DoS assaults rarely result in the theft or loss of sensitive information or other assets, they can cost the victim a lot of time and money to cope with.

DoS attacks can be carried out by flooding services or crashing systems. Flood assaults occur when a system receives too much traffic for the server to buffer, slowing it down and eventually stopping it. Among the most common floods are:

- The most frequent DoS technique is buffer overrun. The idea is to send more traffic to a network address than the system's engineers anticipated. It comprises the attacks described below and those aimed at exploiting flaws in specific programmes or networks.
- ICMP flood - takes advantage of misconfigured network devices by delivering faked packets that ping every computer on the targeted network rather than just one. The network is then activated to increase the traffic volume.
- SYN flood - submits a connection request to a server but does not complete the handshake. Continues until all open ports are flooded with requests, and no legitimate users can connect to them.
- Other DoS attacks simply take advantage of flaws in the target system or service, causing it to crash. In these attacks, input is received that takes advantage of vulnerabilities in the target, causing the system to crash or become significantly destabilized, making it impossible to access or utilize[349].

Advanced Persistent Threat (APT): A set of complicated, concealed, and continuing computer hacking procedures that generally target a specific entity to get into a network and gather sensitive information over a long period of time while avoiding discovery. To obtain access to the targeted network through legitimate means, the attacker usually employs some

[349] https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

form of social engineering. Data breaches can be costly if advanced persistent threat operations are successful.

An advanced persistent threat is an attack in which an unauthorised person gains access to a system or network and remains there without being noticed for a lengthy period of time. Hackers have continual access to sensitive company data, making advanced persistent attacks extremely harmful for businesses. In most cases, advanced persistent attacks do not harm enterprise networks or local PCs. The most common purpose of sophisticated persistent attacks is data theft.

Hacking the network, evading detection, devising an attack plan, mapping company data to determine where the desired data is most accessible, obtaining sensitive company data, and exfiltrating that data are all common aspects of advanced persistent threats.

Advanced persistent threats are notorious for their ability to fly under the radar, undetectable by typical security measures, and have been responsible for several significant, costly data breaches. Furthermore, as cyber thieves seek more complex methods to fulfil their objectives, advanced persistent attacks are becoming more widespread.

How Advanced persistent threats works:

- Advanced persistent threats employ various methods to get initial access to a network. Attackers may use the internet to spread malware and obtain access to secured networks, as well as physical malware infection and external exploitation.
- These attacks differ from many traditional threats, such as viruses and malware, which have a constant pattern of activity and may be repurposed to attack multiple systems or businesses. Advanced persistent threats don't attack in a broad, generic way; instead, they're meticulously organised and targeted to target a single corporation or organisation. As a result, advanced persistent attacks are highly personalised and clever, built expressly to circumvent a company's existing security procedures.
- To acquire initial access, reliable connections are frequently employed. As a result, attackers may use credentials obtained through phishing attempts or other malicious ways to gain access to workers' or business partners' accounts. This helps attackers achieve the critical goal of remaining undiscovered long enough to map the organization's systems and data and design a strategic attack plan to capture firm data.

- Malware is crucial to an advanced persistent threat's success. Malware has the capacity to hide from certain detection systems, navigate the network from system to system, acquire data, and monitor network activities once the network has been compromised. The capacity for attackers to remotely manipulate an advanced persistent threat is also crucial, allowing thieves to roam throughout the organization's network to discover critical data and get access to sensitive information[350].

ATM Skimming and Point-of-Sale Crimes: Installing a skimming device atop the machine keypad to appear as a genuine keypad or a device made to be mounted to the card reader to appear as a part of the machine is a technique of compromising the ATM machine or POS systems. Malware that directly steals credit card data can also be installed on these devices. Skimmers that are successfully installed in ATM machines gather card numbers and personal identification number (PIN) codes, which are then reproduced to carry out fraudulent transactions.

Payment card fraud includes ATM skimming. It involves rigging machines with secret recording devices in order to capture PINs and other information from credit and debit cards.

This scam targets bank ATMs as well as payment terminals at gas stations and other shops. The stolen information is then used to create fraudulent cards and spend the victims' money or withdraw cash directly from their bank accounts.

"If they can get the card number itself, it's usual for them to sell it in batches to other criminal groups who may try to use it for fraudulent purchases," says Nathan Wenzler, chief cybersecurity strategist at Tenable, a cybersecurity business in Columbia, Maryland.

Thieves use a variety of methods to steal data from credit and debit cards' magnetic stripes, including:

- PINs are captured as they are entered via a plastic overlay put over the ATM keypad.
- The data on the magnetic stripe is recorded on an overlay that is placed over the card insertion slot.
- The keypad entries and your fingers as you type are recorded by tiny cameras placed on an ATM.

[350] https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition

- Cameras, card-slot, and keypad overlays are incorporated in an overlay that covers the entire ATM faceplate.

"Skimmers are becoming increasingly difficult to detect," Wenzler cautions, "particularly with the advent of 3-D printers and other low-cost fabrication technologies."

Even more secure than magnetic stripe cards, chip-enabled payment cards remain prone to theft. Thieves can grab your PIN and other card information by inserting a super-thin shim between the chip and the chip reader inside the ATM. Shimmers are the name for these devices, and as chip technology becomes more common, they are beginning to supersede skimmers as the preferred tool of thieves.

Digital skimming: According to Ameet Naik, security advocate and head of product marketing at PerimeterX, a California-based cybersecurity firm, "cybercriminals increasingly practise the concept of digital skimming or e-skimming." "Rather of installing a physical device on the ATM, they upload malicious code into a website script that scrapes credit card data from e-commerce checkout websites."

The firm collects personal data from the buyer during an online payment transaction, explains Naik. Name, email address, phone number, password, payment card data, and verification code are usually included. "At the point of entry, this data is most sensitive," Naik adds.

Because the information was obtained from the consumer's device rather than a company server, the store, payment processor, or bank is often unaware that skimming has occurred, according to Naik.

"Because of the lack of exposure, attacks often go undiscovered for weeks or months," he explains, "while hackers harvest a large number of credit card details to sell on the dark web."

Ways to avoid E skimming

- Don't type your credit card number into a website multiple time. "If your preferred merchant offers the option of saving your card number for future purchases, take advantage of it to reduce the number of times you have to put in your information," Naik says.

- To avoid having to fill in credit card details, use alternative payment options such as Apple Pay, Google Pay, or PayPal. "However, to safeguard these services and avoid account compromise, consumers must use strong passwords," Naik advises.
- Keep an eye out for phoney checkout pages that pretend to be from an online retailer. "Pay attention to payment transactions that appear to fail," Naik says. "If this happens, call your card issuer right away so they can put a fraud alert on your account."
- Monitor your credit reports and bank and credit card statements routinely for suspicious activity, and report it right away[351].

6.5 IMPACT OF CYBERCRIME ON THE FINANCIAL SECTOR

The global banking industry is in a challenging, thought-provoking situation due to geopolitical and global macroeconomic situations. The banking industry is compelled to evaluate its existing policies to analyse better and reduce risks. Technology-driven approaches have been utilised to mitigate risk.

As a result of the advancement of information and technology (IT) and the widespread use of mobile networks in daily life, financial services have become more accessible to the general public. However, technological advancements have increased the likelihood of being a target of cyber-attacks, making financial services more accessible and affordable.

Cyber criminals have devised sophisticated means for not only stealing money, but also spying on organisations and gaining access to sensitive business data, all of which have an indirect impact on the bank's profitability. To tackle cybercrime, the banking industry must collaborate with national authorities and watchdog groups to develop a model that will help control the situation.

The lack of an efficient compilation service in the banking industry that can recognise trends in cybercrime and construct a model based on them is the main source of interest here.

Here is a short list of cybercrimes committed in the financial sector in India.

- The economic offence wing stated that cybercriminals are sending forged links after digital transaction through which they hack the phones of individuals and then compel

[351] https://www.bankrate.com/banking/what-is-atm-skimming

the users to send the one-time password by using which they empty the banks accounts[352].

- The Mumbai police caught individuals involved in cyber fraud racket part of which the accused would steal data from ATM kiosks get clone debit cards made procure swipe machines from banks on the basis of a fake company they had set up to carry out the fraud, and transfer money into their own bank accounts. They stealed card data and pin numbers from ATM kiosk using skimmers and micro cameras for the past three months. They would then get clone cards made and use them on a swiping machine to transfer money into a bank account[353].
- The following report provided that, the hackers are asking users to update their KYC using a particular website link and offering free gifts worth Rs. 50 lakhs form the bank via WhatsApp message. Cyber peace and autobot research wing studied these such incidents which were faced by smartphones users. The link which is provided by the cybercriminals redirects the users to the page of sbi which the genuine website of SBI is not and then it ask to enter sensitive information such as account number password captcha and it sends an otp which is provided by the hackers itself and it causes amount to be debited from the sbi customers[354].
- The following data breach was done to the Air India and 45 lakh passengers' information was breached. information such passport details, credit cards, frequent flyer details were all collected however Air India maintained that CVV/CVC numbers of passengers have not been compromised. Similarly, the spice jet also faced similar kind of data breach of customers and data was stolen[355].
- The kasperkey researchers pointed out the latest financial crimes to be aware in 2021, they are as follows financial cyber criminals are likey to target bitcoins more often, extortion practices will become more widespread and magecarting (stealing data from

[352] Zee News Tech, "C*ybercrimes at its peak New techniques used for financial fraud",* Zee news April 06 2021 at 11:23 pm
[353] Express new service "Bank *swipe machines emerge as latest tool of fraud for cyber criminals in Mumbai",* The Indian Express June 25, 2021 at 7:04 am
[354] India Tv, "*SBI OTP scam: Chinese hackers targeting state bank of India users offering free gifts",* India Tv News, July 08 2021 at 12:08 Pm
[355] Jitesh Vachhatani, "*Air India data of 45 lakh passengers including credit cards leaked in massive breach",* Republicworld , May 21, 2021 at 11: 23pm

e-commerce), hoax emails will rise so financial crimes will be a threat to the whole community at large[356].

The following instances show the serious impact on the financial sector due to the cybercriminals and how the cybercriminals are using technology to deceive the financial sector.

6.6 CYBER SECURITY IN THE BANKING SECTOR

In order to understand the role and importance of cyber security in banking, we should know the aspects of cyber security[357].

The technique of protecting computers, servers, mobile devices, electronic systems, networks, and data from hostile intrusions is known as **cyber security**. It's also known as electronic information security or information technology security. The phrase is used in a range of contexts, ranging from business to mobile computing, and it may be broken down into a few categories.

The practise of securing a computer network from intruders, whether targeted attackers or opportunistic malware, is known as **network security**.

Application security is concerned with ensuring that software and devices are free of dangers. A hacked application could allow access to the data it was supposed to secure. Security starts throughout the design phase, long before a programme or device is deployed.

Data integrity and privacy are protected by **information security**, both in storage and in transport.

The processes and decisions for handling and securing data assets are included in **operational security**. The protocols that dictate how and where data may be kept or exchanged, as well as the permissions users have while accessing a network, all fall under this umbrella.

Disaster recovery and business continuity are terms used to describe how a company reacts in the case of a cyber-security breach or any other catastrophe that results in the loss of

[356] Carin Smith, "Watch *out for these financial crimes threats in 2021",* Fin 24 , https://www.news24.com/fin24/companies/ict/watch-out-for-these-financial-cybercrime-threats-in-2021-20201231 22 Feb 2021 5: 28pm

[357] https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

operations or data. Disaster recovery policies define how an organisation returns operations and information to the same operational capabilities as before the disaster. Business continuity is the plan that an organisation uses when it is unable to operate due to a lack of resources.

End-user education addresses the most unpredictably unpredictable aspect of cyber-security: people. By failing to follow appropriate security measures, anyone can unintentionally introduce a virus into an otherwise protected system. It is critical for every organization's security to teach users to delete suspicious email attachments, not plug in unrecognised USB drives, and a variety of other key teachings.

As we understood the concept of cyber security in the banking sector lets understand its importance in the banking sector[358].

Keeping the bank's reputation safe

The reputation of a company can be severely harmed by a single weak link in its financial technology's cybersecurity. Cybersecurity issues can lead to a loss of public trust and a sense of insecurity among customers. As a result, having a strong team of information security analysts, cyber security analysts, and other cyber security positions becomes critical. Banks should also inform their clients about how to protect themselves against cybersecurity attacks.

Keeping the customer's information safe

Many fraudulent situations have occurred in which the personal information of innocent customers has been utilized to commit crimes. Customers are understandably suspicious and concerned about their data being lost in such circumstances. It has the potential to unleash devastation in the wrong hands. Regardless of the efforts taken, data loss can cause a customer to have many restless nights. As a result, banking must prioritize cybersecurity in order to avoid cyber-threats that put its clients at risk.

Non-compliance by banks will result in penalties.

Banks, like any other organization, must adhere to a set of rules and regulations. One of them is ensuring a robust staff to cope with cybersecurity risks. Noncompliance carries serious

[358] https://www.naukri.com/blog/the-importance-of-cybersecurity-in-banking

consequences. India Bank was fined ten million rupees by the Reserve Bank of India (RBI) in 2018 for failing to follow the RBI's cybersecurity rules There have been other other instances in which the RBI, the country's central bank, has punished various banks around the country for failing to follow its laws and regulations. Customers' data is safe from cybersecurity risks because to a well-defined compliance plan and strict adherence to it.

Safeguarding data

People have started adopting digital payment apps for online shopping, ordering food, transferring money, and other activities as the digitalization wave continues to sweep the globe. With more individuals choosing for digital transactions, hackers can simply breach banking applications and steal users' personal information.

As a result, banking technology must be strict and watchful in the face of cyber-threats. Because of these issues, banks must modernize their banking technology in order to protect themselves and their customers' data from hackers.

6.7 BIGGEST THREATS TO A BANK'S CYBER SECURITY[359]

Much of a bank's or financial institution's business is conducted via technology, especially the Internet. Your bank's sensitive data may be at risk if you don't have strong cyber security procedures in place. The most serious dangers to a bank's cyber security are listed below.

6.7.1 Data That Isn't Encrypted

This is a fundamental but critical aspect of excellent cyber security. All data saved on your banking institution's computers and on the internet should be encrypted. Even if hackers steal your data, if it's encrypted, they won't be able to use it right away - if it's not encrypted, hackers will be able to use it right away, causing major problems for your financial institutions.

6.7.2 Viruses

Malware-infected end user devices, such as PCs and mobile phones, represent a threat to your bank's cyber security every time they connect to your network. Sensitive data goes across this

[359] https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security

connection, and if the end user device has malware placed on it, that malware could attack your bank's networks if it is not secured properly.

6.7.3 Security of third Party Services

In order to better serve their customers, many banks and financial institutions use third-party services from other providers. However, if those third-party providers don't have adequate cyber protection in place, your bank could be the one to bear the brunt of the damage. Before you begin, it's critical to consider how you can protect yourself from security dangers offered by third parties.

6.7.4 Manipulation of Data

Hackers don't always go in to take data; sometimes they just want to tweak it. Unfortunately, this form of attack is difficult to identify immediately away and can cost financial organizations millions, if not billions, of dollars in losses. Because altered data doesn't always appear to be different from unaltered data on the surface, it might be difficult to tell what has and hasn't been changed if your bank has been hacked.

6.7.5 Spoofing

Spoofing is a newer sort of cyber security problem, in which hackers imitate a banking website's URL with a website that appears and functions identically. When a user submits his or her login information, hackers steal it and store it for later use. Even more worrying is the fact that modern spoofing techniques do not rely on a slightly different but similar URL to target viewers who have already visited the right URL.

6.7.6 Social engineering

Social engineering is one of the most serious challenges to banking and finance. People are frequently the weakest link in the security chain, as they can be duped into divulging important information and credentials. This can have an impact on both staff and consumers of a bank.

Social engineering can take numerous forms, such as phishing or whaling campaigns, or sending false invoices that appear to be from a reputable source. It's critical to keep your personnel up to date on social engineering techniques and how these dangers are evolving.

6.7.7 Supply chain attacks

Targeting a software manufacturer and then delivering malicious code to customers and others in the supply chain in the form of products or updates that appear to be legal is becoming an increasingly common way of malware distribution by cybercriminals. These assaults compromise distribution systems, allowing cybercriminals to gain access to the networks of the supplier's customers[360].

6.7.8 Credential Theft and Identity Theft

Account takeover is a particularly serious type of cybersecurity threat to clients, in which a criminal gains access to a customer's account and then alters information on it, preventing the real owner from accessing it or receiving account updates. Credential stuffing, in which hackers utilise computers to continually inserting different credentials until they break into an account, is a common cause of this attack. Because many consumers use the same username and password combinations across different platforms, some thieves go a step further and use that login information to access additional accounts held by the customer. They could even utilise the information acquired to commit identity theft.

6.7.9 Errors by Employees

While banks take great effort in recruiting workers who will not steal from them, employee errors, not purposeful misconduct, pose a significant cybersecurity risk. Employees may, for example, open a phishing email that infects the bank's network. . Given the COVID-19 epidemic and the fact that many banking staff work from home, simple human errors and technology flaws could expose financial institutions to new cybersecurity threats[361].

6.7.10 Business email compromise (BEC)

Malicious actors can use BEC attacks to acquire access to a business email account and impersonate the owner in order to defraud the target company's employees, customers, or partners. As a result, attackers can gain access to critical information through company systems and networks. Financial institutions are the target of BEC attacks because of the valuable information that may be obtained if the attackers succeed. Once inside, the attackers try to dupe

[360] https://www.alert-software.com/blog/cybersecurity-in-banking
[361] https://cisomag.eccouncil.org/cyberthreats-financial-service-providers

other employees into transferring money to criminal bank accounts or revealing access details that would allow them to do so.

6.7.11 Point of Sale (POS) malware

All digital consumer purchases are processed by POS systems, which are made up of hardware (such as the terminal that reads the customer's card) and software that informs the hardware what to do with the data it receives. In recent years, malware designed to infect these systems has grown in popularity, allowing thieves to harvest card data that can then be used or sold, resulting in financial gain for the attacker. This particular threat can be difficult to protect against due to a combination of hard-to-detect data-exfiltrating malware, legacy hardware that is difficult to fix, and general OS weaknesses.

6.7.12 Crypto jacking

Over the year's cryptocurrency has exploded in popularity. With essentially no restrictions in place, the market transfers millions of dollars every day, making it an ideal target for threat actors. Because cryptocurrencies are designed to be hidden and anonymous, it is difficult for victims to protect themselves or their funds in the event of a cyberattack. All an attacker needs is a well disguised phishing email to obtain access to a target's device. They can then generate and send cryptocurrency to their personal accounts from there[362].

6.8 RECOVERING OF MONEY FROM CYBER CRIMINALS, ESPECIALLY FINANCIAL CRIMES

This part of the chapter can assist you if you have lost money due to internet fraud or other types of cybercrime. You could have been duped into sending money to a criminal's account, a criminal could have hacked into your internet banking account and deceived you into permitting payments, you could have been duped into investing in a scam, or you could have been duped into sending money to a romance scammer (catfish).

Follow the steps below regardless of how the money was stolen.

i. **Report it to the cops** - It's critical that you report the problem to the cops as soon as possible. To work with your bank and other organisations, you'll need a crime number

[362] https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/the-10-biggest-cyber-threats-facing-the-financial-services-industry

from the police. You should report the bulk of online frauds and cyber-crimes to Action Fraud. Reporting the fraud will help shut it down and may also help you get your money back.

ii. **Notify your bank** - You should also contact the financial institutions involved in the payments as soon as possible. If it was your bank account that was compromised, call your bank and explain the situation. If you know which bank the money was send to you should also contact them. If this is done quick enough, they may be able to freeze the money if it is still in transit and both should kick off a fraud investigation.

iii. **Beware of money-recovery scams**: after stealing money, criminals frequently call their victims posing as their bank, the police, or money-recovery experts. The goal is to steal more money by requesting that you transfer funds to a "secure" account or tricking you into revealing details that will facilitate a subsequent crime. Do not put your trust in any phone, email, or text messages. Instead, contact the organization directly to ensure that it was they who attempted to contact you.

6.9 APPROACHES TO DEAL WITH CYBERCRIME RELATED FINANCIAL FRAUDS

6.9.1 When you've been duped into paying a fee (authorised push payment)

Since 2019, the majority of institutions have agreed to follow a voluntary agreement on how to handle payments made to scammers. This concentrates on payments that have only been authorised by the victim - in other words, payments that you have made or approved. According to the code, banks cannot simply dismiss victims' accusations; instead, they must investigate and determine whether the bank has fulfilled its obligation to safeguard you from making these types of payments.

i. Report the scam to your bank's fraud team - the first step is to notify your bank's fraud team of the problem. The bank will launch an investigation as a result of this.
ii. Fraud inquiry - your bank has 10 days to investigate and report back on whether or not it will refund your funds.

There are three possible outcomes for reimbursement:

iii. Full reimbursement - your bank admits they didn't do enough to notify you about the transfer; therefore, you get your entire deposit back.
iv. Your bank decides that their warnings were sufficient, and that you ignored them or were 'negligent' in your own checks, therefore they refuse to refund your money.
v. You could have done more and the bank could have done more, which is referred to as Shared Responsibility. You will receive half of your money back.
vi. Making a complaint - If you do not receive a complete refund, you should contact the Financial Ombudsman Services. They may support you because they believe the bank's warnings were insufficient, ineffective, or impactful, or that the bank should have recognised the very unusual transactions.

6.9.2 When a criminal uses your accounts to make a payment (unauthorised payment).

In this case, the criminal gained access to your online bank account and made the transaction despite the fact that you did not authorise it. This happens frequently when people are duped into giving criminals remote access to their computers, allowing them to take control and access their online bank accounts[363].

Steps to followed for filling cyber complaint.

i. The first step in filing a cyber-crime complaint is to file a written complaint with the city's cyber-crime unit. A cyber offence, according to the IT Act, is subject to international jurisdiction. This means a cyber-crime complaint can be filed with any of India's cyber cells, regardless of where the crime was first committed. Most Indian cities now have a separate cyber-crime unit.
ii. When registering a cybercrime report, you must include your name, contact information, and mailing address. You must respond to the written complaint to the Head of the Cyber Crime Cell of the city where you are filing the cyber-crime complaint.
iii. If you are a victim of online harassment, you can get legal advice to help you report the incident to the police station. You may also be asked to submit specific documents with your complaint. This, however, would be contingent on the nature of the offence.

[363] https://www.thecyberhelpline.com/guides/money-recovery

iv. File a First Information Report (FIR) at the local police station if you cannot access any of India's cyber cells. If your complaint isn't accepted there, you can go to the city's Commissioner or the Judicial Magistrate.
v. The Indian Penal Code covers some cybercrime charges. To report a cyber crime, you can file a FIR with the nearest local police station. Every police officer, regardless of the jurisdiction in which the crime was committed, is required by Section 154 of the Code of Criminal Procedure to record the information/complaint of an offence.
vi. The majority of cyber offences are regarded as cognizable offences under the Indian Penal Code. A cognizable offence is one that does not require a warrant for an arrest or inquiry. A police officer is required to record a Zero FIR from the complainant in this scenario. He must then deliver it to the police station in charge of the jurisdiction where the crime was occurred.
vii. Zero FIR provides some relief to victims of crimes that require quick attention/investigation because it avoids spending time engaging the services of a police officer[364].

6.9.3 Keep the following information on digital transactions readily available to you.

i. When a customer is a victim of digital transaction fraud, they must first preserve screenshots of any SMS, email, bogus website, UPI handle, or cell number used to perpetrate the fraud.
ii. Customers who have been cheated via e-commerce platforms could take a snapshot of the merchant's web page and save it.
iii. If they are a victim of ATM skimming, it is the theft of client information via which the crime took place.
iv. Customers who have been cheated via e-commerce platforms could take a snapshot of the merchant's web page and save it. If they are a victim of ATM skimming, which is when a device is placed unlawfully at an ATM terminal to collect client information, the customer should keep a record of the ATM location, address, and phone number.

6.9.4 Who should one report to:

[364] https://ifflab.org/how-to-file-a-cyber-crime-complaint-in-india

i. Once you've realised you've been a victim of payment fraud and written down the details, you'll need to start the reporting process.
ii. Your first port of call should be the bank, NBFC, or payment platform where you were cheated.
iii. Customers should report fraud to their bank as well as the payment company, whether it's Google Pay, Paytm, PhonePe, or another. Whether it be Google Pay, Paytm, PhonePe, or another payment company. Customers should report payment fraud on an e-commerce website, a point-of-sale device, or an ATM to the card issuing bank. If you made a purchase with an SBI debit or credit card, you must report it to SBI.

v. Customers should file a first information report (FIR) with their local cyber-crime police department after filing a complaint with the relevant company. The Ministry of Home Affairs provides a cyber-crime portal that lists the appropriate cyber-crime police stations in each state.
vi. Customers should follow the actions outlined in the NPCI's FAQs in the event of a UPI, IMPS, FASTag, Aadhar Enabled Payments System, or Bharat QR fraud. There is also a dedicated portal for reporting Bharat Bill Payment System grievances[365].

6.9.5 What if I am at fault?

i. Let's be honest about it. Customers' carelessness leads to a number of frauds. For example, giving out OTPs or KYC details over the phone is not something a consumer should do.
ii. However, it is possible. If customers are at fault, would they still be compensated? Not all of the time. When a client's irresponsibility causes a loss, such as when he shares payment credentials, the consumer is responsible for the entire loss until he reports the unauthorised activity to the bank. According to the RBI notification, any loss incurred after the unauthorised transaction has been reported will be borne by the bank.
iii. If the customer contributed to the fraud through their own negligence in both unauthorised electronic bank and PPI transactions, neither the customer nor the bank would be held liable there are further unauthorised transactions conducted after the customer has filed a report then the bank and PPI issuer will bear the loss[366].

[365] rbi.org.in/scripts/Notification User
[366] https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11446

6.9.6 Some of the grey areas:

Payment fraud and culpability for such scams are not black-and-white situations. A variety of grey regions are being contested.

Paytm recently filed a lawsuit against the government and telecom firms in the Delhi High Court.

According to the plea, Paytm lost over Rs 10 crore of its customers' money to criminals between June 2019 and April 2020, according to a copy seen by BloombergQuint. Customers were misled by these con artists using a variety of ways, including mass SMS services offered by telecom companies.

Paytm claims that telcos have failed to stop these phishing efforts and the problem of unwanted promotional messages. As a result, it has claimed Rs 100 crore in damages from them.

The liability of the customer's 'issuing bank' and the 'acquiring bank' utilised by fraudulent merchant users is also a point of contention.

"The lack of accountability on the acquiring bank, which is employed by the merchant to commit the fraud, is an obvious loophole in current legislation." "The regulator should also hold the bank where the money is being syphoned accountable for fraud transactions," said NS Nappinai, a Supreme Court of India counsel and founder of Cyber Saathi.

Another issue is the time it takes to resolve and reimburse clients, even when they follow the reporting deadlines for payment fraud. Even once the customer reports the theft within three days, Memon noted, there is a lot of back-and-forth between companies and the customer, as well as third parties if they are involved. While the RBI guidelines state that customer fraud should be resolved within 90 days, he claims that in fact it might take much longer[367].

[367] https://www.bloombergquint.com/business/bq-explains-hit-by-a-payment-fraud-heres-what-you-need-to-do

CHAPTER VII
CYBERCRIMES IN THE FINANCIAL SECTOR IN MUMBAI: AN EMPIRICAL STUDY

7. 1 INTRODUCTION

In view of the above topic relating to cybercrimes and cyber laws in India: a study with special reference to the financial sector in Mumbai. The present study was analytical as well as empirical in nature. This study followed doctrinal research methods in the compilation, organization, interpretation and systematization of the primary and secondary source material. The researcher used both primary as well as secondary sources. The researcher collects the secondary data from published sources such as various books, Indian and foreign journals, online journals, newspapers, online newspapers, research articles, and various websites to collect literature and data for the study and analysis. The researcher has also adopted the empirical research method in this present study to collect and generalize the information through questionnaires from various respondents on the subject. The primary data is collected from 250 respondents and 20 cyber experts from Mumbai/Maharashtra. In this study, the primary data collected from the respondents have also been used to prove/ disprove the research hypothesis

7.2 METHOD OF DATA COLLECTION

1) The researcher has also adopted the empirical research method in this present study to collect and generalize the information through questionnaires from various respondents on the subject. The primary data is collected on the selected lawyers, cyber experts, Police personnel, law faculties, general respondents, and Banking professional of Mumbai/Maharashtra.

2) In this study, Questionnaire and Personal Interview method has been used for getting the results. An attempt has been made to analyse the views of legal fraternity and cyber experts through an empirical study on the subject. Questionnaires have been framed for legal fraternity, law faculties, banking professionals, general respondents and personal interview for cyber experts and police personnel to gain insights and opinions covering cybercrimes and cyber laws.

3) Universe for the collection of data is Mumbai being the hub of cybercrimes in India. As cases are seen on daily basis. The numbers of respondents are Banking Professional -50, law

faculties- 50, Cyber experts - 10, Police Personnel – 10, Lawyers - 50 and general respondents 100. The questionnaire contains both open ended and close ended questions.

4) The empirical part of the study involved in depth analysis of the responses given by the respondents through various questionnaires and personal interview taken of cyber experts and police personnel. The General respondents Annexure 1 which are the ordinary citizens were selected for the research in order to understand their experiences and how often they are victim of cyber criminals and specially the financial fraud which are mostly faced by citizens.

DATA COLLECTION	**GENERAL RESPONDENTS**	**CYBER EXPERTS**	**LAW FACULTIES-**	**FINANCIAL SECTOR EMPLOYEES**	**POLICE PERSONNEL**	**LAWYERS**
NO. OF RESPONDENTS	**100**	**10**	**50**	**50**	**10**	**50**
METHODOLOGY	**QUESTIONNAIRE**	**PERSONAL INTERVIEW**	**QUESTIONNAIRE**	**QUESTIONNAIRE**	**PERSONAL INTERVIEW**	**QUESTIONNAIRE**

1) The general respondents where from the age group of 18 years to 40+, variety of questions were asked from the respondents so that a clear picture is formed regarding the cybercrime and how much vulnerable individuals are to cyber criminals. The questions varied from basic questions like are you aware of cyber-crime and some difficult questions were also asked from the respondents. Cyber security and cyber-crime in the financial should be prioritized in the current situation. Around 145 responses were received from Mumbai and its nearby areas such as Navi Mumbai, Thane and South Mumbai.

2) Responses from the financial sector were also taken, financial sector employees from different background such as private banks, government banks, payments banks, NBFCs gave their responses regarding the financial crimes in Mumbai. 25 responses from financial sector were received and they were asked questions regarding the crime in the financial sector, how its solved, nature of common offence, how often people are targeted, how its solved all these questions were asked from the financial sector.
3) Responses from the law faculties were also taken regarding the cyber-crimes and Information Technology Act 2000, whether it should be amended or new laws should be introduced regarding the same, question were asked regarding the cyber laws, critical infrastructure, IT Act 2000 amendments, cyber security and its importance.
4) Responses from the lawyers were also taken to understand the nature of practice required to deal with cyber-crimes and how it dealt with daily life in courts. Questions regarding the practice, how difficult it is to practice IT act 2000 and how much aware lawyers are in relation to cyber-crime and cyber laws.
5) Personal/ Telephonic Interview of cyber experts were also taken to under nature and functioning of how cyber criminals work, what nature of co-ordination is required in order to tackle the cyber criminals, how fast one can stop the financial fraud, whether Mumbai is safe in relation to financial frauds in Mumbai.
6) Personal/Telephonic interview of Police personnel were taken in order to understand the nature of working of police, how they function, how much time is taken to solve the crime whether people are aware of how cyber complaint is made.

7.3 CYBER CRIMES IN THE FINANCIAL SECTOR IN MUMBAI: AN EMPIRICAL STUDY

7.3.1 GENERAL RESPONDENTS' OBSERVATIONS

The demographics of the questionnaire of the general respondents belonged to the age group of 18 years to 40+, variety of questions were asked from the respondents so that a clear picture is formed regarding the cybercrime and how much vulnerable individuals are to cyber criminals. The questions varied from basic questions like are you aware of cyber-crime and some difficult questions were also asked from the respondents like cyber security and cyber-crime in the financial should be given priority in the current situation. Around 145 responses were received from Mumbai and its nearby areas such as Navi Mumbai, Thane and South

Mumbai. The responses gave a clear picture about the situation of cyber-crime in the financial sector in Mumbai.

A. The total Number of responses received from the questionnaire of general respondents was 146; in that male were 71 that amounted to 48.6%, and 75 were female that amounted to 51.4% of the total responses as seen Figure 1.

Statistics

Gender

N	Valid	146
	Missing	0

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	71	48.6	48.6	48.6
	Female	75	51.4	51.4	100.0
	Total	146	100.0	100.0	

Figure 1: Total Number of Male and Females of General Respondents

B. The total age of respondents varied from the age group of 18 to 51 plus and 43% of the respondents belonged to the age group of 25-34 as our youth is the perfect example of using the mobile, internet on daily basis as seen in the figure 2.

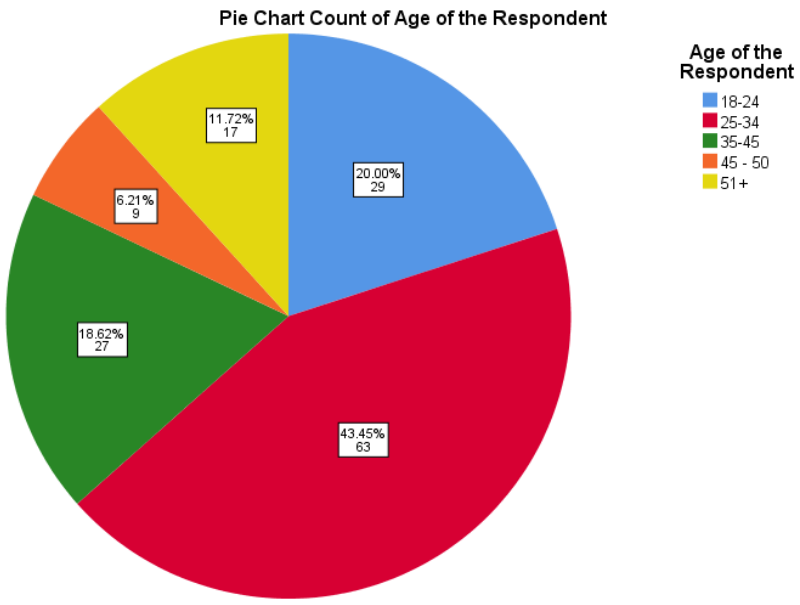


Figure 2: Age of the respondents

The first question asked to the general respondents regarding the awareness of the cyber-crime and the results depicted, 88% i.e., 129 people are aware of cyber-crime and 11% i.e. 17 were unaware of cyber-crime as seen in the figure 3. In reality it is the opposite people are aware but easy targets of cyber criminals. And as suggested by the cyber experts educated people are more unaware of cyber-crimes.

Statistics

Q 1 How much aware you are about cyber crime

N	Valid	146
	Missing	0

Q 1 How much aware you are about cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I am not aware	17	11.6	11.6	11.6
	I am aware	129	88.4	88.4	100.0
	Total	146	100.0	100.0	

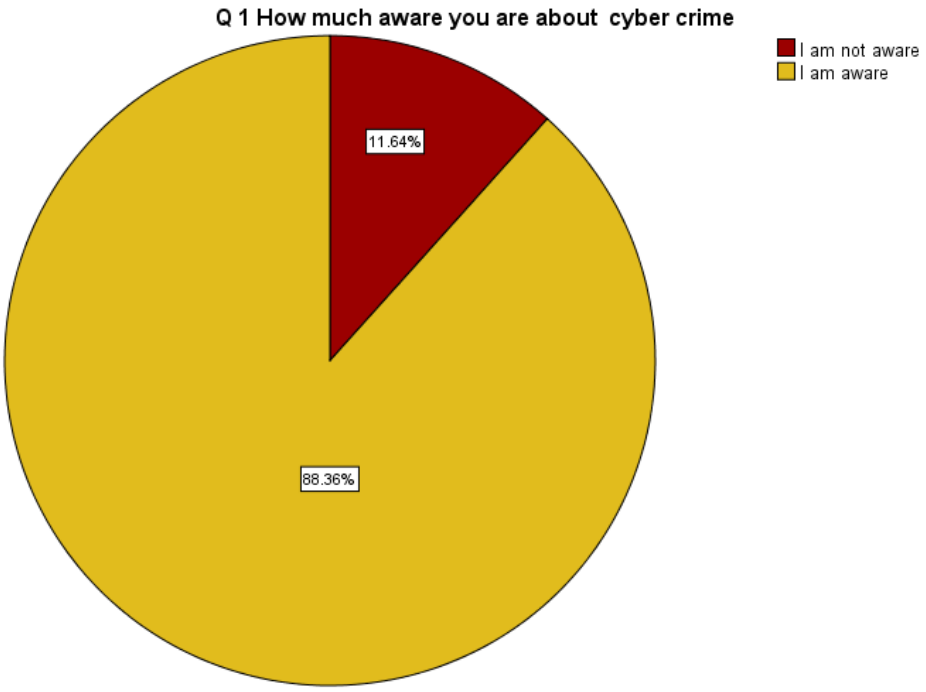


Figure 3: Awareness about cyber crime

Observation: The general respondents were aware of cyber-crime. Awareness regarding cyber-criminals is a positive point as this helps from getting scammed. 88% of the respondents were aware of cyber-crime but awareness and how to tackle cyber-crime is a different thing altogether. People are aware of cyber-crime as they know what is cyber crime but they lack the required essentials to protect themselves from cyber criminals. As a result, they fall prey to cyber criminals on numerous occasions. The police personnel also submitted that Educated individuals are aware of cyber-crime and they though being aware fall prey to cyber criminals. Cyber experts also pointed out that awareness is the main aspect to curb cyber-crime in the current scenario as awareness with protection taken by the individuals is the key to protect one self from the cyber criminals.

2. Respondents were asked about the awareness of cyber security and the data gathered showed that 74% i.e., 109 respondents knew about the cyber security and 25% i.e., 37 people are unaware of the cyber security as seen in figure 4. The main question was to understand that how much people are aware of cyber security. It provided us with data that showed people are aware but in reality, it is not the case cyber security structure is strong but those who are using

it are not aware of how to use the methods given in cyber security. For example, two step verification in WhatsApp most of the people are unaware of the verification provided in the app.

Statistics

Q 2 How much aware you are about cyber security

N	Valid	146
	Missing	0

Q 2 How much aware you are about cyber security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	I am not aware	37	25.3	25.3	25.3
	I am aware	109	74.7	74.7	100.0
	Total	146	100.0	100.0	

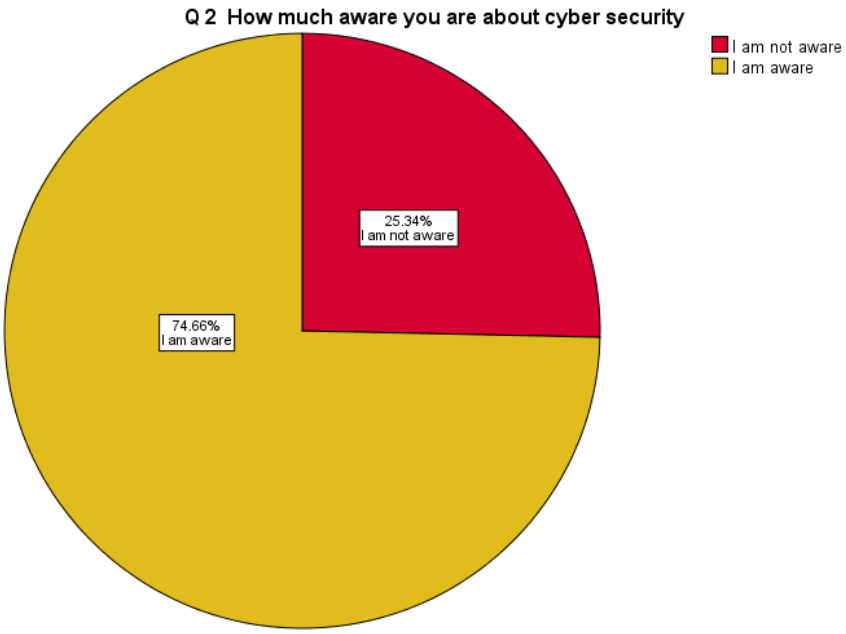


Figure 4: Awareness about cyber security.

Observation: The general respondents were aware of cyber security and but the results of the study depict ignorance and unawareness as submitted by the financial sector respondents agreed to that, citizens are not aware of cyber security its importance. Cyber security in day-to-day life is nothing but not sharing otp, not clicking on any suspicious link, not sharing important passwords to unidentified persons. And cyber security in relation to critical infrastructure is next level of authentication requirements. Cyber security will play a crucial role in the coming future as it will help to curb the cyber-crime and as pointed out by the researcher through the interviews of cyber experts and financial sector response's they admitted that cyber security awareness is missing among the citizens.

3. Respondents were asked about; how safe they feel your information is while using the internet. The responses showed that 50% i.e., 74 respondents felt that their information is not safe at all and 45% i.e., 66 respondents felt that their information is safe and lastly just 4% i.e 6 respondents felt that its very safe. In current situation the information given by the user on the internet is not safe at all as seen in the figure 5.

Statistics

Q 3 While using the internet, how safe do you feel your information is

N	Valid	146
	Missing	0

Q 3 While using the internet, how safe do you feel your information is

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Safe	66	45.2	45.2	45.2
	Very safe	6	4.1	4.1	49.3
	Not safe at all	74	50.7	50.7	100.0
	Total	146	100.0	100.0	

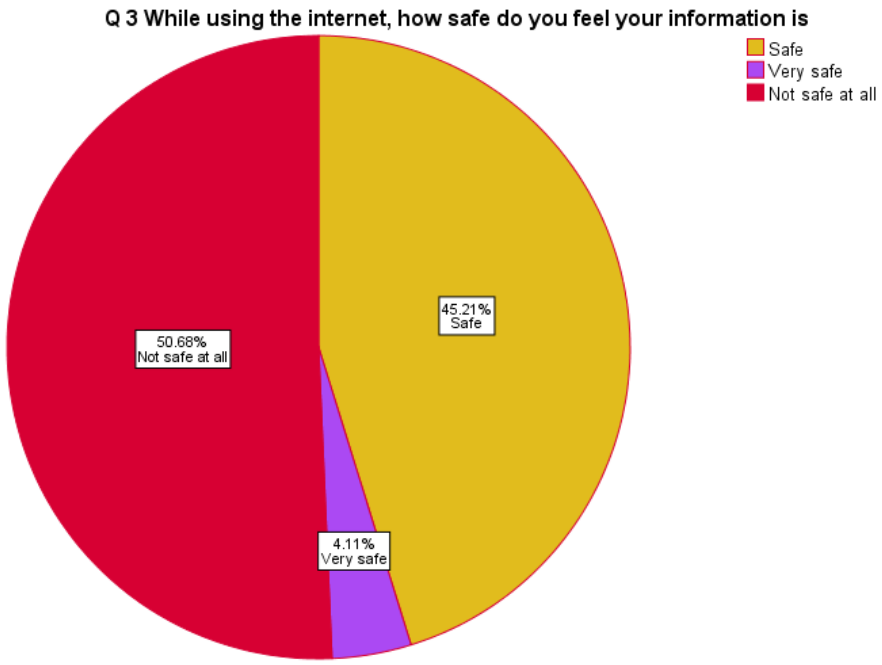


Figure 5: How safe your information is while using internet.

Observation: The general respondents were asked about how safe they feel their information while using the internet and it's the opposite the respondents agreed that their data, information is not safe at all. The general respondents agreed that information on the cyber space is something which is not safe at all. In day-to-day usage one has to enter some or the other credentials on the internet to access something important. 74% of the respondents agreed that any information whether it is personal, financial, or medical is not safe at all. As on numerous occasions the data has been breached by the cyber criminals. Such an example is dominos data leak, mobikwik data leak, linked data leak. This information provides us with the urgent need of data protection bill which is still pending in the parliament. Due importance should be given to the data entered by an individual and third-party corporations should be held liable in case of data breach.

4. Respondents were asked about how important is to have a strong password for financial apps or social media accounts. 86% i.e., 126 respondents voted for its very important to have a strong password for financial as well as social media accounts. 11% i.e., 16 respondents it is just

important. It showed that people are aware regarding the nature of passwords required to overcome the cyber criminals as seen in figure 6.

Statistics

Q 4 How important is it to have a strong password in your social accounts/financial apps

N	Valid	146
	Missing	0

Q 4 How important is it to have a strong password in your social accounts/financial apps

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Important	16	11.0	11.0	11.0
	Very Important	126	86.3	86.3	97.3
	Not Important	4	2.7	2.7	100.0
	Total	146	100.0	100.0	

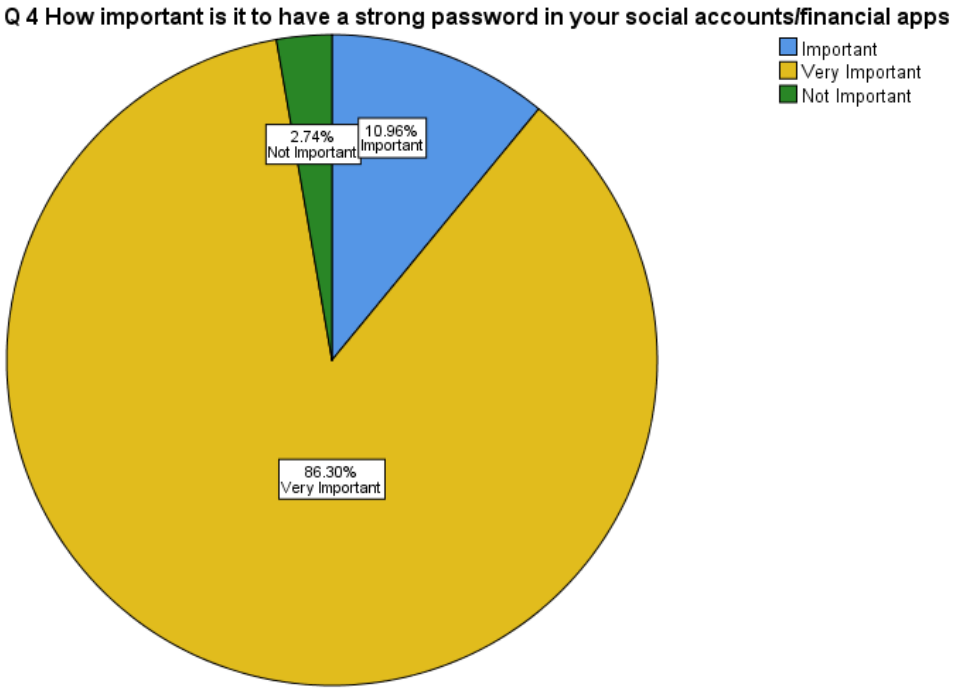


Figure 6: Strong password for financial apps/social media accounts.

Observation: Strong password is the key to curb cyber-crime as per the analysis its visible that 86% of the respondents said that very strong password should be used for financial apps, social media accounts to stop cyber criminals getting access to these accounts. Strong passwords as suggested by the experts that on websites its written that one should change the password frequently and same goes with banking apps it should be changed every month so that if cyber criminals get access to it they cannot use that as it has been changed. Now adays RBI is displaying advertisement regarding the passwords one should have on tv and it should not be shared to anyone. Similarly, third party payment apps such as paytm, google pay display their advertisement suggesting that no one from google pay or paytm will call any person to ask for any password or to update any details.

5. Respondents were asked about the whether they lost money while online shopping, 83% i.e., 122 respondents never lost money due to online shopping and 16% i.e., 24 respondents lost money due to online shopping. It showed that, online shopping with proper e commerce websites its still safe option to the citizens as seen in figure 7. Online shopping done with proper precautions and proper channel will cater to help reduce cyber-crimes in the e-commerce part as seen in the data the number presents a strong case for the e-commerce online shopping websites and application.

Statistics

Q 5 Have you ever lost your money due to cyber crimes online shopping

N	Valid	146
	Missing	0

Q 5 Have you ever lost your money due to cyber crimes online shopping

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Never Lost Money due to online shopping	122	83.6	83.6	83.6
	Money lost due to online shopping	24	16.4	16.4	100.0
	Total	146	100.0	100.0	

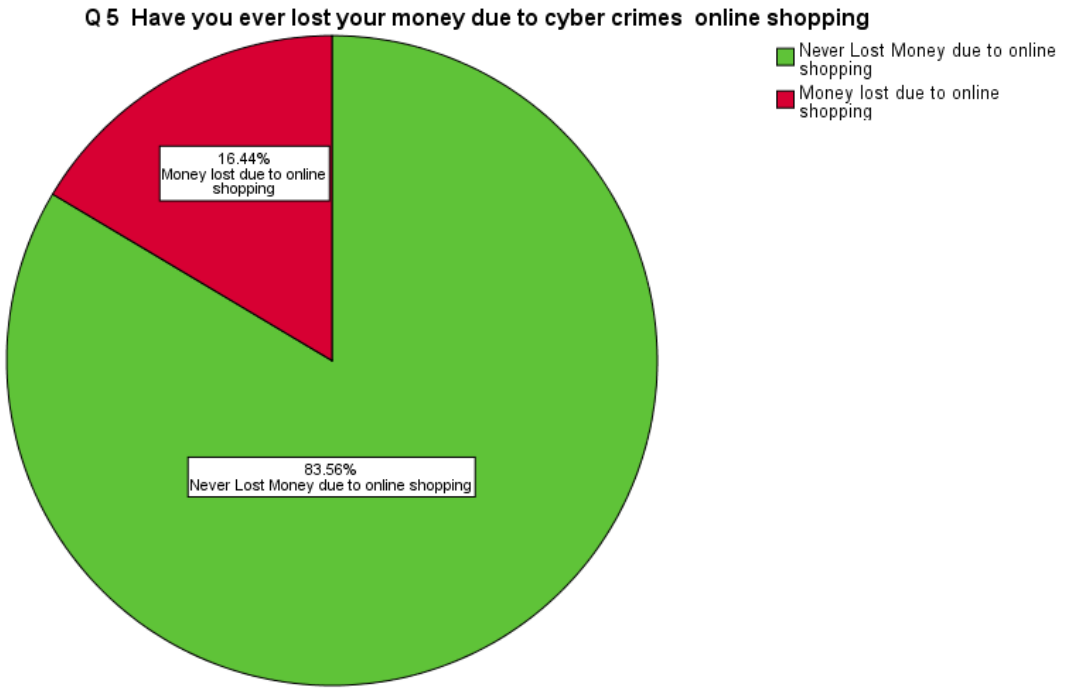


Figure 7: lost money while doing online shopping

Observation: The most positive point of e commerce shopping is that in my responses the respondents never lost money while doing online shopping. This show that if e commerce genuine websites or apps is used it helps to cater cyber-crime as the security and authentication is very high as compared to unofficial websites. 16% of the respondents lost money while online shopping. Cyber criminals usually use the method of customer care calls to an e commerce customer and lure him to click on suspicious links which take them to different website from where they make online transactions, finally their bank amount gets debited and money reaches the cyber criminal's. E commerce with caution is very good example of security and authentication requirements one has to fill to get access in to the account. Similarly one has to be aware whether he is accessing the genuine app or website of the e commerce and any while making transaction on the website, app or browser and if they found any form of discrepancy is their in relation to the link or the website one should stop the payment the immediately.

6. The general respondents were asked about the trojan and malware, auto generated mail, ambiguous material on profiles, never experienced any of these situations. Auto generated

email was the most important factor as cyber criminals mostly prefer the emails, as people tend to click on auto generated emails to reach a different link that is controlled by cyber criminals. 22% i.e., 32 respondents said that they have experienced auto generated emails in the inbox, trojan and malware 15.8% i.e., 23 respondents faced the virus-related issues from the cyber criminals. 57% i.e., 84 respondents never experienced all these situations as seen in the figure 8.

Statistics

Q 6 Have you ever experienced any of these situations

N	Valid	146
	Missing	0

Q 6 Have you ever experienced any of these situations

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Trojan or malware	23	15.8	15.8	15.8
	Auto generated mail in your inbox	32	21.9	21.9	37.7
	Publishing ambiguous material on your profiles	7	4.8	4.8	42.5
	Never experienced any situations	84	57.5	57.5	100.0
	Total	146	100.0	100.0	

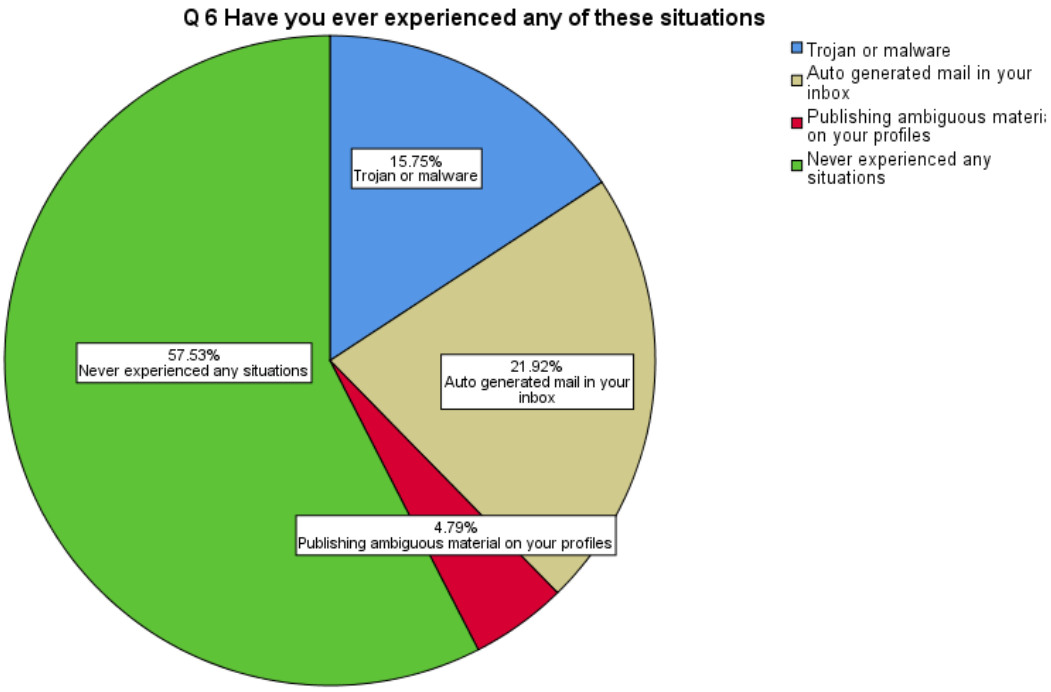


Figure 8: Experienced situations

Observation: Auto generated emails and trojan/malware are the key components which users face on daily basis as these mails and various suspicious links in the e- mail which takes the user to malicious login websites, that take away the login credentials of the user. As 52% of the respondents received auto generated emails and malicious malware. Auto generated emails and suspicious link are the key used by the cyber criminals as this the easiest method adopted by them , one click on the link will make the data of your device easily accessible to the cyber criminals , one should be aware of the frivolous emails and suspected links generated by the cyber criminals.

7. Respondents were asked about the how many times they have a victim been of cyber-crime. The data showed that 72% of the respondents were never been a victim of cyber-crime and similarly 24% i.e., 24 respondents have been victim of cyber-crime once and 3.4% i.e., 5 respondents have been victim 2-4 times. The data showed that, respondents are aware and never had been a victim but they are victim of cyber-crime as auto generated emails targeted the individuals as seen in figure 8. People are targeted but they are not aware that they are been targeted by the cyber criminals. Figure 9 gives a clear picture that most of the respondents are never been a victim of cyber-crime and similarly 35 respondents have been a victim

Statistics

Q 7 How many times you have been a victim of a cyber crime

N	Valid	146
	Missing	0

Q 7 How many times you have been victim of a cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Never been a victim	105	71.9	71.9	71.9
	1 time	35	24.0	24.0	95.9
	2 – 4 times	5	3.4	3.4	99.3
	More than 5 times	1	.7	.7	100.0
	Total	146	100.0	100.0	

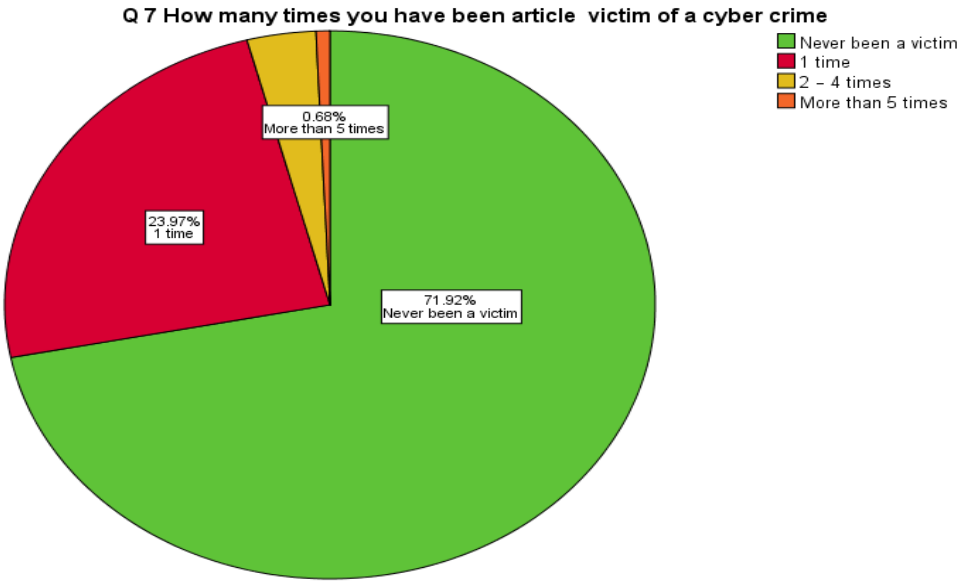


Figure 9: Victim of cyber crime

Observation: The respondents claimed that, most of them were never been victim of cyber-crime as this is a good sign that they are aware of cyber-crime and 23% of the respondents were target of cyber criminals. As the case processing summary, the respondents belonging to

the age group of 25-34 have been victim of cyber-crime in total 19 times this show that, they are aware of cyber-crime but still prone to cyber criminals. Getting victim of cyber crime is common now adays as we receive multiple sms, links, discounts, extra premium on the credit or debit and unaware citizens fall prey to these scams used by the cyber criminals.

7A. Respondents were between the age group of 18 to 51+ and similarly whether they have been article victim of cyber-crime. If we see figure 10 we can see that the respondents belonging to the age group of 25-34 have been victim total 19 times this show that, they are aware of cyber-crime but still prone to cyber criminals.

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Age of the Respondent * Q 7 How many times you have been article victim of a cyber crime	145	99.3%	1	0.7%	146	100.0%

Age of the Respondent * Q 7 How many times you have been victim of a cyber-crime Crosstabulation

Count

		Q 7 How many times you have been victim of a cyber crime				
		Never been a victim	1 time	2 – 4 times	More than 5 times	Total
Age of the Respondent	18-24	18	10	1	0	29
	25-34	43	15	4	1	63
	35-45	20	7	0	0	27
	45 - 50	7	2	0	0	9
	51+	16	1	0	0	17
Total		104	35	5	1	145

Figure 10: Age group and how many times they are victim of cyber-crime.

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.090[a]	12	.608
Likelihood Ratio	12.768	12	.386

Linear-by-Linear Association	5.694	1	.017
N of Valid Cases	145		

a. 12 cells (60.0%) have expected count less than 5. The minimum expected count is .06.

Observation: The respondents belonging to the age group of 25-34 have been victim total 19 times this show that, they are aware of cyber-crime but still prone to cyber criminals. As the young generation is the easiest target of the cyber criminals, lack of awareness among the youngsters and lenient approach towards the financial transactions they make on day-to-basis they easily fall prey to cyber criminals. On the same footing the people above the age of 40 are the easiest target of the cyber criminals as suggested by the financial sector respondents.

8. Respondents were asked about the cyber laws whether it is capable to control the cyber-crimes. 50.7% i.e., 74 respondents felt that yes, it is able to control the cyber-crimes and 49.3% i.e., 72 people felt that it is not able control cyber-crimes as seen in figure 11. In general, it is not able to control crime.

Statistics

Q 8 Do you agree that cyber laws of the country are able to control cyber crimes

N	Valid	146
	Missing	0

Q 8 Do you agree that cyber laws of the country are able to control cyber crimes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	74	50.7	50.7	50.7
	No	72	49.3	49.3	100.0
	Total	146	100.0	100.0	

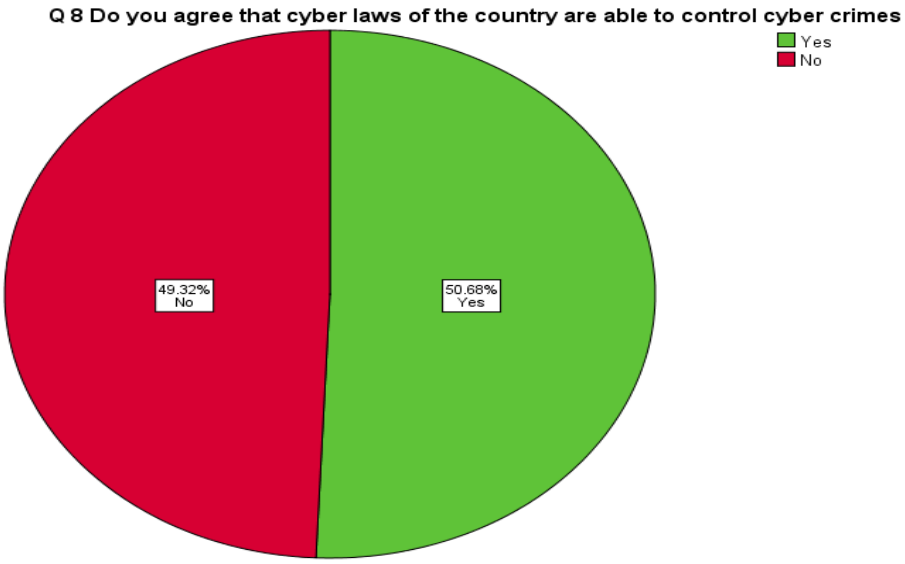


Figure 11: Cyber laws of the country are able to control cyber-crime.

Observation: The respondents believe that cyber laws of the country are not capable of controlling the cyber-crimes in India. 50% agreed that cyber-crime of the are full proof to curb cyber crime in India. Information technology act 2000 is the most important act which can be the saviour to the citizens in the coming future. As we can see its 50%-50% people do believe that current structure of the IT act is not capable to control cyber-crime. Immediate plan should be chalked out to amend improve the IT act so that it will make the life of the cyber criminals tough.

9. Respondents were asked rate on a scale of 5 to 1, where is the most important and 1 is the least important about how important is to be safe online and similarly 71% i.e., 104 respondents felt that is very important to be safe online whether it is social media, financial transactions as seen figure 12.

Statistics

Q 9 How important is it to be safe online (social media, net banking,ETC) (5 is more important, 1 is least important)

N	Valid	146
	Missing	0

Q 9 How important is it to be safe online (social media, net banking,ETC) (5 is more important, 1 is least important)

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	9	6.2	6.2	6.2
	2	5	3.4	3.4	9.6
	3	21	14.4	14.4	24.0
	4	7	4.8	4.8	28.8
	5	104	71.2	71.2	100.0
	Total	146	100.0	100.0	

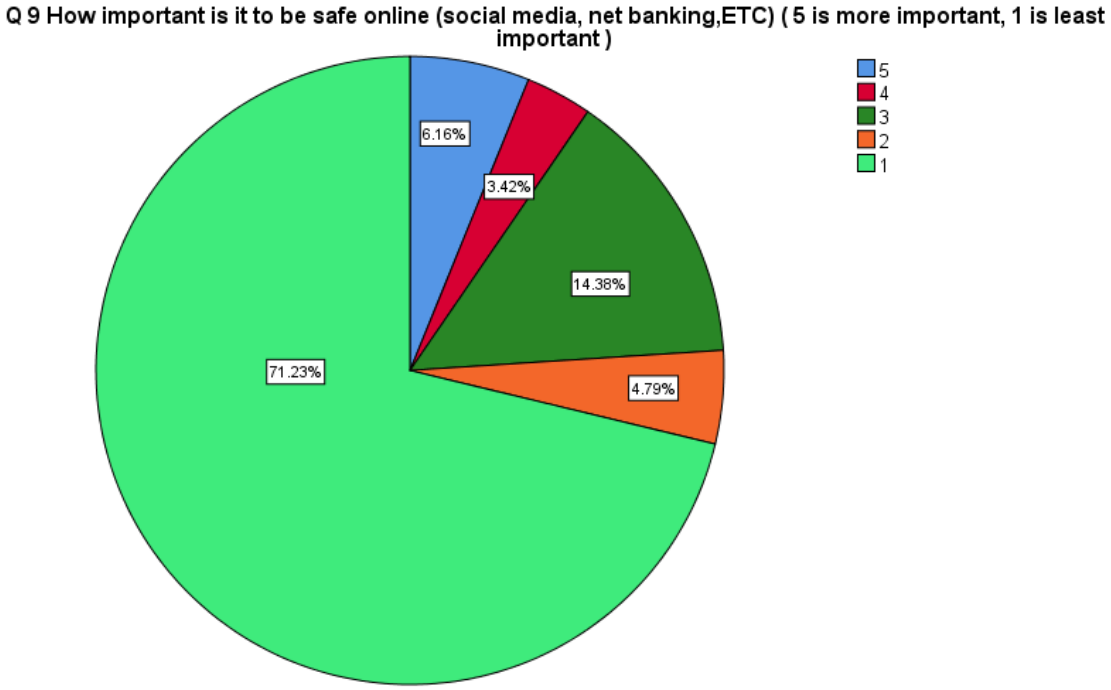


Figure 12: Important to be safe online.

Observation: 71% of the respondents said it's very important to be safe online while doing surfing, financial transactions, chatting, posting personal information. Being safe is the most important part as one must be aware of the which website, app, authorized payment partner one he or she is using as this will help to eliminate the risk of getting scammed by the cyber criminals. Being safe while doing online surfing, while surfing on social media one must avoid people they don't know and avoid clicking unnecessary links which will ultimately take you to some scammer.

10. Respondents were asked about the cyber security measures taken by the financial institution are enough to tackle the cyber-crime in Mumbai. And the answer was evident from the respondents that 66% i.e., 97 respondents felt that it is not enough to tackle the cyber-crimes as seen in figure 13.

Statistics

Q10 Are cyber security measures taken by financial institutions are enough to tackle cyber crime in Mumbai

N	Valid	146
	Missing	0

Q10 Are cyber security measures taken by financial institutions are enough to tackle cyber-crime in Mumbai

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	49	33.6	33.6	33.6
	No	97	66.4	66.4	100.0
	Total	146	100.0	100.0	

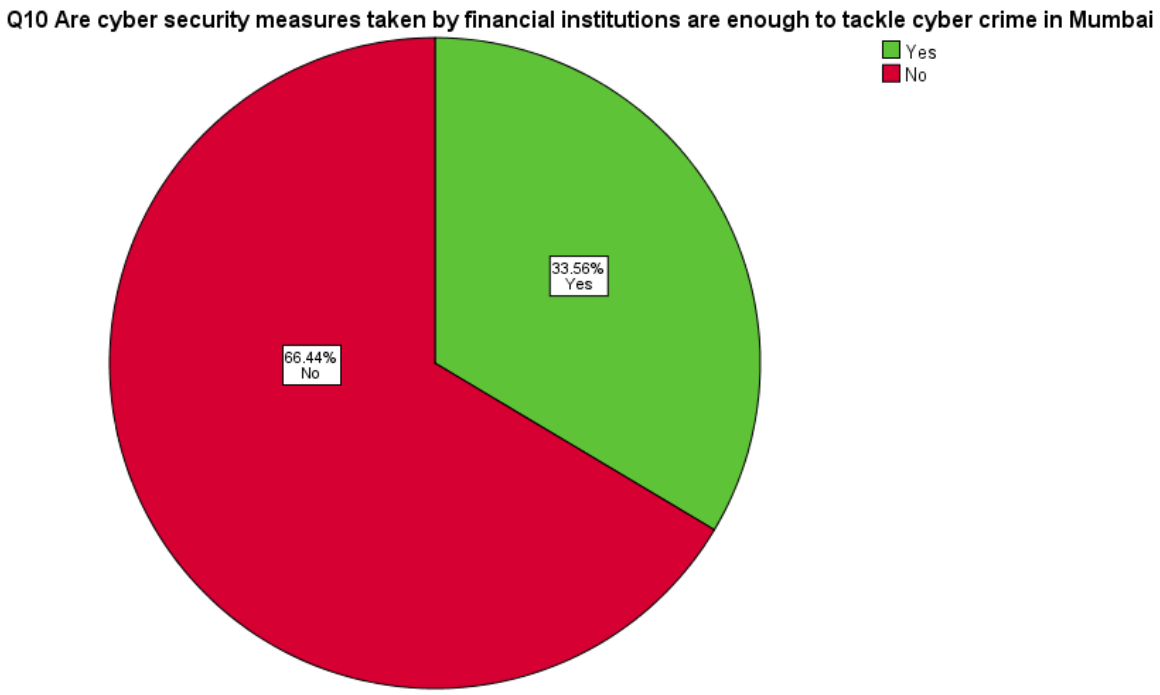


Figure 13: Cyber security measures taken by the financial institutions.

Observation: The respondents agreed to that cyber security mechanism adopted by financial institutions are not capable to cater cyber-crime related problems. 66% i.e., 97 respondents felt that it is not enough to tackle the cyber-crimes as seen in figure 13. Cyber security measures are available on relevant websites, apps as suggested by the cyber experts and on the other hand financial sector respondents agreed that the current methods adopted by financial sector is not capable to cater cyber-crimes. In the true sense methods are to be improved as suggested by the cyber experts and current methods are there to make life easier of the individuals who are using the relevant cyber security methods such as making of passwords, OTP and other aspects of security measures, it's the individual who lacks the awareness as how to perform a particular function or set a difficult password.

11. Respondents were asked about cyber laws should they be amended as per the situation in the financial sector. 92% of the respondents agreed to that it should be amended as early as possible and should be made more deterrent towards cyber criminals as seen in figure 14.

Statistics

Q 11 Should cyber laws be amended as per the situation in the financial sector and make it more deterrent towards cybercriminals

N	Valid	146
	Missing	0

Q 11 Should cyber laws be amended as per the situation in the financial sector and make it more deterrent towards cybercriminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	135	92.5	92.5	92.5
	No	11	7.5	7.5	100.0
	Total	146	100.0	100.0	

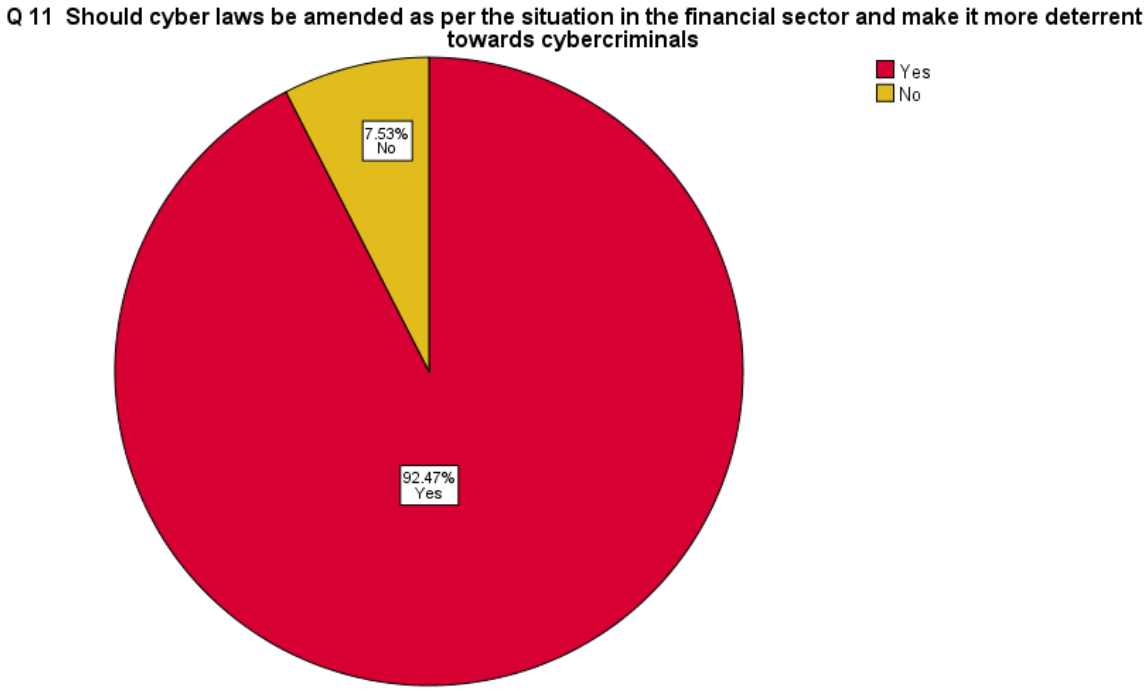


Figure 14: Cyber law should be amended as per situation in the financial sector

Observation: 92% of the of respondents said yes that cyber law of the country should be amended as early as possible and should be made more deterrent towards cyber criminals. As pointed by the researcher it's the need of the hour to amend the IT act as early as possible so that it might reduce the cyber crime to a great extent. And cross borders crimes which are committed by hackers' can be stopped as due action can be taken against them.

12. The respondents were asked about the cyber-crime and cyber security in the financial sector as these two should be given priority. 98% i.e., 144 respondents agreed that it should be taken into priority by the legislature as seen in figure 15.

Q 12 Cyber-crime and cyber security in financial sector should be taken into priority by the legislature

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	144	98.6	98.6	98.6
	Disagree	2	1.4	1.4	100.0

Total	146	100.0	100.0	

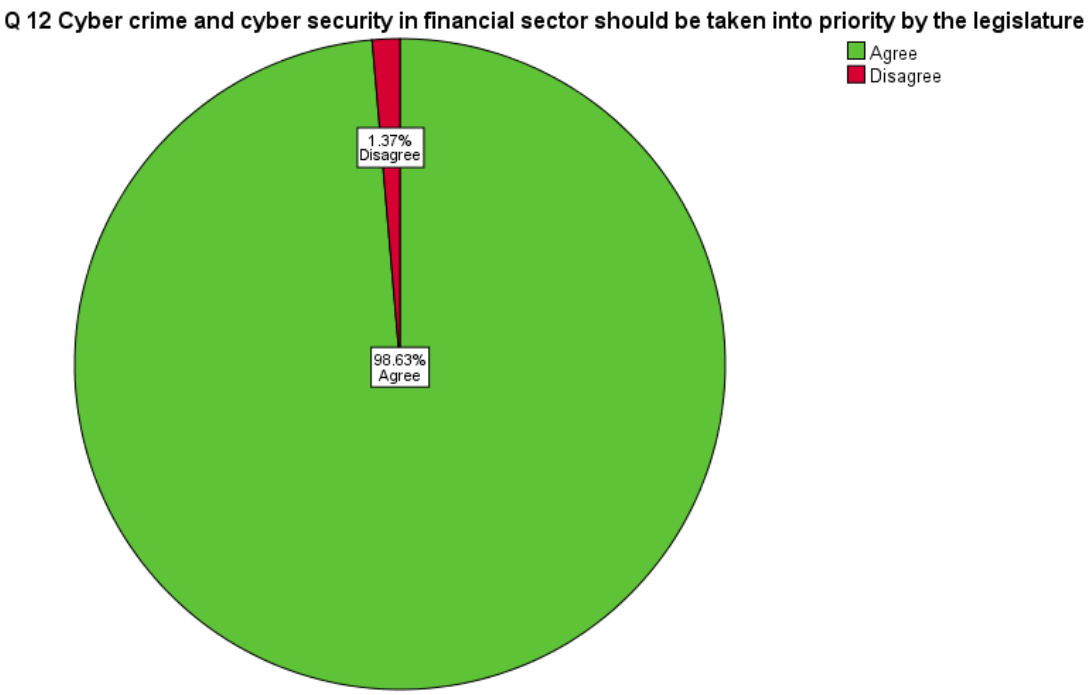


Figure 16: Cyber-crime and cyber security should be given priority

Observation: The respondents agreed that due importance should be given to the cyber-crime and cyber security 98% of the respondents said yes that, cyber security and cyber-crime should be given due importance by the legislative body of the country. Cyber-crime as suggested by the researcher will be a trillion-dollar economy in the coming years. And Indian legislature should immediately come up with relevant amendments in relation to cyber security in the financial sector this will help to control the cyber-crime and reduce the crimes committed on daily basis. Taking example from developed countries separate cyber security law should be introduced.

7.3.2 LAW FACULTIES OBERSERVATIONS

Responses from law faculties were also taken in order understand the current situation of Information Technology Act 2000 and what all changes are required in the act, how full proof the critical infrastructure of the country is, law faculties were from the age group of 18 to 51+ and variety of question were asked to the faculties regarding cyber security, critical

infrastructure, new law for the protection of individuals, does information technology act all aspects of cyber security. Do we require a separate act for cyber security to stop cyber-crime in the present situation? Does critical infrastructure is protected by the IT act 2000 and lastly suggestion was taken from the law faculties. We received 45 responses out of 50 of law faculties from Mumbai and its nearby areas. These responses will give a clear picture regarding the IT act and other aspects of cyber-crimes in Mumbai.

A. The total responses from law faculties was 45 out of 50 in which most of the faculties belonged to the age group of 25-34 that amounted to 69% of the total responses and 3 respondents were in the bracket of 45-50 years of age and one faculty was 50 plus. The age factor and knowledge relating to the law and what is required for the act and for the society can be calculated through this as seen in figure 1.

Statistics

Age of the Respondent

N	Valid	45
	Missing	0

Age of the Respondent

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	4	8.9	8.9	8.9
	25-34	31	68.9	68.9	77.8
	35-45	6	13.3	13.3	91.1
	45-50	3	6.7	6.7	97.8
	51+	1	2.2	2.2	100.0
	Total	45	100.0	100.0	

Figure 1: Ages of the respondent

B. The gender of the respondents of the law faculties amounted to 55% i.e., 25 where female's faculties and 19 where male faculties as seen in figure 2.

Statistics

Gender

N	Valid	45

	Missing	0

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	19	42.2	42.2	42.2
	Female	25	55.6	55.6	97.8
	Prefer not to say	1	2.2	2.2	100.0
	Total	45	100.0	100.0	

Figure 2: Gender of the respondents

1. The law faculties where familiar to the cyber laws as asked in the questionnaire for the research. 86% i.e., 39 of the respondents were aware of the cyber laws and this will help the researcher to ask questions related to cyber laws as seen in the figure 3.

Q 1 Are you conversant with cyber laws

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	39	86.7	86.7	86.7
	No	6	13.3	13.3	100.0
	Total	45	100.0	100.0	

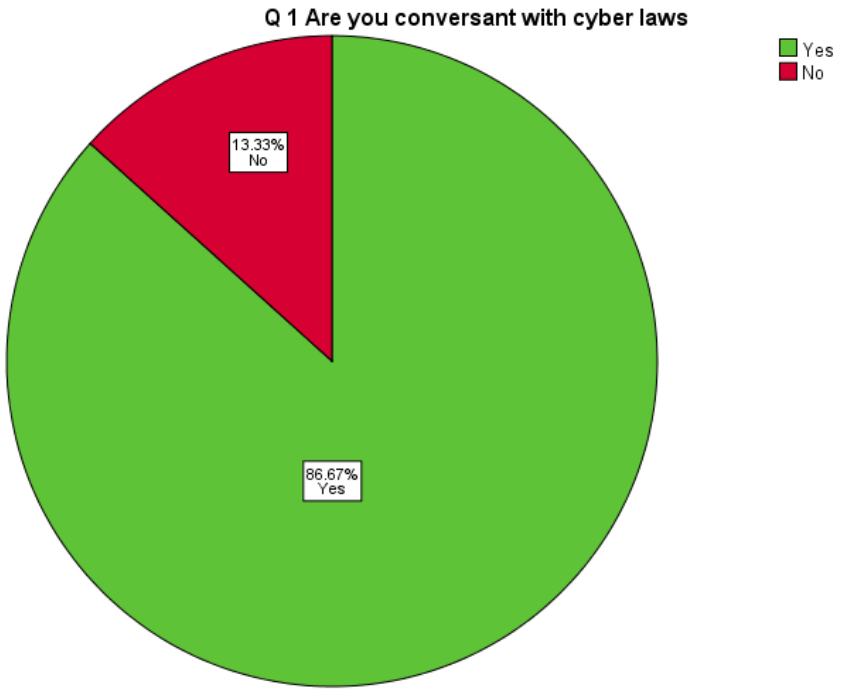


Figure 3: conversant with cyber laws

Observation: The law faculties were conversant with the cyber laws. The law professors of nearby cities such as Mumbai, Navi Mumbai and Thane took part in the questionnaire and they were aware of the cyber laws i.e., The Information Technology Act 2000. The law faculties where conversant with the cyber law as it was very important that Information technology act being a law which is generally is not that much conversant among professionals as this law is not used on daily basis in the functioning of court. As admitted by the advocates it is something which is something new in the practice as compared to the traditional practice of law in the courts. The law faculties awareness towards the cyber law is good factor for the development of the Information Technology act as they know that the punishment mentioned in the IT act doesn't pose that much threat to the cyber criminals and amendment is required as early as possible in the act.

2. The law faculties were asked about that, is the current information technology act 2000 is sufficient to curb cyber-crime in India. 91% i.e., 41 respondents agreed that current Information Technology act is not sufficient to curb cyber-crime in India as seen in figure 4.

Q 2 Is the Current Information Technology Act 2000 is Sufficient to Curb cyber-crime in India

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	4	8.9	8.9	8.9
	No	41	91.1	91.1	100.0
	Total	45	100.0	100.0	

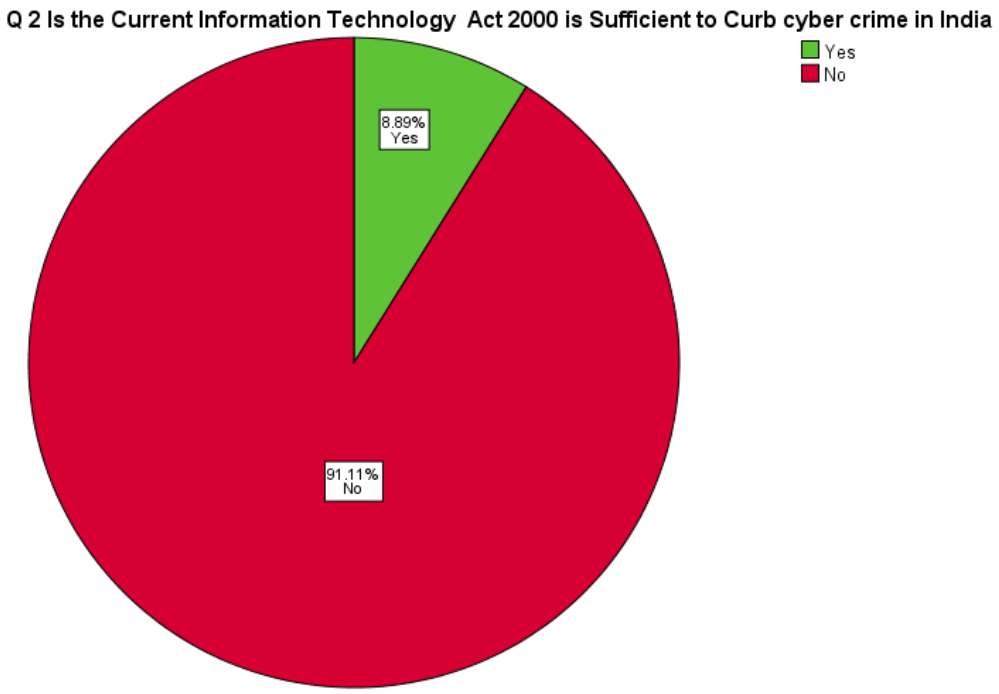


Figure 4: Current IT act 2000 is sufficient or not to curb cyber-crime in India

Observation: The law faculties agreed that current IT act is not sufficient to curb cyber-crime in India. 91% i.e., 41 respondents agreed that current Information Technology act is not sufficient to curb cyber-crime in India. The Information Technology act 2000 and its various amendments are not sufficient to curb the cyber-crime. As pointed out by the experts having law in one place and awareness on the other, it's the awareness which plays a important role to stop the cyber-crime. Information Technology act is becoming redundant as technology is improving day by day and cyber criminals have an upper hand as compared to the citizens who are just having basic awareness of cyber-crime. Current IT act and what changes should be brought by the legislature should be taken into consideration by the relevant authorities on immediate basis.

3. Law faculties were asked about whether more amendments are required in the Information Technology act 2000. The response received was evident as 93% i.e., 42 of the faculties said that more amendments are required in the current situation as can be seen in the figure 5.

Q 3 Information Technology act 2000 requires more amendments relating to cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	42	93.3	93.3	93.3
	No	3	6.7	6.7	100.0
	Total	45	100.0	100.0	

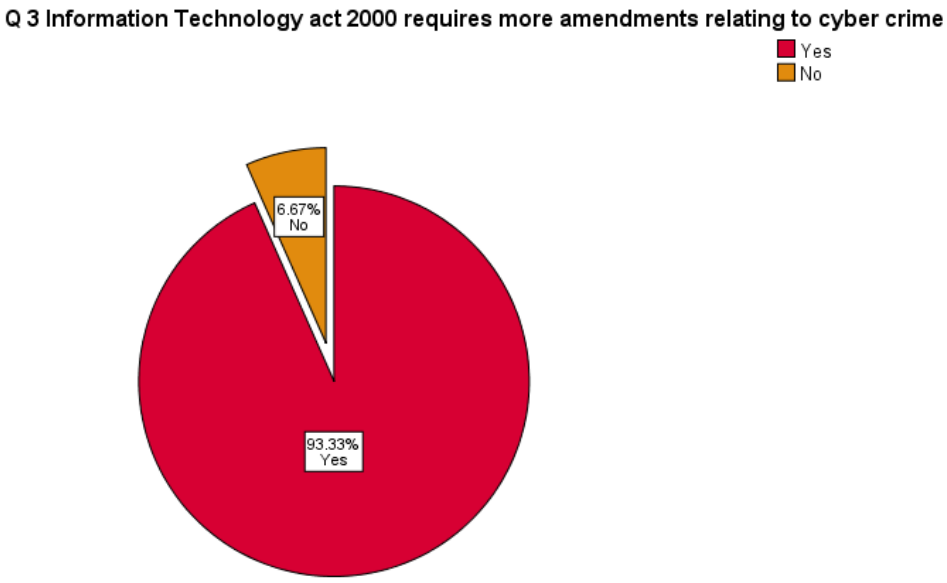


Figure 5: More amendments required in the IT act 2000

Observation: The law faculties agreed that more amendments are required in the IT act 2000 as its not sufficient to curb cyber-crime in India ,93% i.e., 42 of the faculties' said amendments are required. Cyber experts pointed out that amendments are required, same was suggested by the law faculties. As the change will help to curb cyber-crime and impose severe punishment on the cyber criminals this will create a deterrent effect in the minds of the cyber criminals. Penalties should be increased on third party organisations and they should be made liable for any data breach or mishandling of information. Amendments will help, as they should be made in consonance with technologies and methods used by the cyber criminals as they have upper hand in relation technology and cyber crime methods adopted by them this will reduce the crime to some extent.

4. The law faculties were asked about what is cyber security under Information Technology act 2000. And most of the faculties knew as 80% i.e., 36 respondents knew what is cyber security is as seen in the figure 6.

Q 4 Are you aware what is cyber security under Information Technology act 2000

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	36	80.0	80.0	80.0
	No	9	20.0	20.0	100.0
	Total	45	100.0	100.0	

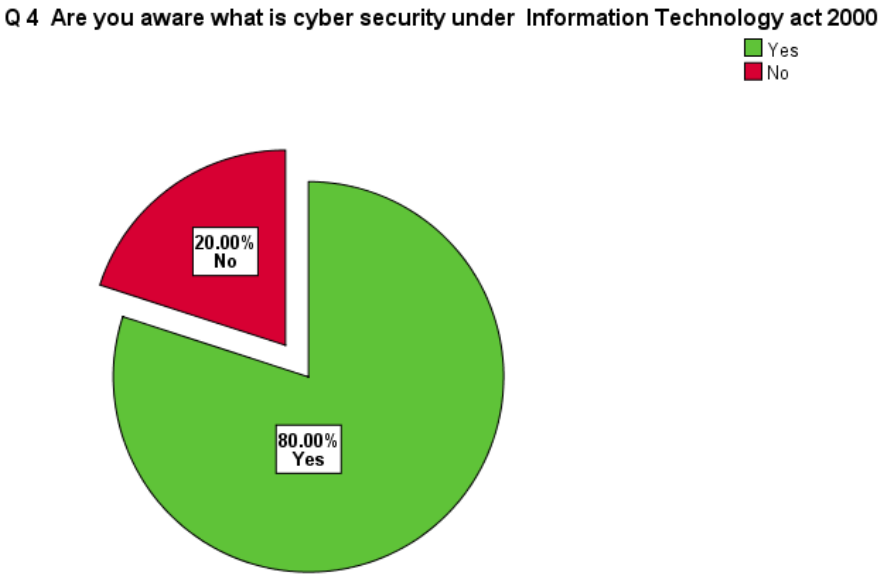


Figure 6: Awareness about cyber security under IT act 2000

Observation: The law faculties said that they are aware of cyber security under information Technology as its very important, but this is not the case as suggested by the financial sector respondents, they said citizens are not aware of cyber security and its importance. Cyber security measures are there as suggested by the cyber experts and on the other hand financial sector respondents agreed that the current methods adopted by financial sector is not capable to cater cyber-crimes. In the true sense methods are to be improved as suggested by the cyber experts and current methods are there to make life easier of the individuals using the relevant

cyber security methods, it's the individual who lacks the awareness as how to perform a particular function or set a difficult password.

5. The law faculties were asked about whether IT act 2000 covers every of cyber security. In that 88.9% i.e., 40 respondents said that it doesn't cover all aspects of cyber security as this could be seen in the figure 7.

Q 5 Does Information Technology act 2000 covers each aspect of cyber security

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	5	11.1	11.1	11.1
	No	40	88.9	88.9	100.0
	Total	45	100.0	100.0	

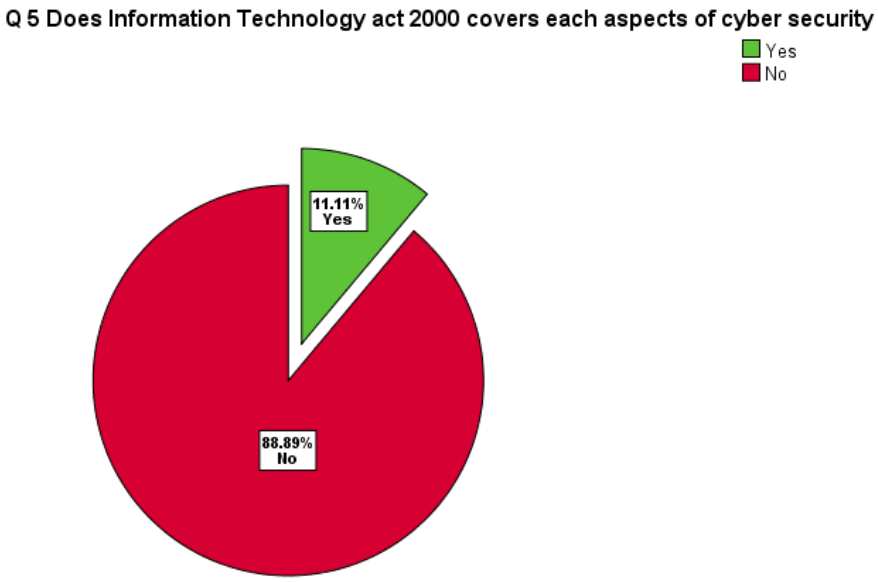


Figure 7: IT act 2000 covers all aspects of cyber security

Observation: The law faculties agreed that Information Technology does not cover each aspect of cyber security. The cyber security is the key to curb the cyber-crime in the coming future. And as suggested by the law faculties it does not cover the aspects of cyber security. Cyber security in relation to the financial sector is most important as it will help to reduce the cyber-crime, a separate act in the line of cyber security will be more efficient as compared to just

adding few provisions in the act. Cyber security mechanism should be improved and awareness drive should be made among citizens.

6. The law faculties were asked about whether IT act 2000 requires changes in the cyber security laws and a separate cyber security act should be introduced to curb cyber-crime. The respondents answered in saying yes a separate act is required 84% of the respondents said that we require change and separate cyber security act is required as seen in the figure 8.

Q 6 Does Information Technology act 2000 requires changes in the cyber security laws and a separate cyber security act should be introduced to curb cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	38	84.4	84.4	84.4
	No	7	15.6	15.6	100.0
	Total	45	100.0	100.0	

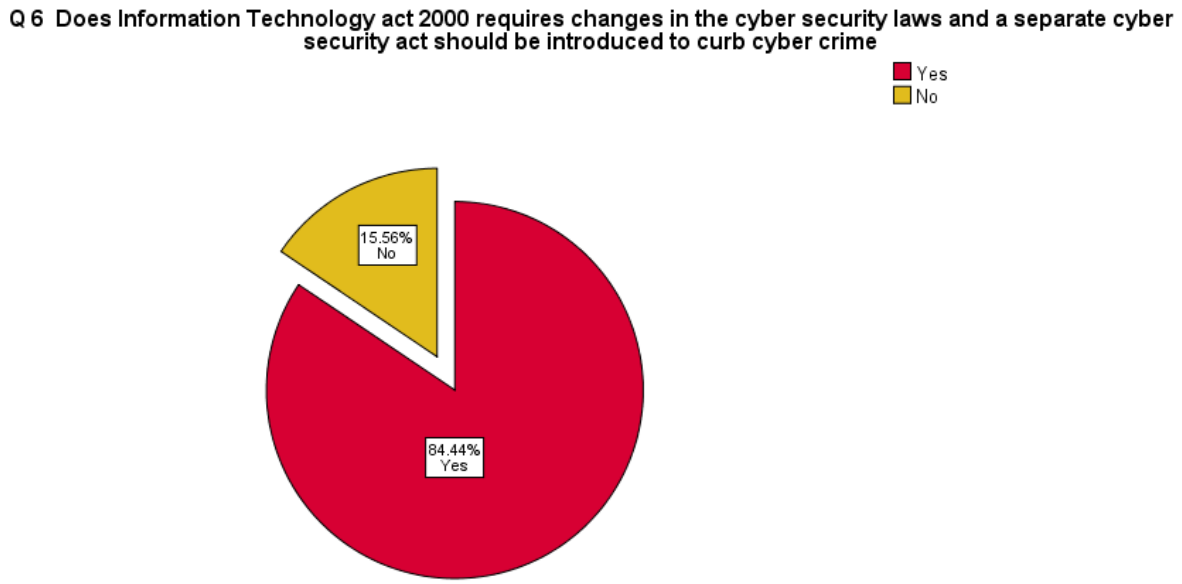


Figure 8: Changes in IT act 2000 and new cyber security act is required.

Observation: The law faculties agreed that there is requirement for new cyber security act, The respondents answered in saying yes, a separate act is required 84% of the respondents said that we require change and separate cyber security act is required. Cyber security act is need of the hour and we should move forward with a separate cyber security act. One of the major reason for having two separate acts is that more efficient application of each act can be made we can take the example of corporate laws such as Insolvency and bankruptcy code act in the lines of companies act we can have Information technology act similarly cyber security act as adopted by the USA.

7. Faculties were asked about what is critical infrastructure under cyber-crime. 66% i.e., 30 respondents were not aware of what is critical infrastructure and 33% were aware of critical infrastructure as seen in the figure 9. The most volatile and important part of the of the system in the county unheard by many.

Q 7 Are you aware of what is critical infrastructure under cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	15	33.3	33.3	33.3
	No	30	66.7	66.7	100.0
	Total	45	100.0	100.0	

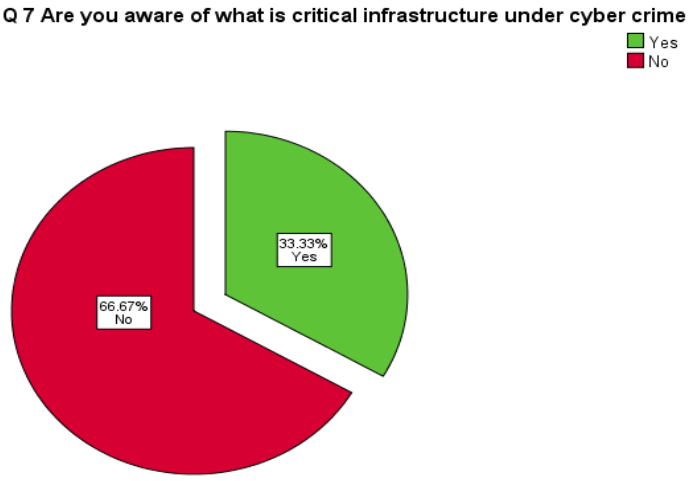


Figure 9: Critical infrastructure under cyber crime

Observation: The critical infrastructure is one of the most important aspect of the country security and most of the faculties failed to recognize that what is critical infrastructure. Critical infrastructure, the heart of any country is to be protected from the cyber criminals at any cost. And due importance should be given to the CI in the Information Technology act as it will play a major role in the coming years.

8. Questions related to critical infrastructure was asked and in that only 77% i.e., 35 respondents were actually aware of what is critical infrastructure as seen in figure 10.

Q 8 Critical Infrastructure under cyber-crime includes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nuclear stations	1	2.2	2.2	2.2
	Electrical grids	7	15.6	15.6	17.8
	Defense equipments	2	4.4	4.4	22.2
	All of the above	35	77.8	77.8	100.0
	Total	45	100.0	100.0	

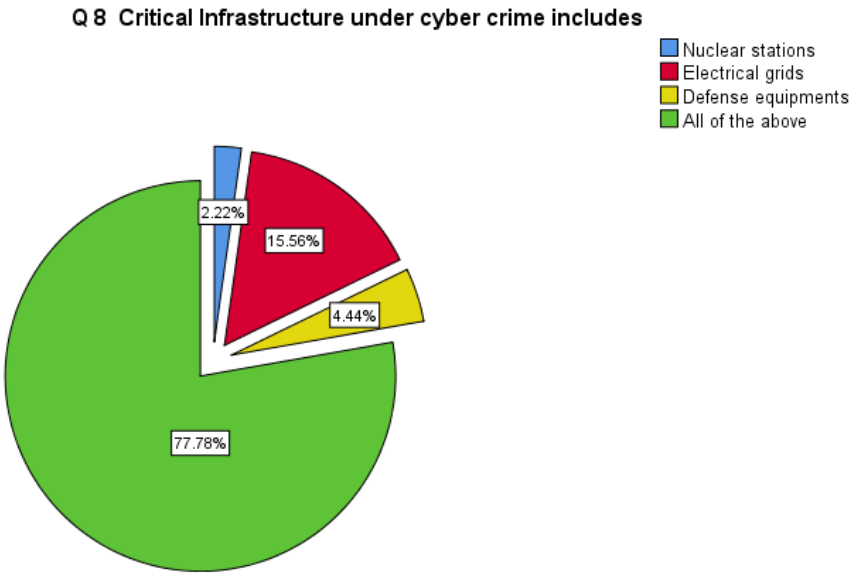


Figure 10: Critical infrastructure under cyber-crime.

Observation: The critical infrastructure one of the most important aspect of the country securities and most of the faculties failed to recognize that what all is covered in the critical infrastructure. It was a mixed response from the law faculties as 77% were aware of what is CI and others fail to recognize what is critical infrastructure this shows that still there is scope for awareness among the citizens. And why its importance to protect the critical infrastructure. The defence, the electrical grids, the stock exchanges, nuclear stations should be protected at any cost, if any cyber-attack happens on this infrastructure, it can cripple the whole country. Few examples cyber-attack on the national Stock Exchange, Mumbai, Cyber-attack on Indian Oil.

9. The law faculties were asked about critical infrastructure and does IT act 2000 covers all aspects of it. The respondents answered correctly as 66% i.e., 30 respondents said it doesn't cover all aspects of critical infrastructure which is most important as per rising cyber-crimes as this could be seen in figure 11.

Q 9 Does Information Technology Act 2000 covers all aspects of critical Infrastructure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	15	33.3	33.3	33.3
	No	30	66.7	66.7	100.0
	Total	45	100.0	100.0	

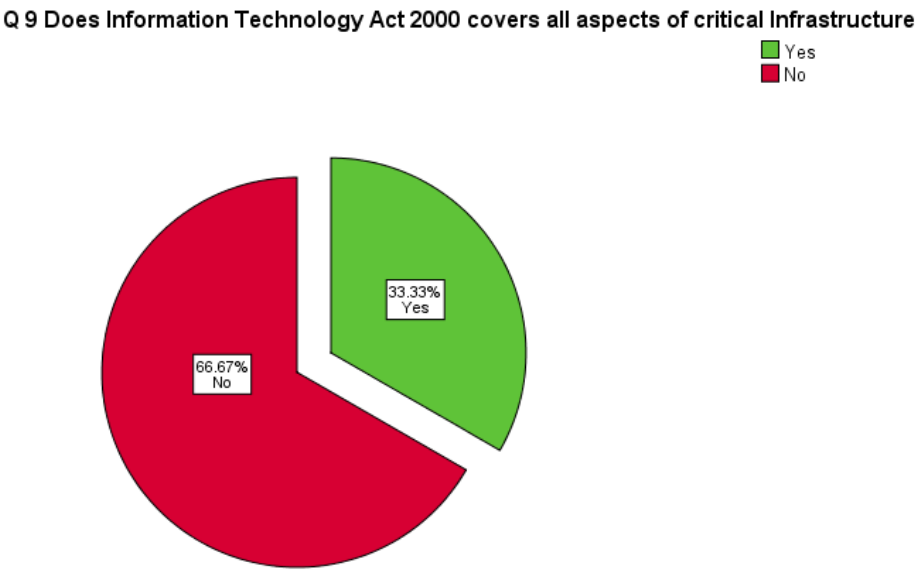


Figure 11: Aspects of critical infrastructure.

Observation: The law faculties agreed that current IT Act 2000 does not cover all aspects of critical infrastructure. 66% i.e., 30 respondents said it doesn't cover all aspects of critical infrastructure. As pointed out by the law faculties IT act does not cover the important parts of the critical infrastructure. There is scope for improvement in the act in relation to the critical infrastructure.

10. The most important question asked to the law faculties was do they feel a separate act is required to protect the critical infrastructure from cyber-crimes. 73% i.e., 33 respondents said that we need a separate act for the critical infrastructure to protect the critical infrastructure of our country as can been in figure 12.

Q 10 Do You feel a separate act is required to protect the critical infrastructure from cyber crimes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	33	73.3	73.3	73.3
	No	12	26.7	26.7	100.0

Total	45	100.0	100.0	

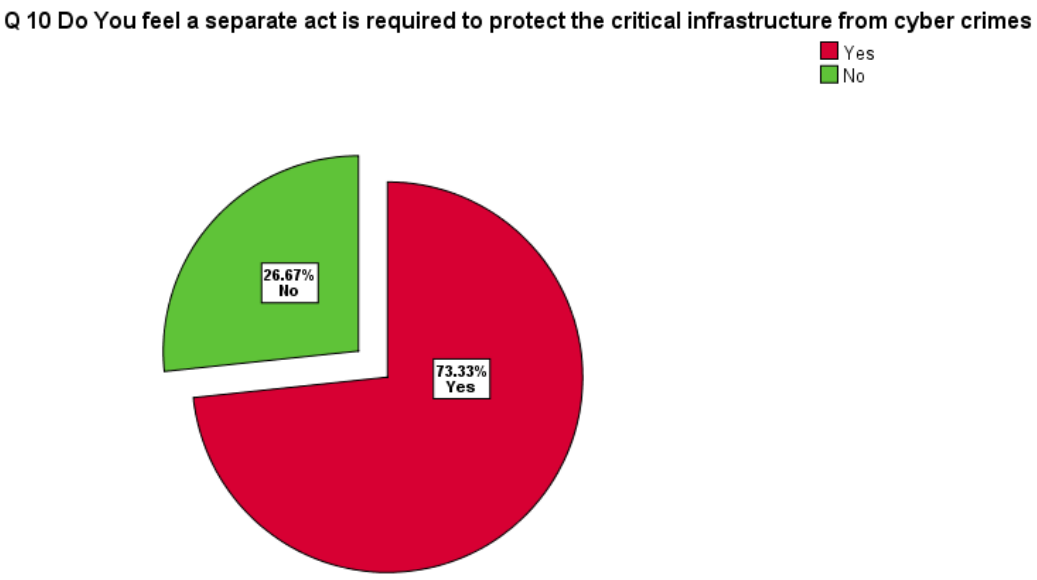


Figure 12: Separate act for critical infrastructure.

Observation: The law faculties agreed that, separate act is required to protect the critical infrastructure of the country through cyber criminals. 73% i.e., 33 respondents said that we need a separate act for the critical infrastructure to protect the critical infrastructure. It's the most important part, a separate act is the need of the hour in relation to the critical infrastructure as it will reduce the burden on the information technology and separate act will only focus on the critical infrastructure and its relevant bodies. As we have seen there has been attack on dams in the USA and gas pipelines by cyber criminals and India can be the target of the cyber criminals in the near future.

7.3.3 LAWYER'S OBSERVATIONS

The researcher made questionnaire for the advocates to know about what all changes are required in the current scenario and about Information Technology act 2000. Variety of questions were asked to advocates such as does Practicing Advocates have Awareness regarding cyber security & data protection, are there enough cyber lawyers currently in

Mumbai, is Cyber law practice a new practice altogether for the litigating lawyers in Mumbai, the police officials generally lack knowledge regarding the cyber laws, and how Information Technology act 2000 sections to be applied while framing charges against the accused, questions relating judicial infrastructure were also asked. The responses received from the advocated gave a clear picture about the cyber law and its practise in Mumbai and what are the difficulties faced by the lawyers while practising the law in Mumbai.

A. The advocates were from the age group of 18 to 51+, 55% i.e., 30 of the respondents belonged to the age group of 25-34 which is most important in relation to the responses as they are practising advocate and having knowledge of courts and 2 respondents where from the age group of 51+ as seen in the figure 1.

Statistics

Age of the Respondents

N	Valid	54
	Missing	0

Age of the Respondents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	9	16.7	16.7	16.7
	25-34	30	55.6	55.6	72.2
	35-45	12	22.2	22.2	94.4
	45-50	1	1.9	1.9	96.3
	51+	2	3.7	3.7	100.0
	Total	54	100.0	100.0	

Figure 1: Age

B. The Advocate respondents were majorly male as 77.8% i.e., 42 respondents were male and 12 were female as its evident in Mumbai more males are practicing lawyers as compared to women but this doesn’t make any reference in the knowledge and practice of the advocate’s as seen in the figure 2.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	42	77.8	77.8	77.8
	Female	12	22.2	22.2	100.0
	Total	54	100.0	100.0	

Figure 2: Gender

1. The advocates were asked the question whether they are aware of cybercrime. As evident they were aware of cyber-crime but practicing part is still missing as cyber law practise is something new for the advocates. 92% of the advocates are aware of cyber-crime as seen in the figure 3.

Q 1 Are you aware of cyber crime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	92.6	94.3	94.3
	No	3	5.6	5.7	100.0
	Total	53	98.1	100.0	
Missing	System	1	1.9		
Total		54	100.0		

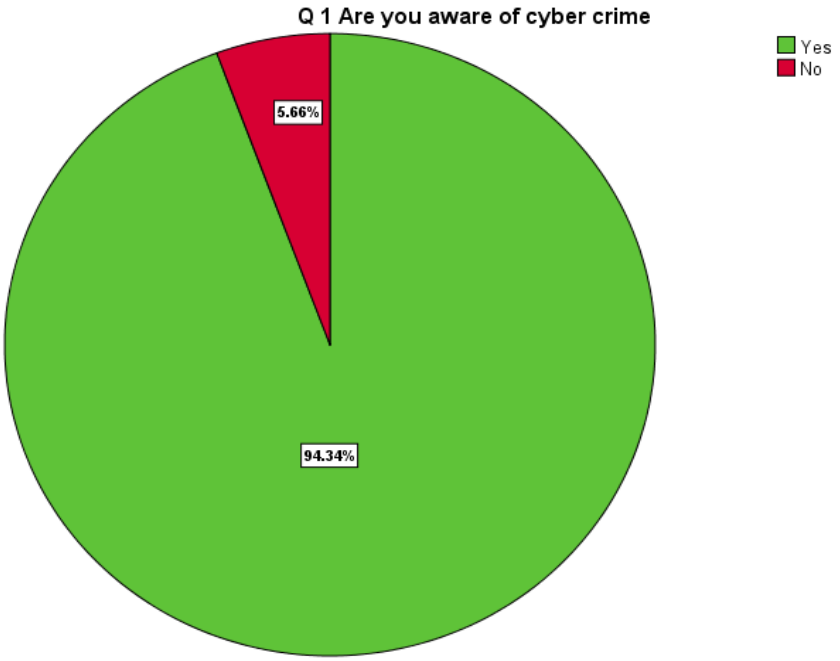


Figure 3: Awareness of cyber-crime.

Observation: 92% of the advocates agreed that they are aware of what is cyber-crime and its nuisances. That is very positive sign in relation of the knowledge relating to cyber criminals and the methods adopted by them. Awareness was there among the lawyer's fraternity but the main aspect in relation to cyber law practice was missing as suggested by the lawyers. Cybercrime and cyber law practice are not going hand in hand, advocates are finding it difficult at present how to deal with cyber related matters. Awareness plus implementation of cyber law in the courts is required to deal with the cyber criminals and take punitive action the culprits which are using the technology to scam innocent people.

2. The advocates were asked about the awareness regarding cyber security and data protection. As 57% i.e., 31 of the respondents knew about the cyber security and data protection and on the same line 42% i.e., 23 respondents are unaware of the cyber security and data protection as seen in the figure 4.

Q 2 Does Practicing Advocates have Awareness regarding cyber security & data protection

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	31	57.4	57.4	57.4
	No	23	42.6	42.6	100.0
	Total	54	100.0	100.0	

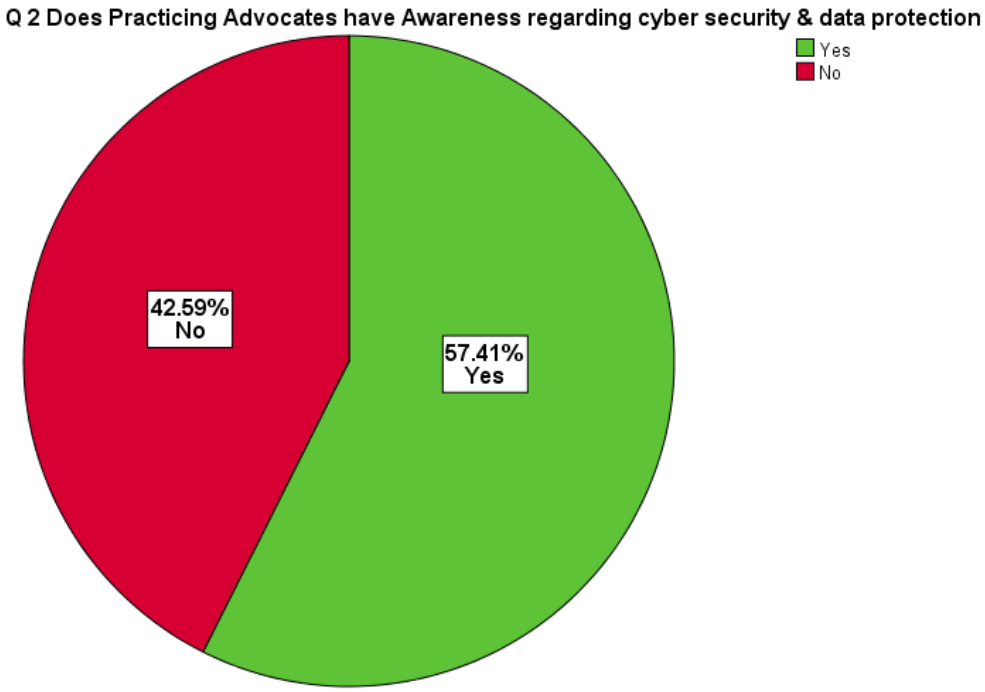


Figure 4: Practicing advocates aware of cyber security and data protection.

Observation: 42% of the practising advocates are unaware regarding cyber security and data protection and 57% of the advocates are aware. The advocates were lacking the information regarding cyber security. But if we see the numbers are not encouraging enough to say that practising advocates are prepared regarding cyber security and data protection issues. As suggested by the cyber expert's technical know-how is the key behind cyber security as, technical knowledge will play an important role in the practice of cyber law matters in Mumbai courts. Cyber experts pointed that judge also should be technologically well versed so that the interpretation could be easier for the parties.

3. The advocates were asked about that is their enough cyber lawyers in Mumbai, 88% said that no there are not enough cyber lawyers in Mumbai as seen in figure 5.

Q 3 Are there enough cyber lawyers currently in Mumbai

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	11.1	11.1	11.1
	No	48	88.9	88.9	100.0
	Total	54	100.0	100.0	

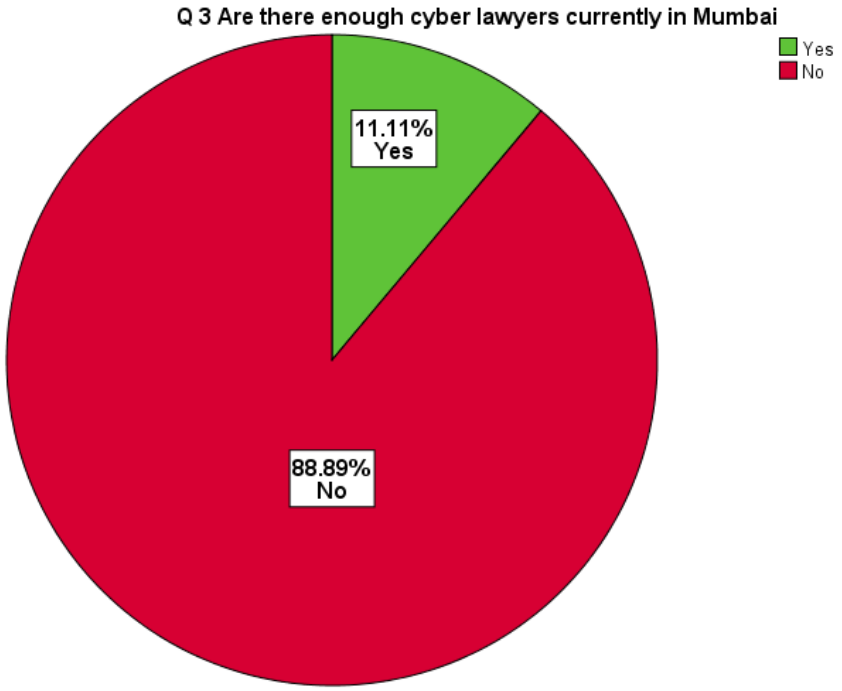


Figure 5: Enough cyber lawyers in Mumbai

Observation: 88% of the advocates agreed that there are not enough cyber lawyers currently in Mumbai. Which is major drawback in relation to trial of cyber criminals. Lack of advocates and especially cyber lawyers are missing. Practicing the civil, criminal, family matters advocates are accustomed, but cyber law practice is something new as agreed by the advocates respondents. At present we need advocates that are well versed with cyber law and other technological aspects to counter the cyber criminals as they are having edge over the citizens who are missing technological know-how.

4. The most important question to the advocates was is cyber law a new practice altogether for the litigating lawyers in Mumbai. And 88.9% i.e., 48 respondents said yes it's a new practice altogether for litigating lawyers as seen in the figure 6.

Q 4 Is Cyber law practice a new practice altogether for the litigating lawyers in Mumbai

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	48	88.9	88.9	88.9
	No	6	11.1	11.1	100.0
	Total	54	100.0	100.0	

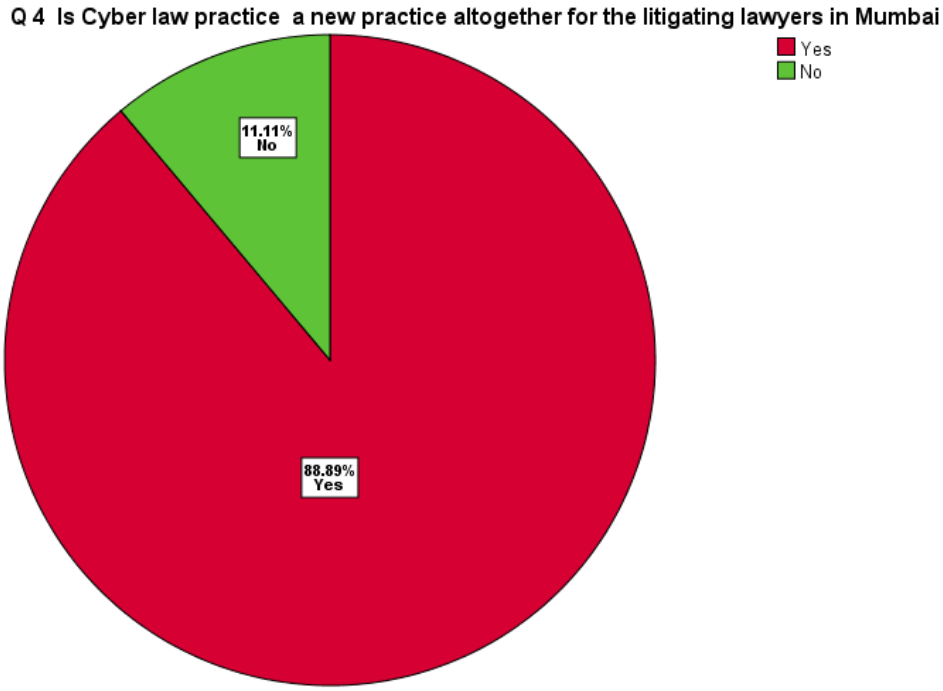


Figure 6: Cyber law practice a new practice altogether for lawyers in Mumbai.

Observation: 88% of the advocates agreed that cyber law practice is something new which advocates are learning on day-to-day basis. The practice in relation to civil, criminal or family matters advocates are used to, but cyber law and its nuisances is something new for the advocates. Cyber law practise as agreed by the advocates is new and emerging practise on the similar stage of IBC laws, minimum 5 years from now is required to develop an infrastructure

that favour the cyber law practise and technicalities which is required for the proper implementation of the law and its practise. The lawyers should be trained according to the development in the technology to keep pace with the cyber criminals.

5. The prosecution and the defense advocates find it difficult to decide matter before presiding judges due to lack of knowledge related to cyber law as its evident 92.6% of the respondents said yes, its very difficult to come to stand due to lack of knowledge as seen in figure 7.

Q 5 The Prosecution and the Defense Advocates find it difficult to decide the matter before presiding judges in Mumbai due lack of knowledge related to cyber law

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	50	92.6	92.6	92.6
	No	4	7.4	7.4	100.0
	Total	54	100.0	100.0	

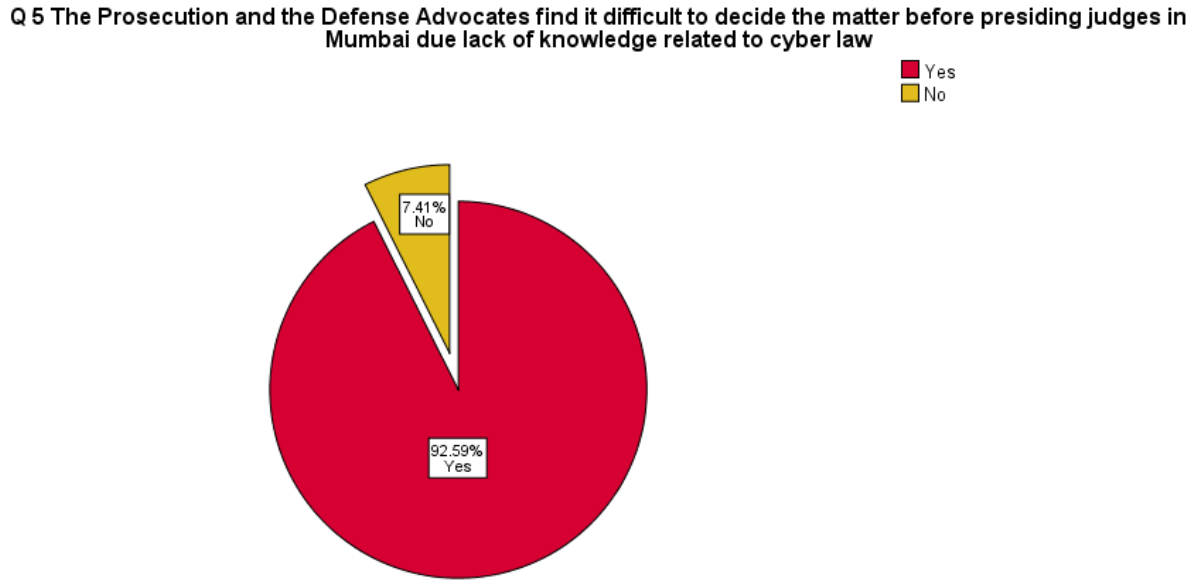


Figure 7: lack of knowledge of advocates and prosecution

Observation: 92.6% of the respondents said yes, its very difficult to come to an concrete decision due to lack of knowledge of cyber law and the judicial officers find it difficult to

conduct the trial. As its evident that cyber law practise being a new practise for the advocates it makes the life of the prosecutor and defense to decide the matter before presiding judges as they lack the relevant knowledge related to cyber law. The knowledge of the parties representing the matter and the judge should be capable to interpret the best possible result for the parties and this will require time as at present 92% of the advocates finds it very difficult to deal with such matters.

6. The police officials lacked know lodged regarding cyber laws and to frame charges against accused. 94% i.e., 51 of the respondents admitted that police official lack required expertise as required to put someone behind bars as seen in the figure 8.

Q 6 The police officials generally lack knowledge regarding the cyber laws, and how Information technology act 2000 sections to be applied while framing charges against the accused

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	51	94.4	94.4	94.4
	No	3	5.6	5.6	100.0
	Total	54	100.0	100.0	

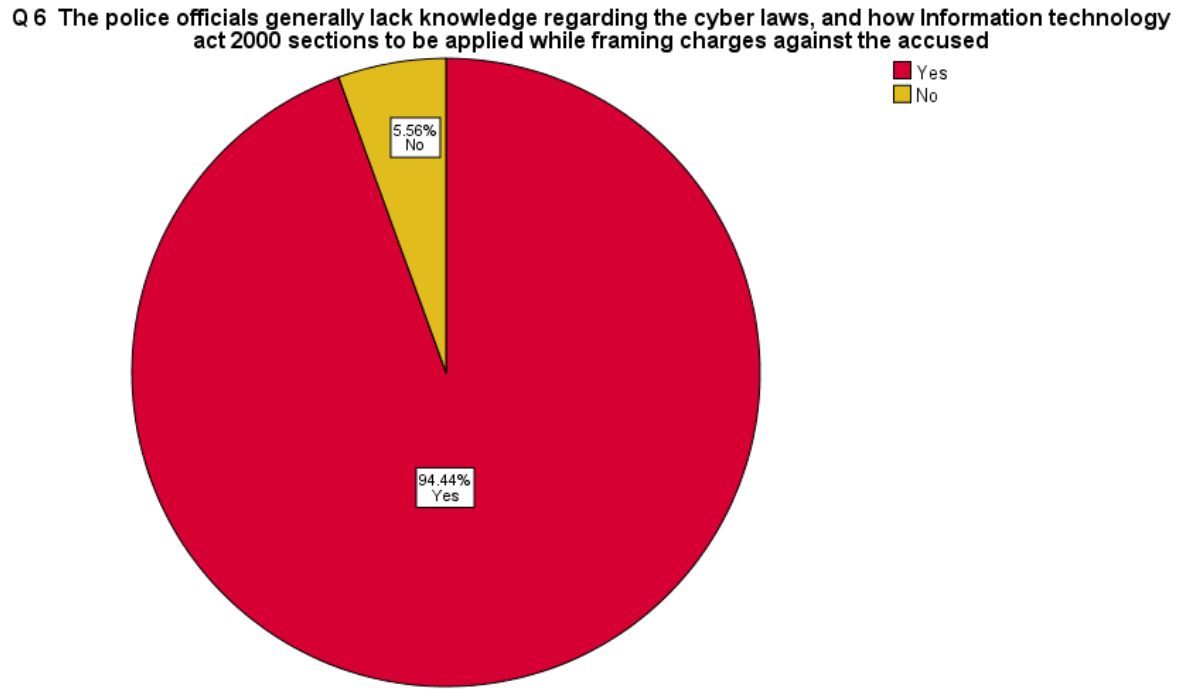


Figure 8: lack of knowledge of police officials.

Observation: The advocates agreed that, police officials lack knowledge in relation how to apply information technology provisions and its application. 94% i.e., 51 of the respondents admitted that police official lack required expertise. After interviewing the police officials, they admitted that, yes police officials lack the relevant knowledge regarding the cyber law and the information technology act 2000. As they don't the provisions and its interpretation what is the procedure behind relevant case.

7. The judicial infrastructure in Mumbai is not prepared to decide cyber related matters due to lack of knowledge as 87% i.e., 47 of the respondents admitted that Mumbai is not having proper infrastructure to cater to cyber related matters as seen in figure 9.

Q 7 The Judicial infrastructure is not prepared for deciding cyber related matters and cyber security matters due to lack of knowledge

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	47	87.0	87.0	87.0
	No	7	13.0	13.0	100.0
	Total	54	100.0	100.0	

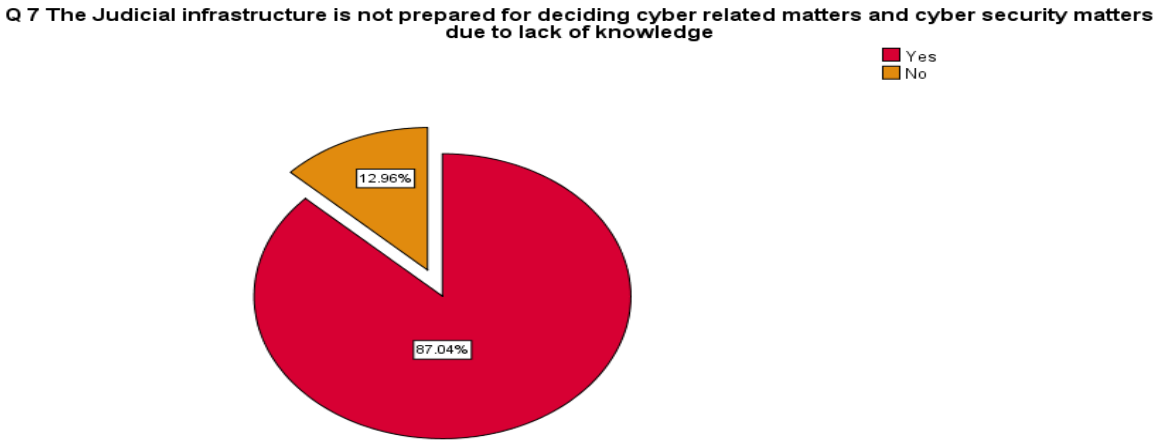


Figure 9: lack of Infrastructure to deal with cyber related matters.

Observation: The advocates agreed that judicial infrastructure is not prepared for deciding cyber related matters and required expertise is missing due to lack of knowledge.87% of the advocates agreed to it. Judicial infrastructure is the key to develop the technological knowledge of the advocates and presiding judges. Proper training to the advocates and sessions should be organised so that they get well versed with day-to-day practise and this was admitted by the advocates as there should be training of the judicial officers on quarterly basis.

8. The litigating lawyers admitted that there should be amendments in the Information Technology Act 2000 for better implementation. 96% i.e., 52 of the respondents agreed to it as seen in the figure 10.

Q 8 Should there be amendments in the present Information technology Act 2000 for better implementation in the litigation part

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	52	96.3	96.3	96.3
	Disagree	2	3.7	3.7	100.0
	Total	54	100.0	100.0	

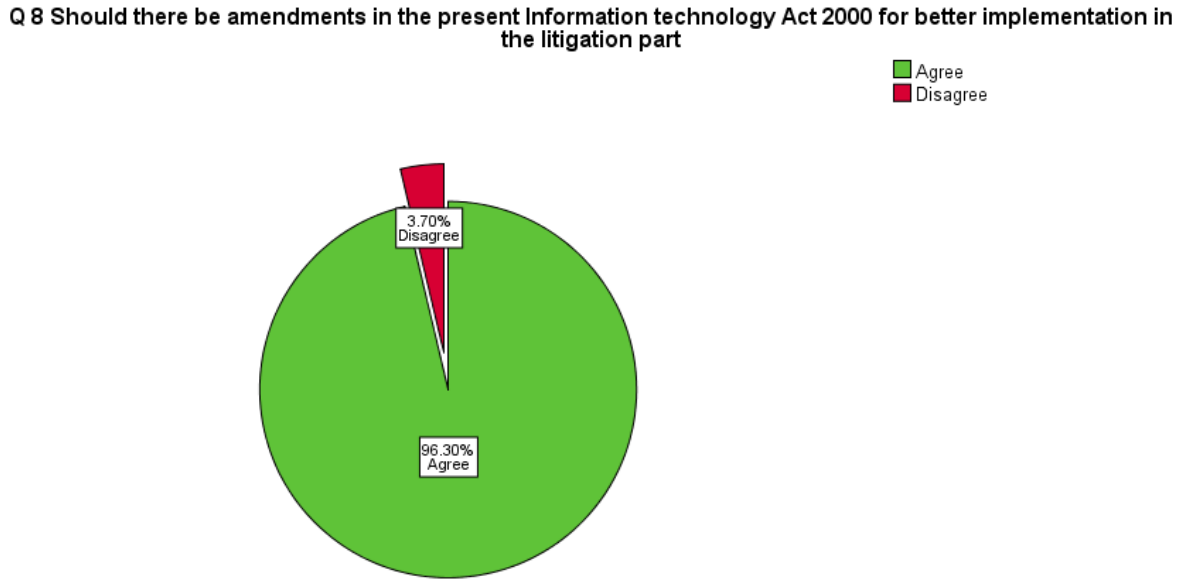


Figure 10: Amendments in the IT act 2000 for better implementation

Observation: 96% of the litigating lawyers admitted that there should be amendments in the Information Technology Act 2000 for better implementation. The general respondents, the law faculties and now the advocates respondents came to the same conclusion, with 96% of the respondents agreeing there is requirement to amend the Information technology act 2000 for better implementation of the cyber laws and have deterrent effect on the cyber criminals.

9. The advocates admitted in the questionnaire that IT act 2000 will play an important role in the coming years to help the judicial body. As 98% of the respondents admitted this as seen in the figure 11.

Q 9 Information technology act 2000 will play an important role in the Coming years to educate cyber law matters in the judicial infrastructure

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	53	98.1	98.1	98.1
	Disagree	1	1.9	1.9	100.0
	Total	54	100.0	100.0	

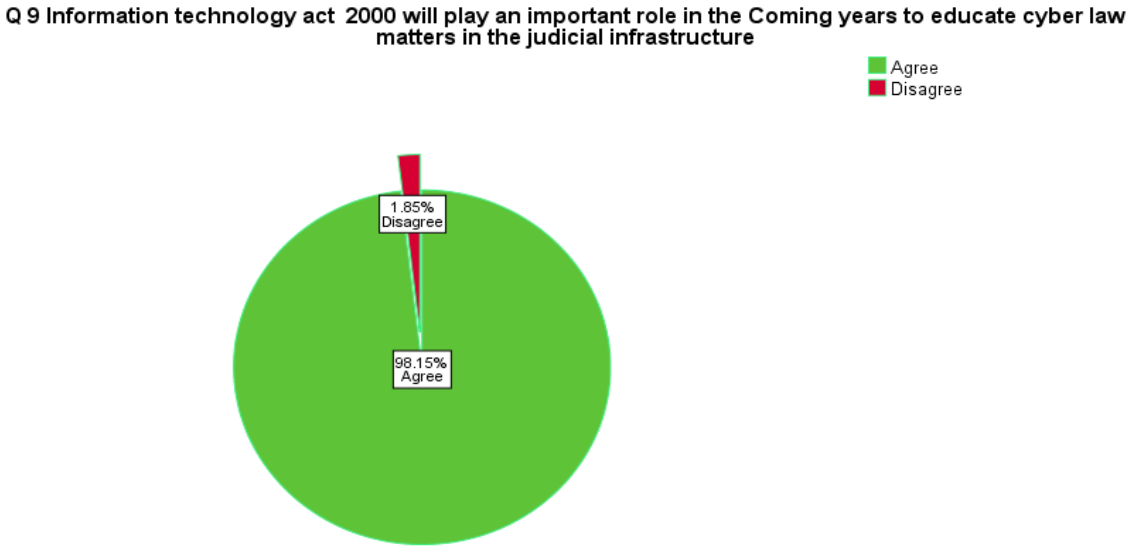


Figure 11: IT act 2000 and its importance in the coming years.

Observation: 98% advocates admitted in the questionnaire that IT act 2000 will play an important role in the coming years to help the judicial body. As admitted by the general respondents, law faculties, advocate also believe that Information technology act will play crucial role in the coming future as cyber-crime will increase in the coming years and will not reduce. Amendments and quick response from the authorities will play a crucial role in the coming years and this can be done by giving due importance to the IT act 2000.

10. Advocates admitted that conferences should be organised for the advocates and make them understand the litigation part of cyber law. 98% of the advocates admitted that as seen in the figure 12.

Q 10 Workshop and Conferences should be organized to help Advocates to understand the importance of Information technology act 2000 and make them understand the litigation part of cyber law

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	53	98.1	98.1	98.1
	Disagree	1	1.9	1.9	100.0
	Total	54	100.0	100.0	

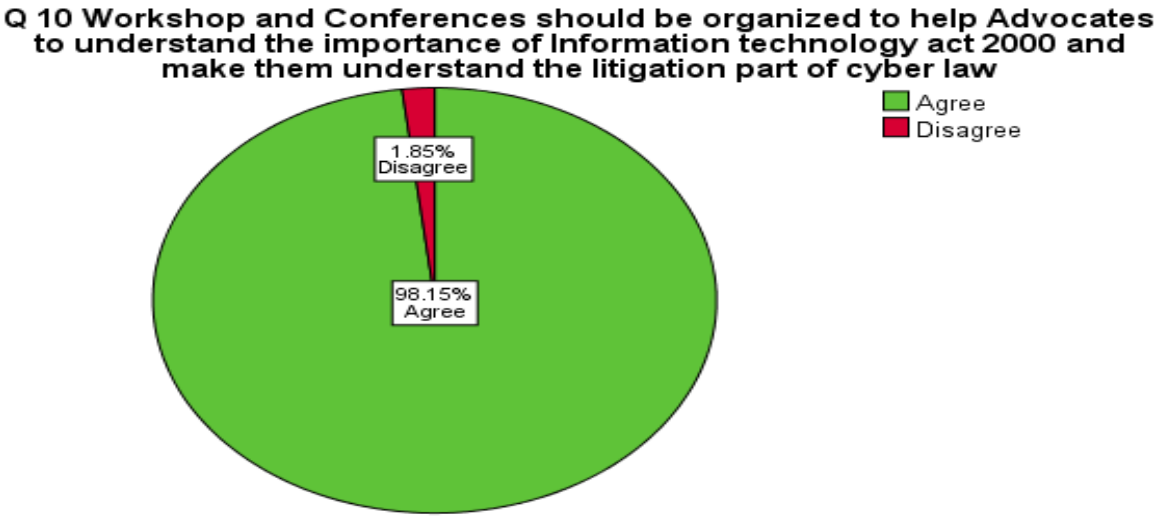


Figure 12: workshop and conferences for the advocates.

Observation: 98% Advocates admitted that conferences should be organised for the advocates and make them understand the litigation part of cyber law. As admitted by the advocates judicial infrastructure will play an important role. Workshop and conferences should be organised to make understand the advocates and judges the importance of IT act 2000 and make them accustom to the litigation part. As this will help the practise a lot easier for the both the parties.

11. The advocates also agreed on the cyber security experts and cyber law practise are required in each state bar council to promote it importance and educated advocates regarding cyber law matters. 100% of the advocates agreed to it as seen in the figure 13.

Q 11 Cyber law practice and cyber security experts are required in each state bar council to promote its importance and to educate advocates regarding cyber law matters

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	54	100.0	100.0	100.0

Figure 13: Promotion of cyber law practice in each bar council

Observation: 100% advocates also agreed on the cyber security experts and cyber law practise are required in each state bar council to promote it importance and educated advocates regarding cyber law matters. The importance of cyber security experts in each state bar council will promote the cyber law practise and educate lawyers to deal with cyber law matters. This process will take time but once the infrastructure is established the practise for the parties will be lot easier. Interpretation and execution will be done at a quick speed.

7.3.4 FINANCIAL SECTOR OBSERVATIONS

The financial sector was also included in the questionnaire and responses were taken from the financial sector employees to know the impact of cyber-crime in the financial sector in Mumbai. Different sector of the financial sector was chosen such as private, public, payments, NBFC, small payments bank. Questions related to KYC fraud, OTP, bar code fraud, link related fraud also is covered in the questionnaire, debit and credit card fraud also covered as most frequent these two are used by cyber criminals. How much percentage of financial fraud gets solved, do customers recognize fake websites related to financial sector, whether the current cyber security infrastructure Sufficient to curb cyber-crime in the financial sector, is the current methods adopted by the financial sector for prevention of cyber-crime is enough to cater to the rising problems of citizens these are the questions asked to the financial sector to reach a conclusion how much impact does the cyber-crimes are having on the financial sector in Mumbai.

1. The total number of responses received were 25 out of 50. Most of the responses came from the public sector banks which amounted to 52% of the total responses 13 and 5 were from the NBFC, and 4 were from the Private sector as seen in figure 1. The responses came from all financial sector as required for the research to know the impact of cyber-crime in the financial sector in Mumbai. The respondents have good amount of experience as 36% i.e., 9 of the respondents had 5-8 years of work experience which is the requirement as they are more experienced and have seen most of the cyber-crimes in their day-to-day life and 7 of the respondents are having 8-10 years of experience as seen in the figure 2.

Statistics

Q 1 In which financial sector do you work

N	Valid	25
	Missing	0

Q 1 In which financial sector do you work

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Private sector	4	16.0	16.0	16.0
	Public sector	13	52.0	52.0	68.0
	NBFC	5	20.0	20.0	88.0
	Small finance Bank	1	4.0	4.0	92.0
	Others	2	8.0	8.0	100.0
	Total	25	100.0	100.0	

Figure 1: Financial sector in Which respondents work.

Q 2 How many years of experience you have in financial sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	0-1	2	8.0	8.0	8.0
	1-3	2	8.0	8.0	16.0
	3-5	5	20.0	20.0	36.0
	5-8	9	36.0	36.0	72.0
	8-10	7	28.0	28.0	100.0
	Total	25	100.0	100.0	

Figure 2: Years of experience of respondents in the financial sector

Observation: The respondents have good amount of experience as 36% i.e., 9 of the respondents had 5-8 years of work experience which is the requirement as they are more experienced and have seen most of the cyber-crimes in their day-to-day life and 7 of the respondents are having 8-10 years of experience.

2. The financial sector respondents were asked about cyber frauds people in day-to-day transactions. OTP and link related fraud amounted to 80% of the transactions of the total. This shows that the most common form of fraud is still the OTP and link related fraud used by the

criminals, credit and debit card fraud amounted to 8% of the cyber-crimes as seen in the figure 3.

Q 3 What kinds of cyber frauds people face in day-to-day transactions

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Credit Card Fraud	1	4.0	4.0	4.0
	Debit Card Fraud	1	4.0	4.0	8.0
	OTP Fraud	10	40.0	40.0	48.0
	Link related Frauds	10	40.0	40.0	88.0
	KYC fraud	3	12.0	12.0	100.0
	Total	25	100.0	100.0	

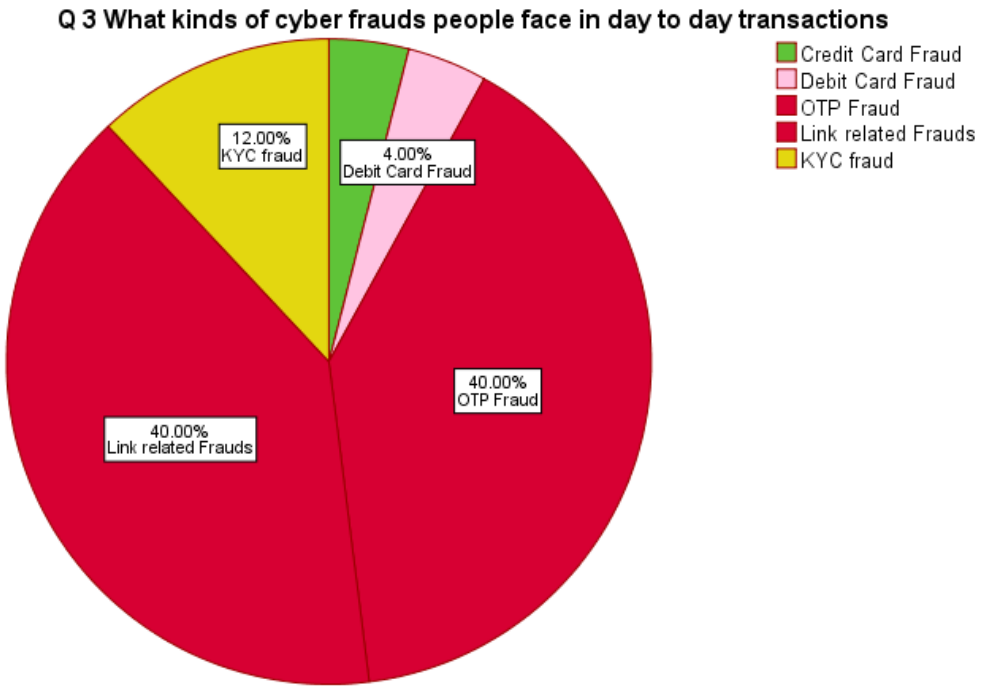


Figure 3: kinds of frauds individuals face on daily basis.

Observation: The financial sector respondents agreed that cyber frauds in day-to-day transactions are more in relation to OTP and link related fraud amounted to 80% of the transactions of the total. Otp fraud the most common and widely used by the cyber criminal's

people tend to give otp to criminals and their amount gets debited. And on the same line it's the link related fraud fraudulent link are sent by the cyber criminals to scam individuals in relation to financial transaction. Criminals make them to install suspicious apps through link then they take away the hard-earned money of an individual.

3. As seen in general the percentage of financial crime gets solved is still at low level. Only 5%-10% i.e on an average of 15 cases gets solved. This shows that still improvement is required as seen in the figure 4.

Q 4 How Much Percentage of financial crime gets solved

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5%-10%	15	60.0	60.0	60.0
	10%-20%	5	20.0	20.0	80.0
	20%-30%	3	12.0	12.0	92.0
	30%-40%	2	8.0	8.0	100.0
	Total	25	100.0	100.0	

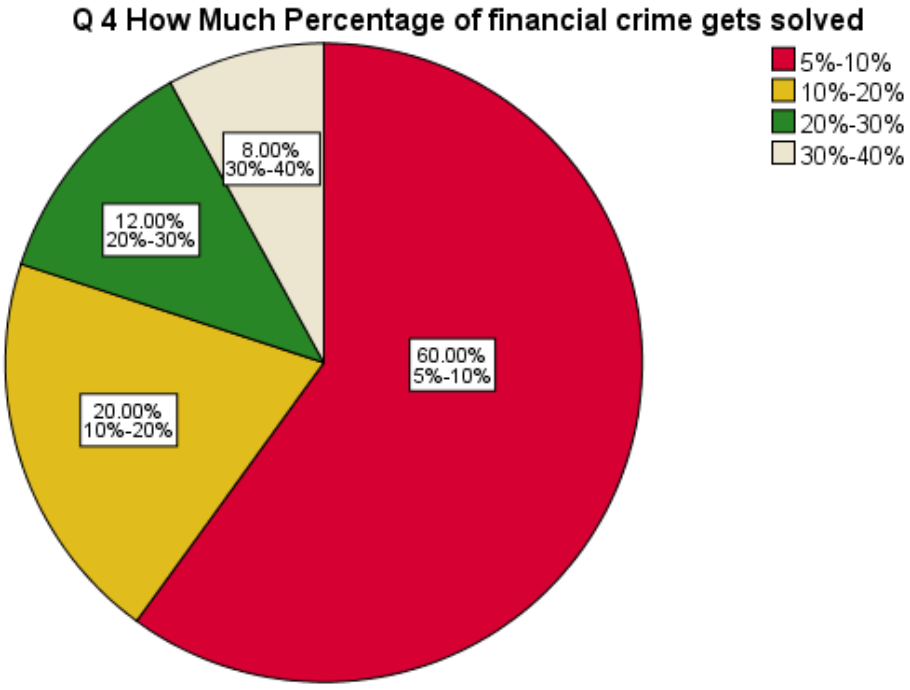


Figure 4: Percentage of financial crime gets solved

Observation: As seen in general the percentage of financial crime getting solved is still at low percentage. Only 5%-10% i.e on an average of 15 cases gets solved. The cyber-crime in relation to financial are not getting solved as admitted by the financial sector respondents. The crime rate is increasing and on the other hand, solving the crime is at tortoise speed. The crime gets committed but never gets solved as admitted by the financial experts. The solve rate of the crimes should be increased as admitted by the police officials they consider the case depending upon the situation and depending on the media coverage.

4. The financial sector respondents were asked about the common cyber threats customers are aware of mostly Phishing, bugging 64% in total of all these common cyber threats as seen in the figure 5.

Q 5 Which are the common cyber threats customers are aware of

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Phishing	8	32.0	32.0	32.0
	Bugging	1	4.0	4.0	36.0
	All of the above	16	64.0	64.0	100.0
	Total	25	100.0	100.0	

Figure 5: Common cyber threats customers aware of

Observation: Phishing and bugging are the most common cyber threats customers are aware. Phising and bugging the most common methods adopted by the cyber criminals in order to scam the citizens and take advantage of them. Bugging and phishing malicious link are sent or email or citizens are lured by sending lottery scam messages.

5. The debit and credit fraud amounted to 40% i.e., 10 frequency which is a shocking number as most of the fraud are related to debit and credit customers usually face as seen in figure 6.

Q 6 How much percent of debit and credit frauds customers usually face

	Frequency	Percent	Valid Percent	Cumulative Percent

Valid	5% -10%	9	36.0	36.0	36.0
	10%-20%	10	40.0	40.0	76.0
	20%-30%	1	4.0	4.0	80.0
	40% and above	5	20.0	20.0	100.0
	Total	25	100.0	100.0	

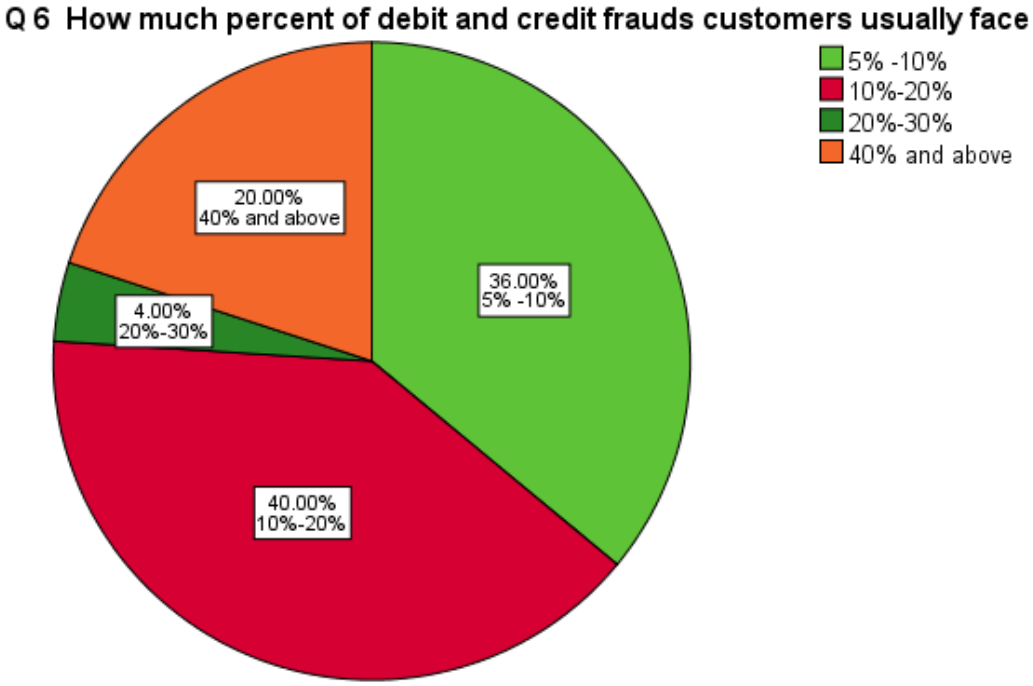


Figure 6: Percent of Debit and credit card frauds customer face.

Observation: The debit and credit fraud amounted to 40% i.e. 10, frequency of debit & credit fraud, which is a shocking number as most of the fraud are related to debit and credit customers usually face. As it's the most common form used by the cyber criminals, they ask for the details of credit or debit and ask for cvv which is most important number in the card and people fall prey to cyber criminals.

6. As admitted by the financial sector authorities' customers do report to the banker, police station as it amounted to 60% of the responses as seen in the figure 7.

Q 7 To whom do customers report cyber fraud incidents

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Banker	6	24.0	24.0	24.0

	Police	4	16.0	16.0	40.0
	All of the above	15	60.0	60.0	100.0
	Total	25	100.0	100.0	

Figure 7: customers report cyber fraud incidents.

Observation: customers do report to the banker, police station as it amounted in total 60% of the financial sector respondents people report to these authorities. As people are not aware of the net banking and official websites of these authorities to complain. System is their to reach the proper authority but lack of knowledge among the individuals, this make the citizens run pillar to pillar.

7. The financial sector questionnaire had this very important of how they deal with financial frauds which the general people face. 28% i.e., citizens are asked to communicate to police authorities if they contact concerned financial body and secondly police authorities are informed as seen in figure 8.

Q 8 How do you deal with financial frauds which the general people face

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Customer care help given to the victims	3	12.0	12.0	12.0
	Dedicated Team is appointed	2	8.0	8.0	20.0
	Transaction is freezed	4	16.0	16.0	36.0
	Police authorities are informed	6	24.0	24.0	60.0
	Citizens are asked to communicate police authorities	7	28.0	28.0	88.0
	Citizens are asked to call relevant Payment apps customer centre	3	12.0	12.0	100.0
	Total	25	100.0	100.0	

Figure 8: Financial frauds people face and how it is dealt.

Observation: The financial frauds which people and how its dealt, financial frauds which the general people face. 28% i.e., citizens are asked to communicate to police authorities if they contact concerned financial body and secondly police authorities are informed. Generally citizens are asked to reach police station and then police station officials tell them to go financial authority again this makes the system more cumbersome for the individual who has faced the crime.

8. The number of active customers having E Banking and payments are increasing and as seen in the figure 9, 48% i.e 40% and above customers are having payment apps and e banking apps.

Q 9 How many percent of active customers are having E Banking and Payment apps

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5% -10%	3	12.0	12.0	12.0
	10%-20%	2	8.0	8.0	20.0
	20%-30%	8	32.0	32.0	52.0
	40% and above	12	48.0	48.0	100.0
	Total	25	100.0	100.0	

Figure 9: Customers having payment apps and E banking

Observation: 40% and above customers are having payment apps and e banking authorization with them. That is a good number as a greater number of people using such apps and systems more vulnerable, they are becoming to the cyber criminals if they lack cyber awareness and how to protect themselves from the cyber criminals. The number will increase in the coming years as digitalisation is increasing and e governance is taking place in each city and district. The numbers will increase and it will create open field for the cyber criminals.

9. One of the most important aspects of financial sector is logging into credentials for getting access into one own profile, in such situation recognition of original website is very important. The financial sector admitted that people tend to not recognize the fake websites 76% i.e., 19 of the respondents admitted people tend to not recognize as seen in figure 10.

Q 10 Do customers recognize fake websites of the financial sectors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	24.0	24.0	24.0
	No	19	76.0	76.0	100.0
	Total	25	100.0	100.0	

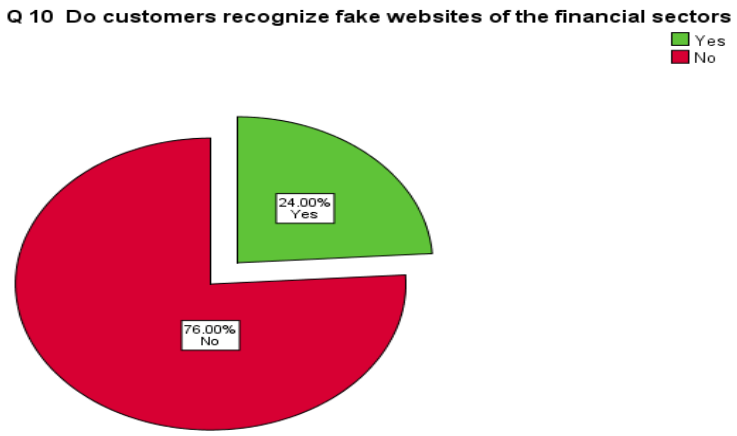


Figure 10: fake website recognition

Observation: The financial sector respondents agreed that people don't recognize fake websites. This will make the life of the cyber criminals easier as they will get access of the login credentials of the user very easily. Fake websites are increasing day by day as on the line of sbi, hdfc, axis exact website are created by the cyber criminals so that people will enter the credentials on the fake website.

10. The most important part is the cyber security in the financial sector. 92% i.e 23 respondents are very much aware of importance of cyber security in the financial sector as seen in figure 11.

Q 11 Are you aware about importance cyber security in the financial sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	23	92.0	92.0	92.0

	No	2	8.0	8.0	100.0
	Total	25	100.0	100.0	

Figure 11: Cyber security importance in financial sector

Observation: The financial sector respondents are pretty much aware of the importance of the cyber security in the financial sector as it creates a block chain and authentication between the customer and the financial system.

11. The financial sector respondents admitted that the current cyber security infrastructure is not sufficient to curb cyber-crime in the financial sector as seen in the figure 12.

Q 12 Is the current cyber–Security Infrastructure sufficient to curb cyber-crime in the financial sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	24.0	24.0	24.0
	No	19	76.0	76.0	100.0
	Total	25	100.0	100.0	

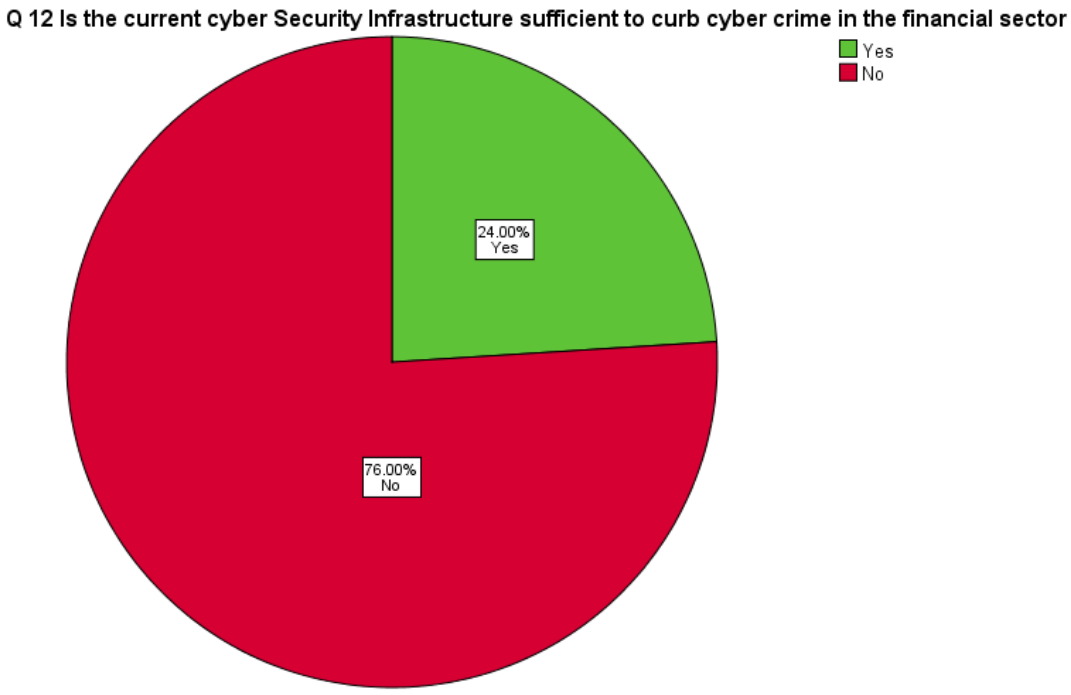


Figure 12: Cyber security Infrastructure not sufficient to curb cyber-crime.

Observation: The financial sector respondents agreed that current cyber security infrastructure is not sufficient to curb cyber-crime in the financial sector. People working in the financial sector agreeing to that cyber security infrastructure should be given priority. Cyber security infrastructure is not sufficient as pvt bank and public banks, co-operative have different cyber security infrastructure.

12. Respondents of the financial sector were asked about the method adopted by the financial sector for prevention of cyber-crimes are enough to cater to the rising problems of citizens. As evident 72% of the respondents answered that it is not sufficient to cater to the rising problems as seen in the figure 13.

Q 13 Do the current methods adopted by the financial sector for prevention of cyber-crime is enough to cater to the rising problems of citizens

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	7	28.0	28.0	28.0
	No	18	72.0	72.0	100.0
	Total	25	100.0	100.0	

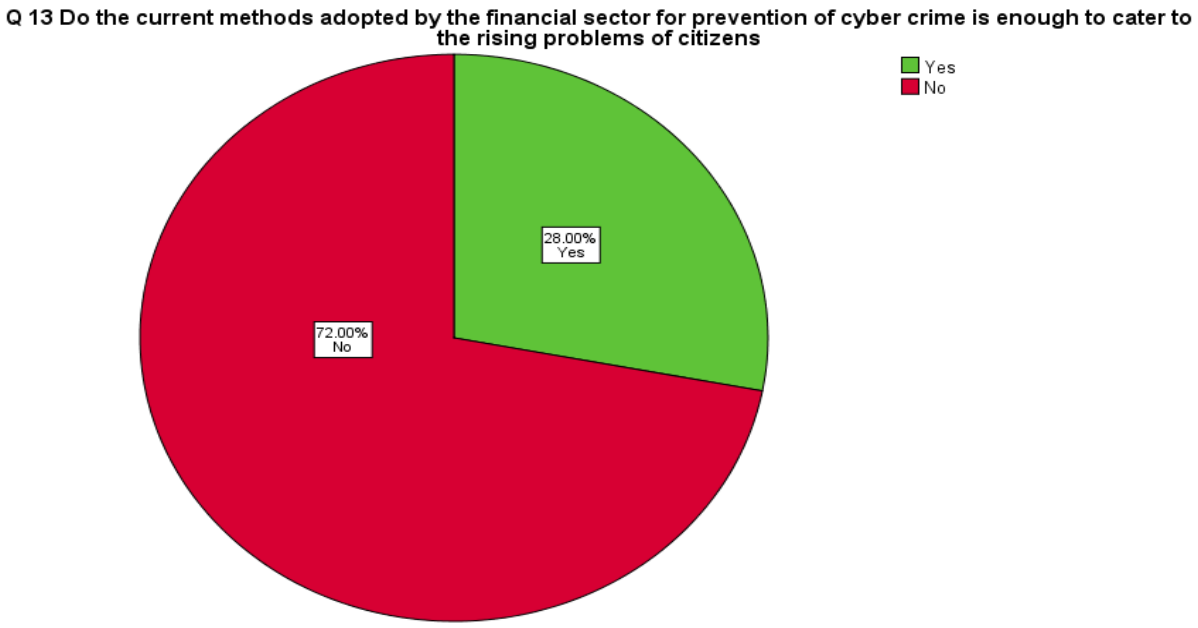


Figure 13: Current methods adopted by the financial sector to cater cyber crime

Observation: 72% of the financial sector respondents agreed that current methods adopted by the financial sector is not sufficient to curb cyber-crime in the financial sector. The prevailing methods adopted by the financial is not enough to put the cyber criminals on the frame. Improvement in authentication and other verification should be made more stronger and awareness among the citizens is the key.

13. Citizens are not aware about the cyber security and its importance in the financial sector. As admitted by the answers given in the questionnaire 64% i.e., 16 respondents of the financial sector believe that citizens are not aware of cyber security and its importance as seen in the figure 14.

Q 14 Are citizens aware of what cyber security is and its importance in the financial sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	9	36.0	36.0	36.0
	No	16	64.0	64.0	100.0
	Total	25	100.0	100.0	

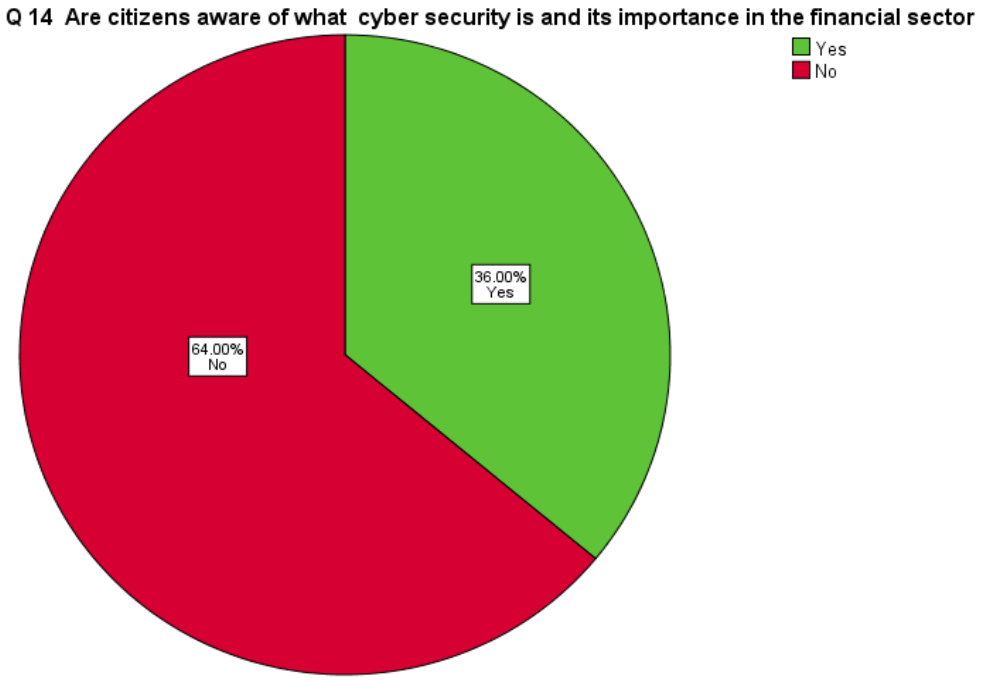


Figure 14: citizens awareness about cyber security and its importance

Observation: 64% of the financial sector respondents agreed that citizens are not aware of cyber security and importance which is the most important part in relation awareness regarding cyber-crime. The most important part citizens are not aware of the cyber security and its importance basic password, link, otp these are small steps towards verification and citizens lack that knowledge.

14. Third party payments application such net banking, internet banking and upi are vulnerable as admitted by the financial sector respondents. 32% i.e 40% above responses show that it is vulnerable and cyber criminals can easily target them as seen in the figure 15.

Q 15 How Much percent of third-party payments applications such as net banking, internet banking, UPI are vulnerable to cyber criminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	5% -10%	8	32.0	32.0	32.0
	10%-20%	6	24.0	24.0	56.0
	20%-30%	3	12.0	12.0	68.0
	40% and above	8	32.0	32.0	100.0
	Total	25	100.0	100.0	

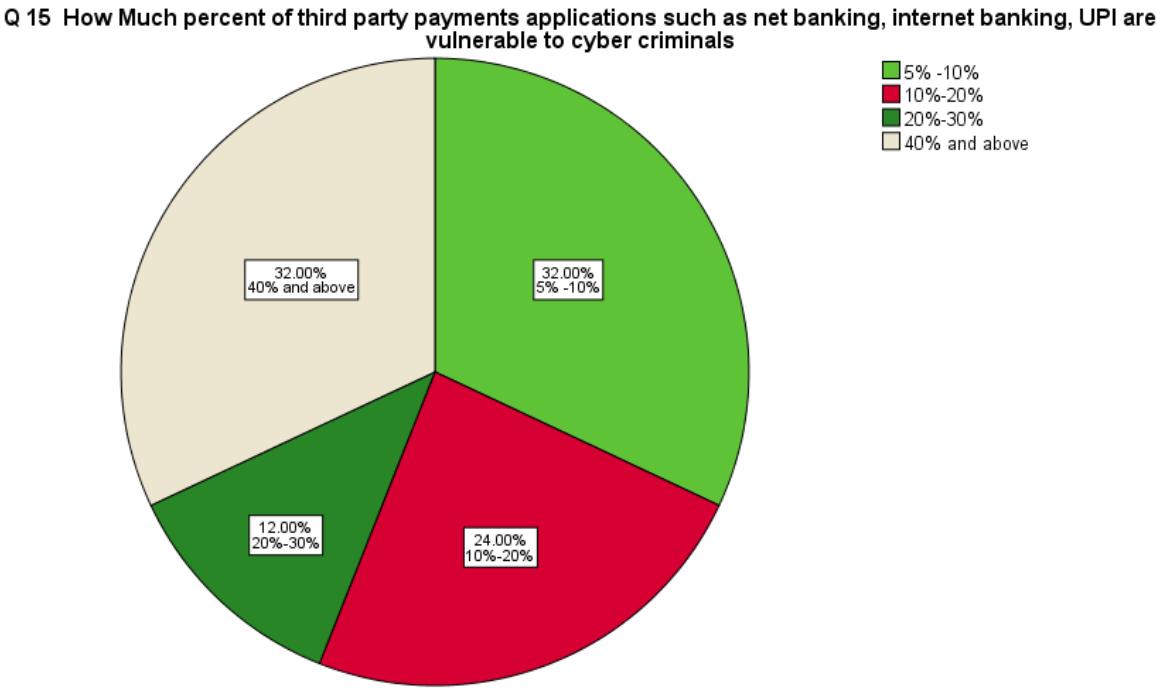


Figure 15: Percent of third-party apps vulnerable to cyber criminals.

Observation: Third party payments application such net banking, internet banking and upi are vulnerable as admitted by the financial sector respondents. 40% and above application are vulnerable to cyber criminals. Third party apps will be increasing in the coming years, and it will give the cyber criminals new methods to by pass the cyber security methods adopted by these apps.

15. Financial sector respondents admitted that people around the age of 40 years of age are not aware of internet or e banking and they are easy targets of cyber criminals. 80% of the respondents admitted that they are prone to cyber criminals as seen in the figure 16.

Q 16 Do you believe People around the age of 40 to years of age are not aware of the internet or E banking, UPI and they are easy targets of cyber criminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	20	80.0	80.0	80.0
	No	5	20.0	20.0	100.0

	Total	25	100.0	100.0	

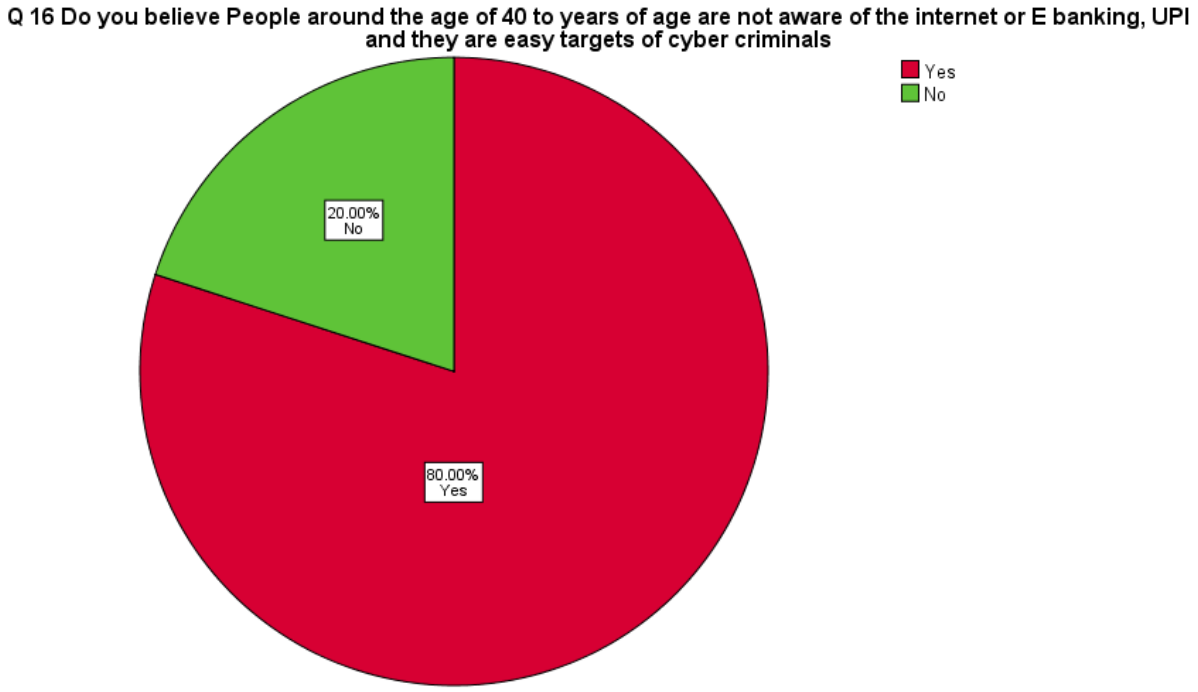


Figure 16: People around the age of 40 are more prone to cyber criminals.

Observation: People around the age of 40 are more prone to cyber criminals as they are not aware of how to use the new technology of which the cyber criminals take the advantage. The old age citizens will be more hit by the cyber criminals as they lack the technological know how they tend to fall prey of the cyber criminals by giving all the details of the credit card debit card otp etc.

16. The financial sector respondents admitted that there is requirement of separate act to protect the financial sector from cyber criminals. 92% of the respondents believes that a separate act is need of the hour as seen in figure 17.

Q 17 Do you feel a separate act is required to protect the financial sector from cyber criminals

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	23	92.0	92.0	92.0
	No	2	8.0	8.0	100.0

	Total	25	100.0	100.0

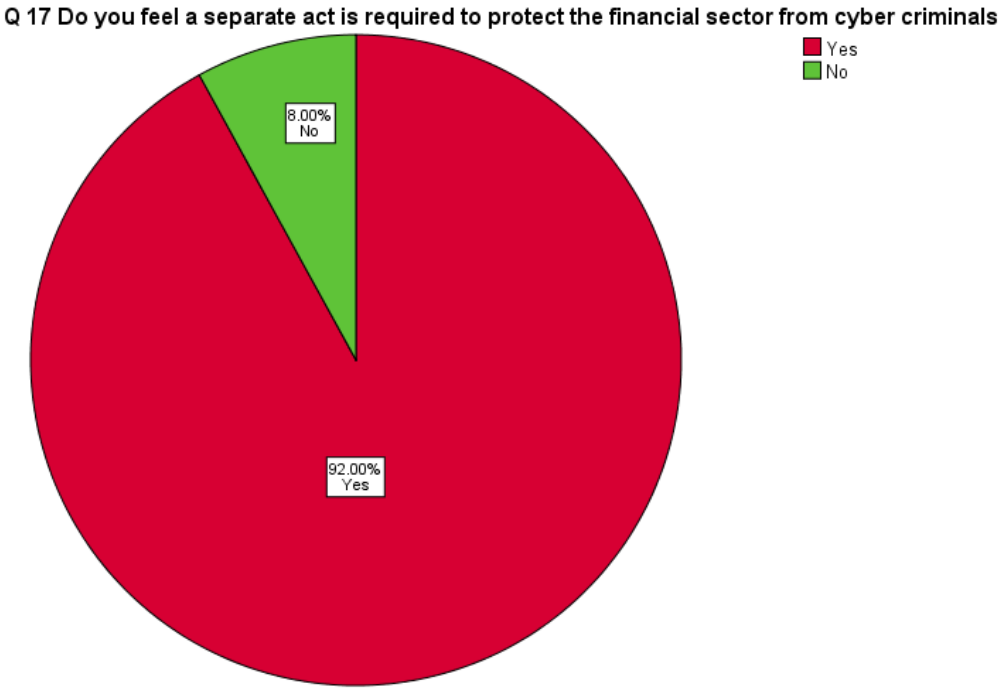


Figure 17: Separate act for financial sector

Observation: The financial sector respondents agreed that new Information Technology is required in relation to financial sector. The general respondents, the law faculties, the advocates and the financial sector respondents agreed that amendments are required in the IT act and plus new act should be introduced for the financial sector as it will be the major target of the cyber criminals in the coming years.

7.3.5 CYBER EXPERTS' OBSERVATIONS

Interviews of the cyber experts were taken for the empirical research. Cyber experts were chosen from Mumbai and nearby cities Thane, Navi Mumbai, Kalyan. Cyber experts' opinions and suggestions were very important for the researcher as it dealt with the important aspects of cyber-crime and cyber laws in Mumbai with reference to the financial sector in Mumbai. Personal interviews and telephonic interviews were conducted by the researcher to know about the cyber-crimes and cyber laws in Mumbai. Questions such as, current structure of Cyber-crimes and cyber laws in India, whether Cyber-crimes are affecting financial sector in Mumbai critical infrastructure and its importance, Opinion on current cyber act i.e., is

information technology act 2000, Cyber security infrastructure in the financial sector whether they are capable of catering Cyber-crimes. Most of the cyber experts stressed on awareness that citizens are lacking and pointed out that the current structure of Cyber-crimes and cyber laws in relation to the financial sector in Mumbai is lacking and more improvement is required Such as improving cyber security mechanism two factor authentication awareness regarding usage of financial information and financial apps.

1. Mr Pankaj Bafna Cyber expert, Mumbai

The first question which I asked Mr Pankaj Bafna was his own opinion on the current structure of Cyber-crimes and cyber laws in India.

1. He stated that the current structure is imbalanced and cyber laws are to be improved and changed as per the technology is developing
2. The methods adopted by the cyber criminals are way ahead of the technology we are using, as we are one step behind the cyber criminals.
3. Mr Bafna pointed out that the structure is to be improved regarding the laws but still awareness was the key part he was focusing on as Laws can be made strict but still its the individual should have the awareness regarding the cyber-crime.

The second question which I asked Mr Bafna was regarding the cybercrimes whether they are affecting the financial sector in Mumbai and if so what are his opinion how it can be tackled

1. He stated that financial players are at risk.
2. He pointed out that usually the crime committed is mostly on the financial part as most of the crimes committed by the cyber criminals leads to the financial part as compared to the crimes committed which are like hacking of social media, hacking of emails as it doesn't affect the financial aspects of an individual.
3. His suggestion on how it can be tackled was very easy, he said that the person sitting at home can curb that financial crime by just calling the telecom operators and the nodal officers to be contacted of that state or that district they will immediately start working.
4. He suggested that a person should be vigilant and should visit the authorized websites of Banking or financial sites in that nodal officer’s phone numbers are given or email ids are given so that the person can be contacted when such crime gets committed.

The third question which I asked Mr Bafna was regarding his opinion on the current cyber act whether it is capable to cater Cyber-crimes in the financial sector.

1. He stated that amendments are required in the current information technology act 2000.
2. new amendments are on its way as severe punishments are being prescribed in the coming new bill on information technology act in which Mr Bafna was in the drafting committee.
3. He Pointed out that it's not the act or law which should be made stringent, it is the people who should be aware of present laws.

The fourth question which was regarding the critical infrastructure and its importance how it can be strengthened

1. He pointed out that there is a positive point on the critical infrastructure as the required internet speed is not there with India, let’s speed doesn't help the cybercriminals to attack the critical infrastructure that is the electrical grid nuclear power plants.
2. He Pointed out that the critical infrastructure in relation to Defense is very different as they have layers involved if one attack is committed and Immediately that layer is stopped and other layers keep functioning that can be tackled accordingly.

The next question which i asked was regarding whether new information technology act should be introduced to cater cyber crimes

1. He stated that amendments are to be made in the new bill which is due in the coming year and designated powers are to be allotted to High Court
2. for the functioning of the courts the appointment of judges should be made and it would be based on the qualification such as BSc, Msc and LLB
3. In every High Court new cyber branch is to be introduced and the High Court to be given powers to establish in each district cyber court for the functioning and of Cyber matters.

The next question which I asked was regarding the cyber security infrastructure in the financial sector whether they are capable of catering Cyber-crimes.

1. he stated that cyber security infrastructure is goods as controlled by the RBI in private and public banks and private banks are having a more advantageous position as compared to the cyber security infrastructure it's the people who are not aware and they fall into the Trap of Cyber criminals
2. He pointed out that cooperative banks are more at risk as compared to other banks as they lack the required infrastructure which is to be there to avoid cyber criminals.

Lastly i asked about his comments, opinions on cyber-crimes and cyber laws and simple act on the financial sector in Mumbai

1. He stated that the financial sector is in a disastrous position.
2. The government should look into this as early as possible as there is a situation in which a financial war could emerge in India by the cyber criminals.
3. He pointed out that an educated person who is having two mobile phones should keep his financial apps in different mobile phone and social media apps in other phone so that the financial aspect would not get affected if a mobile phone gets hacked.

2. Mr. Chaitanya Bandari Cyber Expert

The first question which I asked Mr Bhandari was regarding the current structure of Cyber-crimes and cyber laws in India.

1. He stated that improvement is required in the current IT Act 2000 As it is not capable of dealing with the rising Cyber-crimes in India.
2. Cyber laws are not working as it is required. IT Act 2000 is not having a deterrent effect on the cyber criminals.
3. Cyber cells are required to work in a more efficient manner.

The next question which I asked Mr Bhandari was regarding Cyber-crimes affecting the financial sector in Mumbai and what are his opinions on how it can be tackled.

1. The answer was the same as given by Mr Pankaj Bafna, Mr Bhandari also pointed out that awareness is required for the common man. He stated that awareness is the key towards catering Cyber crimes

2. Cyber criminals are using new Trends Day by day and we have to be on the same line in relation to Cyber-crimes.
3. He pointed out that awareness should be made regarding the anydesk app, so that citizens don't fall prey to cyber criminals in relation to financial crimes committed by the cyber criminals.

The third question which I asked to Mr Bhandari was regarding the current cyber act whether it is capable of cater the rising Cyber-crimes in the financial sector.

1. He Pointed out that extreme level amendments are required in the current IT Act 2000.
2. Section 66C and section 66D should be made non bailable offence in the current IT Act 2000.
3. He was of the opinion that Fastrack cyber courts should be introduced to Cater cybercriminals.

The next question which I asked was regarding the critical infrastructure and its importance and how it can be strengthened.

1. Mr Bhandari was of the opinion that the designated officer should be appointed in the particular department.
2. Technical knowledge should be given to the designated officer in the particular Domain so that if any cyber-attacks are committed then such officer is capable of stopping that cyber-attack.

The fifth question which I asked Mr Bhandari was whether a new information technology act should be introduced.

1. He suggested that amendments will work as of now as the new bill will take too much time to be implemented.
2. He pointed out that for the critical infrastructure separate provisions should be introduced.

I asked Mr Bhandari on his view on the cyber security infrastructure in the financial sector whether they are capable of dealing with cyber crimes

1. He pointed out that the critical infrastructure is not well equipped in the State Bank of India.
2. He is of the opinion that the financial sector is at a great risk from the cyber criminals in the current situation and improvements are required in the cyber security infrastructure.
3. There is scope for improvement in the cyber security infrastructure

Lastly, I asked about his suggestions, comments and opinions on cyber-crime, cyber law and its impact on the financial sector in Mumbai.

1. He was of the opinion that cybercrime in the coming future will increase at a greater pace.
2. He suggested that the impact will be more severe as compared to the situation now.
3. Lastly, he said that cybercrime will increase in the financial sector in Mumbai.

3. Mr Abhishek Mishra cyber expert

The first question which i asked Mr. Abhishek was regarding the current structure of Cyber-crimes and cyber laws in India.

1. Mr Abhishek Seth stated that the Information Technology Act 2000 is specific and not dynamic. IT Act 2000 is lacking the Global perspective which is required to cover every aspect of Cyber-crimes in the current scenario. He stated that India is standing nowhere in relation to Cyber-crimes and cyber laws.
2. We are in the first stage in relation to Cyber-crimes and cyber laws in India.
3. He stated that technology is overpowering us and lack of awareness is the key which the cyber criminals are using against us.

The second question which I asked Mr Abhishek was regarding whether Cyber-crimes are affecting the financial sector in Mumbai. What are his opinions and how can they be tackled?

1. He stated that the financial sector is targeted on a daily basis as compared to other Cyber-crimes.
2. As stated by other two cyber experts Mr. Abhishek also pointed out that lack of awareness is the key that is used by cyber criminals to lure individuals. Educated people also get trapped in the scam of Cyber criminals.

3. He also suggested that we have technology that is there for the help of the people but it is used in a wrong way and not used properly in relation to the financial scams which are committed by the cyber criminals.
4. His focus was on Awareness of Cyber-crimes in general public and vigilance.

The next question which I asked was about the current cyber act whether it is capable to deal with the rising Cyber-crimes in the financial sector.

1. He was of the opinion that the current information technology is not powerful and impactful.
2. IT act is dependent on other laws.

The next question which I asked was about critical infrastructure and its importance and how it can be strengthened.

1. Mr. Abhishek pointed out that security agencies are efficient to deal with cyber-crimes in relation to critical infrastructure in India.
2. Mr Abhishek pointed out about knox security system at hardware level that is provided at different Agencies specially the defense system which helps to deal with cyber-crime at critical infrastructure level.
3. Whenever critical infrastructure is hacked at different channels there are different stages so if one channel is hacked then there is scope for the other channel to be switched off.
4. Advanced technology is used under critical infrastructure so that cyber criminals cannot bypass that security.

The next question which i asked was regarding whether new information technology act should be introduced to deal with cyber-crimes.

1. He pointed out that new hierarchy is needed in the information technology act 2000.
2. Cyber courts should be introduced and it is required to deal with cyber-crimes.
3. He pointed out that biometric laws should be introduced in the current scenario.
4. Harsh punishment should be introduced in the information technology act 2000 to deal with cyber-crimes.

The next question which I asked Mr Abhishek was regarding the cyber security infrastructure in financial sector whether they are capable of dealing with cyber crimes

1. He was of the opinion that banks are strengthening their cybersecurity infrastructure it is the lack of awareness which are resulting in the financial Cyber-crimes.
2. Awareness regarding OTP sharing, auto payment system should be stopped, minimum limit on upi should be introduced, international transaction should be stopped, this would help in strengthening the cybersecurity infrastructure in relation to financial Cyber crimes

Lastly, I asked about his suggestion, comments and opinions on cyber-crime cyber laws and its impact on the financial sector in Mumbai

1. He was of the opinion that improvement is required in relation to Cyber Law and its impact on the financial sector in Mumbai.
2. Overall information technology act 2000, RBI guidelines to be followed very strictly.

4. Mr. Sachin Dedhia Cyber Expert.

The first question which I asked Mr Sachin was regarding the current structure of Cyber-crimes and cyber laws in India.

1. He was of the opinion that the current structure of Cyber-crimes and cyber laws in India is not full proof.
2. He pointed out that cybercrimes will increase in the coming years, laws will not have that much effect on cyber-crime.
3. New methods are being adopted by cyber criminals in relation to Cyber-crimes.

The next question was regarding whether Cyber-crimes are affecting financial sector in Mumbai what are your opinions and how it can be tackled

1. He was of the opinion that the financial sector will be Hit hard as most of the times the crimes committed are in relation to scams of monetary level as compared to other Cyber-crimes.
2. Technologies are overpowering individuals; awareness should be there among citizens.
3. He was of the opinion that human errors should be reduced as it is the most common form where an individual get scammed by the cyber criminals.

The next question was regarding the current information technology act whether it is capable to deal with rising Cyber-crimes in the financial sector.

1. Mr Sachin stated that improvement is required in the current IT Act.

The fourth question was regarding the critical infrastructure and its importance how it can be strengthened.

1. Mr. Sachin stated that, the critical infrastructure and the systems, whether it is of hardware and software level are self-owned and not from any third party so it becomes very difficult for the cybercriminals to attack the critical infrastructure.
2. He stated that multiple attempts are required to hit the critical infrastructure but it can be done by the cyber criminals.
3. He also pointed out about the knox software which are used by the critical infrastructure agencies to deal with cyber-attacks.
4. Critical infrastructure are having different channels and different stages and different networks so it becomes very difficult to attack the critical infrastructure, different stages are there , one have to bypass each and every stage so it helps to protect the other system

The next question was regarding whether new information technology act should be introduced to deal with cyber crimes

1. He was of the opinion that amendments are required and that should be given the top most priority.
2. Technology and law should go hand in hand, provision should be introduced as the technology is developing.

The next question was regarding whether cyber security infrastructure in financial sector are capable of dealing with cyber-crimes.

1. Mr Sachin stated that cyber security infrastructure at the financial level is good but not the best it can be by- passed by hackers.
2. Human errors should be reduced.

Lastly, I asked about his suggestion, comments and opinions on cyber-crime cyber laws and its impact on the financial sector in Mumbai

1. He was of the opinion that the financial sector will be hit hard.
2. The RBI guidelines should be followed in relation to the financial sector.
3. Awareness is the most important aspect of cyber-crime and cyber laws and its impact on the financial sector in Mumbai
4. He was of the opinion that Technology will over override awareness

5. Mr Prem Sagar Gavli Cyber Expert

The first question which I asked Mr Prem Sagar Gavli was regarding the current structure of Cyber-crimes and cyber laws in India.

1. Mr Sagar was of the opinion that amendments are required in the IT Act 2000.
2. Technology and law should go hand in hand as required in the information technology act 2000.

The next question was regarding whether Cyber-crimes are affecting financial sector in Mumbai what are your opinions and how it can be tackled

1. Mr. Sagar was of the opinion that Cyber-crimes are affecting the financial sector in Mumbai and specially awareness is required among the citizens.
2. He was of the opinion that cyber experts are required in each district depending upon the population to deal with cyber-crimes.

3. His was of the opinion that the financial crimes can be reduced on awareness with the help of awareness on Simple concepts such as don't share OTP, don’t click on the suspicious link, barcode scanning

The next question was regarding the current information technology act whether it is capable to deal with rising Cyber-crimes in the financial sector

1. Mr. Sagar said that amendments are required in the IT Act 2000
2. Cyber-crimes related to financial sectors and its related provisions should be added in the IT Act 2000
3. Organized structure should be there in relation to IT Act, CrPC and IPC provisions.

The fourth question was regarding the critical infrastructure and its importance and how it can be strengthened.

1. He pointed out that Cyber experts are required in critical infrastructure Agencies and corporations.
2. Individual training of Cyber related crimes and cyber-attacks should be given at the local level to the uppermost level

The next question was regarding whether new information technology act should be introduced to deal with cyber crimes

1. He was of the opinion that, Amendment should be made and should be given the most top most priority.
2. He said that structured form is required in the information technology act between all sectors.

The next question was regarding whether cyber security infrastructure in the financial sector is capable of dealing with cyber-crimes.

1. He was of the opinion that cyber cyber security infrastructure is not that much capable to deal with cyber-crimes.

Lastly, I asked about his suggestion, comments and opinions on cyber-crime cyber laws and its impact on the financial sector in Mumbai

1. Mr Sagar pointed out that cyber-crime is so grievous it tends to get converted into real crime.
2. There is denial from the police, cyber-crime systems should be developed and complaints, grievance should be taken immediately.
3. He pointed out that rural areas are more vulnerable as compared to urban areas as they don't have any source for their grievances.
4. Tracking system should be made faster so that the cyber-criminal can be caught at an early stage of the crime

6. Mr. Snehal Vakilna Cyber Expert

The first question which I asked Mr. Snehal Vakilna was regarding the current structure of Cyber-crimes and cyber laws in India.

1. He pointed out the current Cyber-crimes and cyber laws in India are not that efficient to curb the cyber-crimes in the near future .
2. He was of the opinion that the technology is developing day by day and we should Go hand in hand with the technology and as well as keep developing the cyber laws in the country.

The next question was regarding whether Cyber-crimes are affecting financial sector in Mumbai what are your opinions and how it can be tackled

1. He pointed out that Cyber-crimes affecting the financial sector in Mumbai the reason behind that, awareness was the most important part which was lacking among the individual.
2. Awareness was the most important thing to deal with the rising Cyber-crimes in the financial sector

The next question was regarding the current information technology act whether it is capable to deal with rising Cyber-crimes in the financial sector

1. He was of the opinion that the information technology act should be amended in relation to the rising technology which is used by cyber criminals.
2. The current laws should be made in consonance with the laws which are related to the financial sector and punishment should be given to the cyber criminals, to show deterrent effect on cyber criminals

The fourth question was regarding the critical infrastructure and its importance and how it can be strengthened.

1. He stated that critical infrastructure is a very important aspect of India and it should be protected from cyber criminals.
2. Cyber experts and domain related experts should be appointed in the critical infrastructure departments so that the cyber criminals cannot attack those agencies.

The next question was regarding whether new information technology act should be introduced to deal with cyber crimes

1. He was of the opinion that and amendment should be made as early as possible so that the technology which is getting developed day by day can be tackled by the provisions that are readily available in the information technology act 2000.
2. Stringent laws should be introduced in relation to financial crimes that are committed by the cyber criminals in the cyber world.

The next question was regarding whether cyber security infrastructure in the financial sector is capable of dealing with cyber-crimes.

1. Cyber security infrastructure needs improvement as there should be consonance and cooperation between the telecommunication department, the banking officials and the police officials and any other financial corporation that are involved in the financial Crime.
2. Cyber security in infrastructure is pretty much equipped in private banks as compared to the public sector banks and cooperative banks.

Lastly, I asked about his suggestion, comments and opinions on cyber-crime cyber laws and its impact on the financial sector in Mumbai

1. Cyber laws should be amended as early as possible.
2. Financial crime will increase day by day in the coming future.
3. More importance should be given to Cyber-crimes and and to the cyber criminals
4. Consonance of each department should be there while dealing with cyber-crimes as it would help in speedy disposal of Cyber-crimes cases

7.3.6 POLICE OFFICIALS' OBSERVATIONS

Interviews of the police officials were taken for the empirical research. police officials were chosen from Mumbai and nearby cities Thane, Navi Mumbai, Kalyan.police officials opinions and suggestions were very important for the researcher as it dealt with the important aspects of cyber-crime and cyber laws in Mumbai with reference to the financial sector in Mumbai. Personal interviews and telephonic interviews were conducted by the researcher to know about the cyber-crimes and cyber laws in Mumbai. Questions such as How cyber-crime matters are solved, What is the current structure of communication between banks Telecom operators and police officials after cyber-crime is committed , Whether cyber-crime is solved if solved in how many days, Whether people know how to file cyber complaint , Experience with cyber criminals Appellate mechanism of Cyber complaint, More cyber cells are required, Suo Moto cognizance, Citizen cyber cells should be introduced Lastly opinion suggestions how Cyber-crimes can be dealt in Mumbai

1. Mr. Prashant Chougule (Police inspector) (Maharashtra cyber Nodal office)

The first question which I asked Mr Prashant was regarding how Cyber-crimes matters are solved.

1. He stated that cyber-crime matters are solved on a case to case basis, for example financial fraud, Email fraud, Link related fraud.
2. To Solve cyber related matters IP address, place a major role for tracking the person.
3. From the IP address police official track the details of the cyber-criminal.

4. IP address helps the police officials to find the user Detail mobile number bank account details

The second question which I was regarding current structure of communication between banks Telecom operators and police officials after cyber-crime is committed

1. Mr Prashant pointed out that the golden hours that is the first two hours after a crime is committed is very important and plays a major role in tracking the cyber criminal
2. He said that the three parties are working in tandem but it is very much different as Prashanth has stated
3. When the complaint is filed with the police station the police officials and send letter to the to the Banking authorities and they apply within .72 hours
4. Mr Prashant stated that in order to avoid the money to be circulated in different accounts after the commission of the cyber-crime the most important thing is that the bank officials must slow down the process of crediting the account in different different accounts

The next question was in how many days cybercrime matter is called

1. Mr Prashant stated that normally 72 hours is the normal scenario in which a reply comes from any of the intermediaries which are involved in the cyber issue
2. Secondly, he stated that the importance of the case is also taken into consideration by the police officials depending upon the nature of the offence and the amount involved
3. He said that minimum seven days is the normal number which can be given to an individual in relation to Cyber-crime to be solved.

The next question was regarding whether people are aware how to file cyber complaint

1. He said that urban areas people are aware of how to file a cyber complaint
2. He stated rural areas people are not aware of how to file a cyber complaint whom to approach where to go
3. Police officials also do not know how to deal with the people who come to them with the cyber complaints

Next question was regarding the experiences of police official with cybercriminals

1. Mr Prashant stated that mostly the cybercriminals are uneducated those who are dealing with crime such as lottery credit card and debit card related scam OTP scam
2. He stated that hackers are more trained and more educated as compared to the criminals who had just walking with the system and know how to deal with the system and to crack the individuals depending upon their psychology

The next question was regarding the mechanism of Cyber complaints

1. 1930 cyber complaint number which is available 24 into 7 all India
2. Ncrb portal
3. Cyber cell in the nearest police station
4. Lastly the nearest police station

The next question was regarding more cyber cells are required in each police station

1. Mr. Prashant stated as there is no requirement of more cyber cells in each police station
2. He stated that there is requirement of awareness among the police officials and training should be provided to them in relation to Cyber-crimes and cyber criminals

The next question was regarding whether police take to a Moto cognizance of an Cyber crime

1. He stated that police officials can take suo Moto cognizance of cybercrime

The next question was regarding citizen cyber cell should be introduced in each area

1. He stated that under cyber police station citizens can be appointed to take complaint

The last question was regarding his suggestions or opinions how cyber-crime in Mumbai can be streamlined to cater Cyber crimes

1. The foremost thing was the awareness part which the people was lacking

2. He stated that educated people are more prone to Cyber criminals as compared to the uneducated
3. The do's and don'ts should be followed by the citizens very carefully to avoid Cyber crimes
4. Data plays an important role in the cyber crimes
5. Psychology of people also plays an important role which are used by the cyber criminal's greed is the most important factor of which cyber criminals are taking advantage

The following observations of Cyber experts and police officials and the questionnaires for the general respondent, advocates, for law faculties and the financial sector gave us the required data to come up to an conclusion that we are Vulnerable to the cyber criminals as they are developing their Technology day by day. As admitted by cyber experts and as well as the police officials that awareness was the most important key which was lacking among the individuals and the citizens of Mumbai. Data collected by the researcher helped to reach to an result which is very much required for the empirical part and for the analysis of the responses given by the respondents.

7.4. HYPOTHESES TESTING

The researcher formulated the following hypothesis before the research begin.

- ❖ The Information Technology act is inadequate to tackle cybercrimes. In spite of the existing laws there is still space for formulating provisions and making necessary amendments to combat the menace of cybercrimes.

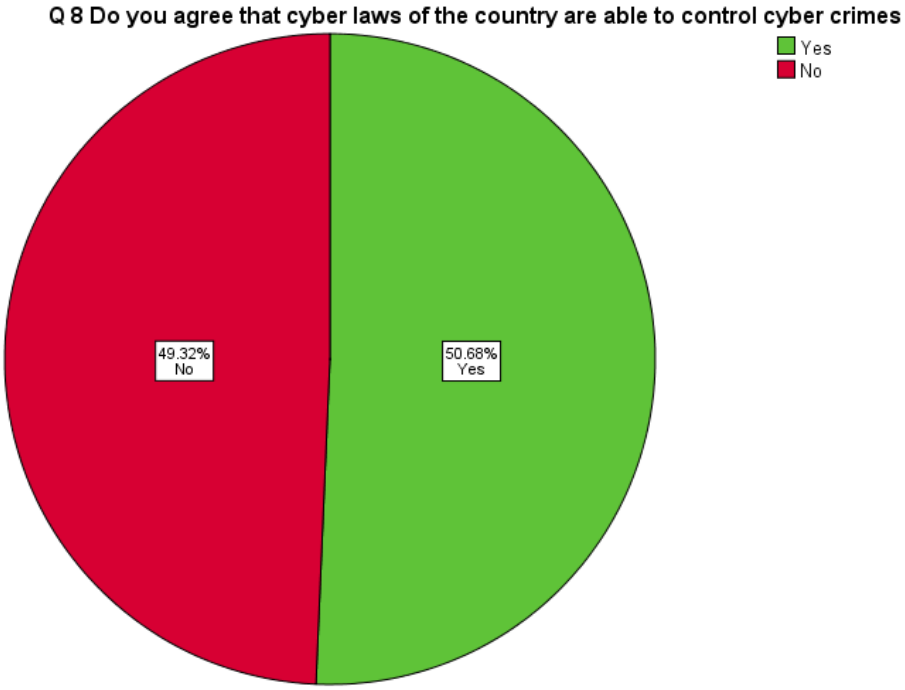
The following hypothesis is proved through the empirical research conducted by the researcher with all relevant data supporting the hypothesis. The researcher floated questionnaires to general respondent's, lawyers, law faculties, advocates and took personal interviews of cyber experts. In which researcher asked various questions relating to Information Technology Act 2000 and whether its capable to curb cyber-crime in the country, whether amendments are needed or we need a new act altogether to curb cyber-crime in the county.

Similarly, questions relating to cyber security mechanism adopted is not capable to cater the fast pace technology and that is hitting the financial sector the most as admitted by the cyber

experts in their interview. The financial sector questionnaire also pointed that the cyber security mechanism is not full proof.

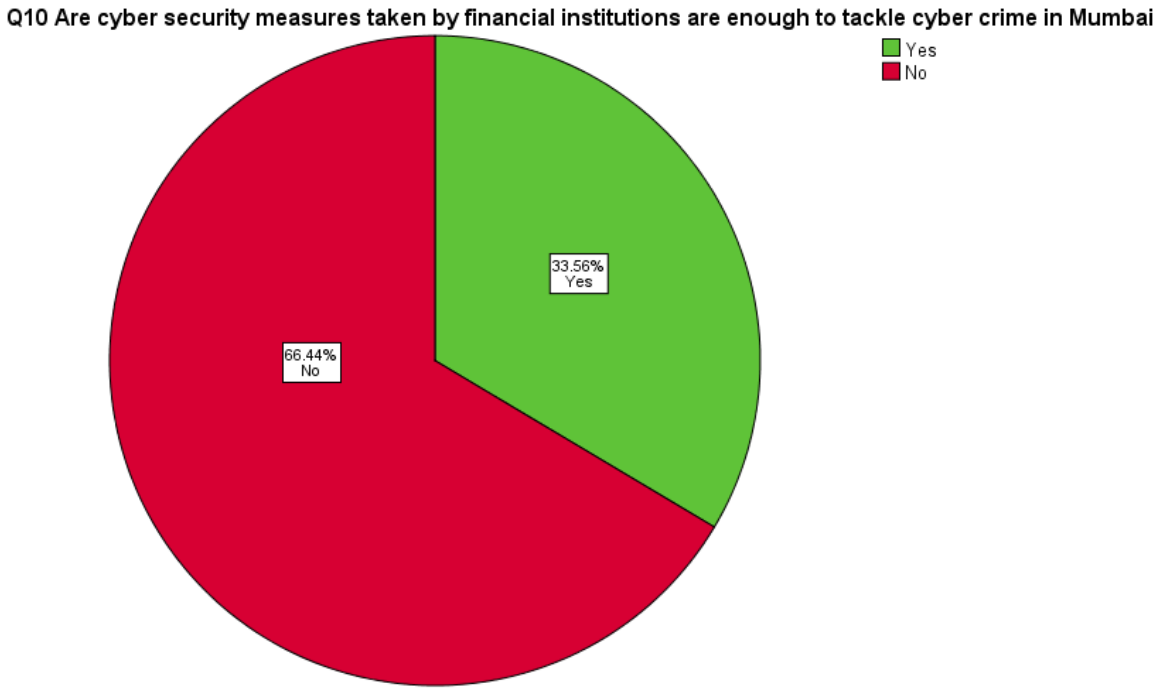
The Justification can be read with following analysis done by the researcher.

1. The general respondents were asked the question whether the current cyber act of the country is sufficient to curb the cyber-crime.



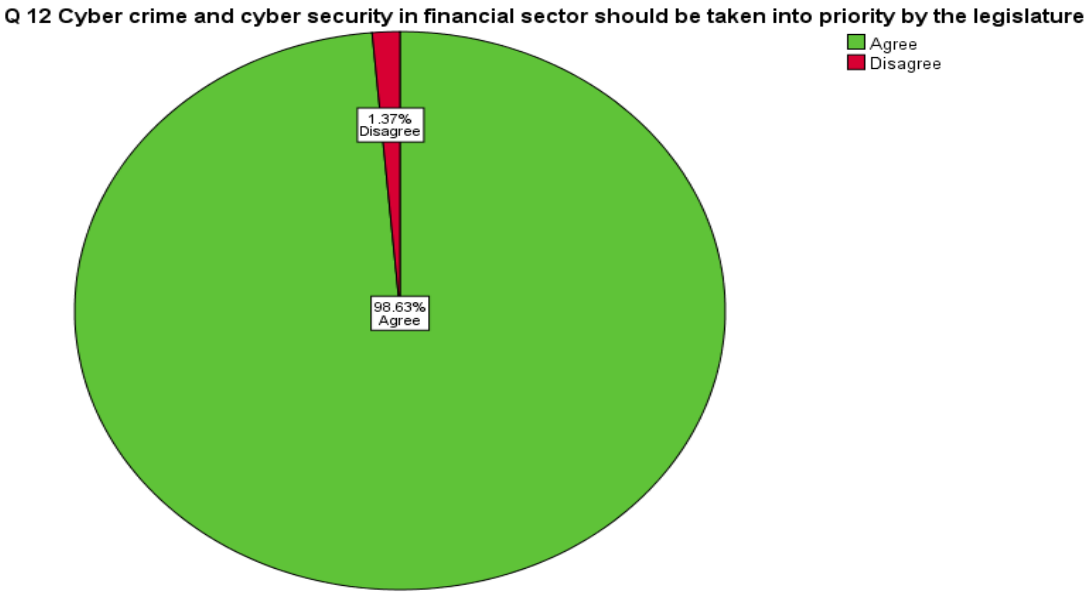
50.7% i.e., 74 respondents felt that yes, it is able to control the cyber-crimes and 49.3% i.e., 72 people felt that it is not able control cyber-crimes as seen in figure 11. In general, it is not able to control crime.

2. General Respondents were asked about the cyber security measures taken by the financial institution are enough to tackle the cyber-crime in Mumbai.



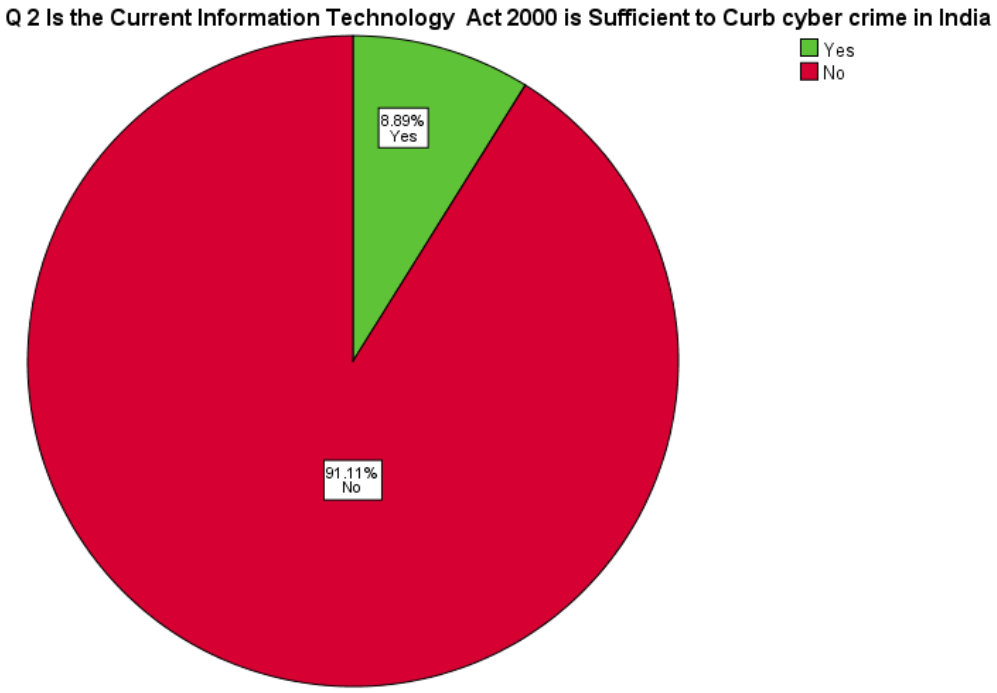
The respondents agreed to that cyber security mechanism adopted by financial institutions are not capable to cater cyber-crime related problems. 66% i.e., 97 respondents felt that it is not enough to tackle the cyber-crimes in the pie diagram.

3. The general respondents were asked about the cyber-crime and cyber security in the financial sector as these two should be given priority.



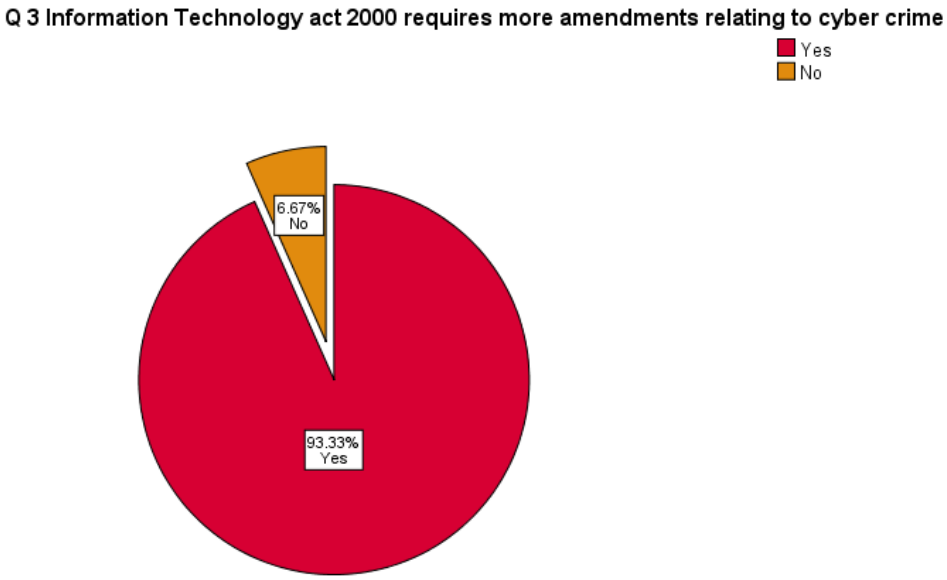
The general respondents agreed that due importance should be given to the cyber-crime and cyber security 98% of the respondents said yes that, cyber security and cyber-crime should be given due importance by the legislative body of the country

4. The law faculties were asked about that, is the current information technology act 2000 is sufficient to curb cyber-crime in India.



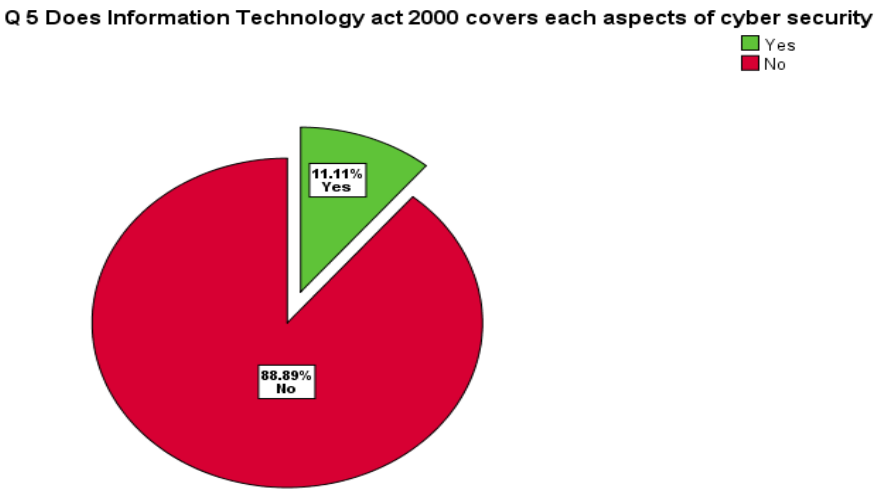
The law faculties agreed that current IT act is not sufficient to curb cyber-crime in India. 91% i.e., 41 respondents agreed that current Information Technology act is not sufficient to curb cyber-crime in India

5. Law faculties were asked about whether more amendments are required in the Information Technology act 2000.



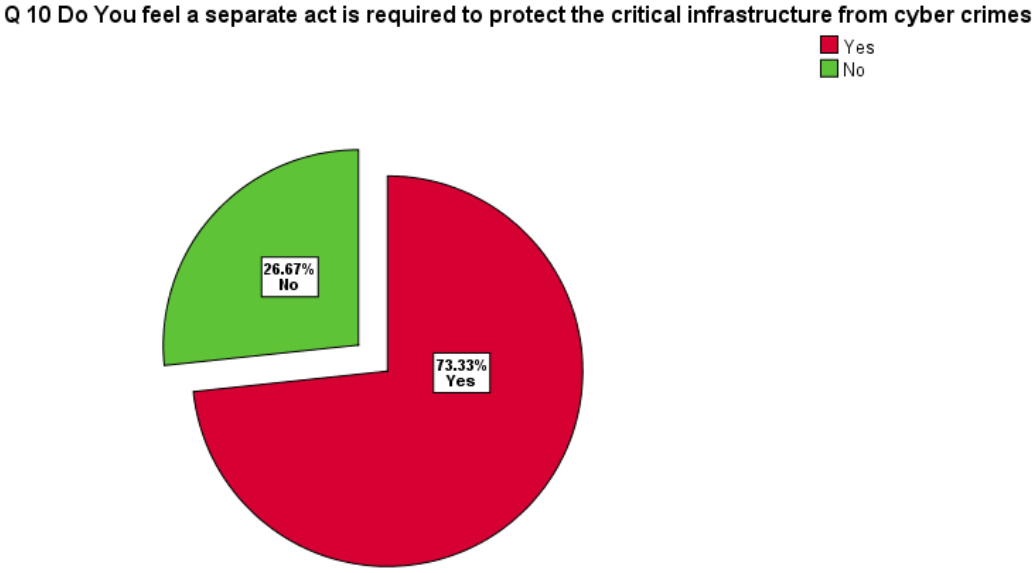
The law faculties agreed that more amendments are required in the IT act 2000 as its not sufficient to curb cyber-crime in India ,93% i.e., 42 of the faculties' said Yes amendments are required.

6. The law faculties were asked about whether IT act 2000 covers every aspect of cyber security.



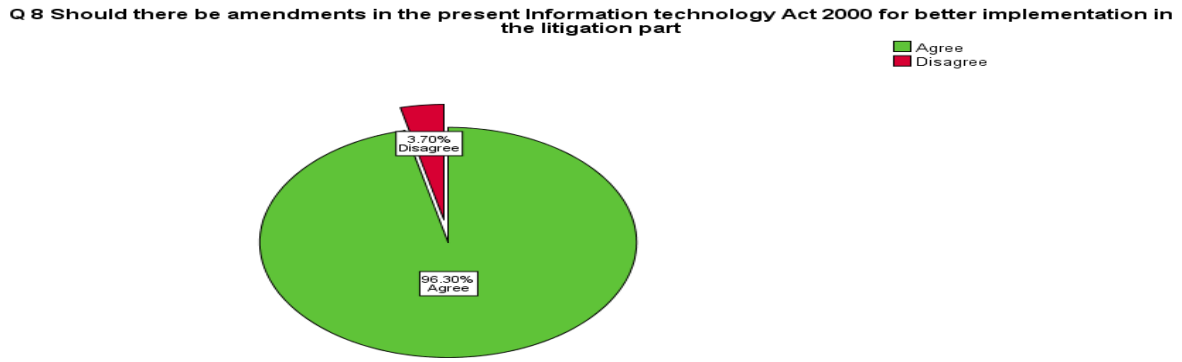
The law faculties agreed that Information Technology does not each aspect of cyber security. 88.9% i.e., 40 respondents said that it doesn't cover all aspects of cyber security

7. The most important question asked to the law faculties was do they feel a separate act is required to protect the critical infrastructure from cyber-crimes.



The law faculties agreed that, separate act is required to protect the critical infrastructure of the country through cyber criminals. 73% i.e., 33 respondents said that we need a separate act for the critical infrastructure to protect the critical infrastructure

8. The litigating lawyers admitted that there should be amendments in the Information Technology Act 2000 for better implementation.



96% of the litigating lawyers admitted that there should be amendments in the Information Technology Act 2000 for better implementation.

9. The financial sector respondents admitted that the current cyber security infrastructure is not sufficient to curb cyber-crime in the financial sector

Q 12 Is the current cyber–Security Infrastructure sufficient to curb cyber-crime in the financial sector

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	6	24.0	24.0	24.0
	No	19	76.0	76.0	100.0
	Total	25	100.0	100.0	

The financial sector respondents agreed that current cyber security infrastructure is not sufficient to curb cyber-crime in the financial sector.76% of the financial respondents said No the current system is not capable.

10. Respondents of the financial sector were asked about the method adopted by the financial sector for prevention of cyber-crimes are enough to cater to the rising problems of citizens.

Q 13 Do the current methods adopted by the financial sector for prevention of cyber-crime is enough to cater to the rising problems of citizens

		Frequency	**Percent**	**Valid Percent**	**Cumulative Percent**
Valid	Yes	7	28.0	28.0	28.0
	No	18	72.0	72.0	100.0
	Total	25	100.0	100.0	

72% of the financial sector respondents agreed that current methods adopted by the financial sector is not sufficient to curb cyber-crime in the financial sector.

The following hypothesis is proved through the empirical research conducted by the researcher with all relevant data supporting the hypothesis.

- ❖ The current cyber security mechanism in India is not capable to cater with the fast pace of developing technology at the hands of cyber criminals, that could hit the critical infrastructure of India such as the defense sector, financial sector, the grid lines and the corporations.

The following hypothesis is disproved through the empirical research conducted by the researcher with all relevant data supporting the hypothesis. The researcher took personal interviews of cyber experts and telephonic interviews of the experts in Mumbai and some of the experts where from nearby Mumbai. In which researcher asked various questions relating to Cyber security mechanism of India is not capable to protect its Critical Infrastructure and Information Technology Act 2000 lacked the cyber security mechanism and whether its capable to curb cyber-crime in the country.

Similarly, questions relating to cyber security mechanism adopted by India, is not capable to cater the fast pace technology and that is hitting the financial sector the most as admitted by the cyber experts in their interview. The cyber experts' personal interviews and telephonic interview disproved my hypothesis.

The Justification can be read with following analysis done by the researcher.

The fourth question of my personal interview with Mr. Pankaj Bafna, a well-known cyber expert of Mumbai was regarding critical infrastructure and its importance how it can be strengthened

1. He pointed out that there is a positive point on the critical infrastructure as the required internet speed is not there with India, let's speed doesn't help the cybercriminals to attack the critical infrastructure that is the electrical grid nuclear power plants.

2. He Pointed out that the critical infrastructure in relation to Defense is very different as they have layers involved if one attack is committed and immediately that layer is stopped and other layers keep functioning that can be tackled accordingly.

The same question regarding the critical infrastructure was asked by me to Mr. Chaitanaya Bhandari well known cyber expert of Mumbai he stated that,

1. Mr Bhandari was of the opinion that the designated officer should be appointed in the particular department.
2. Technical knowledge should be given to the designated officer in the particular Domain so that if any cyber-attacks are committed then such officer is capable of stopping that cyber-attack.

The same question was asked by me to Mr. Abhishek Mishra cyber expert hailing from Delhi and taking matters of cyber-crimes in Delhi he pointed out that,

1. Mr. Abhishek pointed out that security agencies are efficient to deal with cybercrimes in relation to critical infrastructure in India.
2. Mr Abhishek pointed out about knox security system at hardware level that is provided at different Agencies specially the defense system which helps to deal with cyber-crime at critical infrastructure level.
3. Whenever critical infrastructure is hacked at different channels there are different stages so if one channel is hacked then there is scope for the other channel to be switched off.
4. Advanced technology is used under critical infrastructure so that cyber criminals cannot bypass that security.

Mr. Sachin Dedhia cyber expert also had the same opinion, that it is not easy to crack down the critical infrastructure, he stated that,

1. Mr. Sachin stated that, the critical infrastructure and the systems, whether it is of hardware and software level are self-owned and not from any third party so it becomes very difficult for the cybercriminals to attack the critical infrastructure.
2. He stated that multiple attempts are required to hit the critical infrastructure but it can be done by the cyber criminals.

3. He also pointed out about the knox software which are used by the critical infrastructure agencies to deal with cyber-attacks.
4. Critical infrastructure is having different channels and different stages and different networks so it becomes very difficult to attack the critical infrastructure, different stages are there, one has to bypass each and every stage so it helps to protect the other system

Mr Prem Sagar Gavli, one of the cyber experts practicing in Mumbai and Nagpur also had the same opinion but not in the concrete sense, he stated that,

1. He pointed out that Cyber experts are required in critical infrastructure Agencies and corporations.
2. Individual training of Cyber related crimes and cyber-attacks should be given at the local level to the uppermost level

Mr Snehal Vakilna well known cyber expert of Gujarat pointed out that, critical infrastructure needs different sets of people and intelligence at every level. He was of the opinion that, it cannot be by passed by the cyber criminals until and unless it lacks the required personnel and equipment's, he stated that,

1. He stated that critical infrastructure is a very important aspect of India and it should be protected from cyber criminals.
2. Cyber experts and domain related experts should be appointed in the critical infrastructure departments so that the cyber criminals cannot attack those agencies.

The following hypothesis is dis-proved through the empirical research conducted by the researcher with all relevant data supporting the hypothesis.

CHAPTER VIII
CONCLUSION, FINDINGS & SUGGESTIONS

8.1 CONCLUSION

"The Information Technology Act, 2000" passed in the year 2000 and now it's 2023, 23 years have passed since it was passed. Act provides for the laws relating to cyber-crime and intermediaries and other aspects of cyber-crime. As the current scenario is pretty much different as compared to the year 2000 the technological developments which has taken in these 23 years is un comparable to the year 2000. The types of cyber-crime committed by the cyber criminals has reached new heights. India is climbing the online ladder more quickly this year, presenting the second-largest web client base of a brazen 560 million users. Furthermore, with network protection being a $6.7 billion industry, there is a more noteworthy requirement for harsh and inflexible digital laws in India.

The attack on the cyber security is increasing day by day causing harm to companies and individuals. Moreover, the pandemic was vital to the growth of cyber-crime as for a period of 2 years most of the countries in the world were made to work from home and this made the cyber criminals to have an advantage of the situation to attack those who were unaware of the how cyber-crime is committed. Cybercrimes can be managed, but it takes the combined efforts of the government, Internet and network providers, middlemen like banks and retail establishments, and, most importantly, the customers. Online security and adaptability can only be attained via the wise efforts of these partners, who will be imprisoned under cyberspace legislation.

The types of cyber-crime have found new grounds as compared to the traditional methods adopted by the cyber criminals previously is not practiced by the cyber criminals now a days, they have found new innovative and simple methods to do cyber-crime. To name a few cybercrimes which are used to commit cyber-crime man made intelligence attacks, Insider threats, eavesdropping attacks DDos attacks, phishing, malware, logic bomb, spamming, cyber stalking, identity theft, credit and debit card fraud, social media hack, cyber terrorism.

The following cybercrimes have a negative impact on the society such as identity theft and privacy are comprised. The most important impact is the impact on the economy cyber-crime is becoming a economy if measured in terms of a country. Social life is also impacted as all the data is readily available to cyber criminals and individuals post each second of their life on social media which make the life of the cyber criminals pretty easier. National security is

also comprised the attacks on the critical infrastructure could cripple the country in the hands of the cyber criminals.

India is moving quickly up the digital ladder; this year, there were 560 million internet users in the country, ranking second in the world. In 2021, the pandemic will push this figure even higher, with projections of at least 600 million users[368]. Cyber security is the most important step that can put the cyber criminals to an end as it's the cyber security when the cyber security is unbreakable the cyber criminals will not be able to do anything to commit any cyber-crime. Hackers are always improving their skills and finding new ways to access new systems, despite the fact that cybersecurity is improving every day. This underlines the significance of both improved cybersecurity technology and robust cyberlaws. In order to lessen cybercrime and fraudster attempts, governments must also be aware of any cybersecurity holes and fix them immediately.

The legal framework in relation to the cyber-crime, cyber security , critical infrastructure, data protection, intermediaries is to be strengthened and is having few legislations and few are yet to implemented as they on the drafting stage to name a few "the Information Technology act 2000 and its amendment in 2008," cyber security policy which gave the insights on the cyber security plan to be implemented in India to curb the cyber-crime and but it's still on paper as compared to its implementation. "The Indian Computer Emergency Response" Team the ICERT is there to stop websites on the direction of the government and reduce obscenity. The national cyber security strategy 2020 seeks to examine various facets of cyber security under the umbrella of three pillars: securing the country's cyberspace; strengthening the structures, people, processes, and capabilities; and synchronizing the resources as well as cooperation and collaboration. The government is in the process of creating the policy and had requested opinions and ideas on several parts of the NCSS by January 10, 2020. The legal framework is gaining importance day by day as there is development also in the technological field and similarly it has to changed accordingly.

There are various challenges to cyber security such as cyber terrorism, digital data threat, cyber warfare, lack of co-ordination. The cyber security is a concern for national security instances have shown that national security can be comprised in the hands of cyber criminals. Few examples which show that national security was comprised the attacks on the electrical

[368]Available at https://www.statista.com/statistics/255146/number-of-internet-users-in-india/ accessed on 12 Aug 2023

grid in Mumbai, Aadhar software hacking, cyber-attack on cosmos bank, kundakulam power plant was hacked. The judicial perspective regarding the Information Technology act also had role in the changes of the IPC, use of electronic evidence in legal proceedings, Indian Evidence Act - admissibility of electronic records, authenticity certification, email, WhatsApp, call records, and use of electronic media in legal proceedings. The Banker's Book Evidence Act amendments. Due to which several landmark cases were decided all over India such as "UOI v. Shreya Singhal, Shamsher Singh Verma v. Haryana State, Syed Asifuddin and Others v. Andhra Pradesh State and Others, Nakul Bajaj & Ors. v. Christian Louboutin SAS, Avnish Bajaj v. Delhi State (NCT)."

In order to understand the legislative framework of other countries and to understand its application in their country. The countries like USA and Israel are far more ahead of India having separate acts for cyber security, critical infrastructure, data protection which India is still on the verge of drafting and no separate act for critical infrastructure which is the most important one in relation to national importance of a country. The privacy protection act of Israel and critical infrastructure act of the USA are the acts which India have to think to implement as early as possible as these two acts plays a important role in the national security. The amount of digital transactions in the nation has grown along with the frequency of banking scams. In fiscal year "2020–21," India experienced an average of 229 financial frauds each day, with fewer than 1% of the total amount recovered, according to data from "the Reserve Bank of India."

At a total cost of "Rs. 1.38 lakh crore," there were "83,638 incidences" of banking fraud in India in FY21. Only "Rs 1,031.31 crore" has been recovered thus far, according to information provided by the RBI in response to a Right to Information request made by India Today. Nonetheless, compared to FY20, when India experienced an average of 231 financial scams per day, the data for FY21 show a slight improvement. In FY 20 of 2016, "84,540 frauds" were reported. Cyber-crimes are those that use a computer or network as a route, source, instrument, target, or setting for a crime. Due to the increased popularity of e-commerce and e-transactions, economic crime has shifted online. Cybercrime is increasing globally, and recent years have seen a notable increase in cybercrime-related cases in India. According to a report from cyber security ventures USA, by 2025, cybercrime would cost the world "$10.5 trillion" each year.

Internet banking and mobile banking is gaining impetus as Indians are moving towards digitalization and technological changes at a rapid pace. The use of debit card, credit card, atm,

point of sale has increased considerably in these 5 years as compared to the 2000-2010. The most prominent cyber-crime in the banking sector in the current era are hacking, phishing, email- spoofing, spamming, atm skimming and point of sale, digital skimming this has made a huge on the financial sector. To avoid this the cyber security infrastructure in the financial sector needs to be strengthened as early as possible.

Some of the biggest threats to the financial sector are viruses, services provided by the third parties, spoofing, credential theft, identity theft. Individuals are not aware of how to tackle cyber-crime whom to approach what to do where to file complaint. All this also were the problems faced by the citizens as admitted by the police officials also that people do lack the awareness regarding cyber complaint and various grey areas of cyber-crime and cyber law is yet to be unearthed. After doing the empirical research on cyber-crime and cyber laws in India with reference to financial sector in Mumbai. The collected data was analysed through SPSS, frequency and percentage distribution was calculated. In which it was evident that from the general respondents till cyber experts agreed that, we need to amend "the Information Technology Act, 2000" as early as possible and people were aware but still, they were target of cyber criminals in Mumbai.

The researcher achieved most of the objectives of the research in relation to the **"Cyber-crime and cyber- laws in India: A study with special reference to financial sector in Mumbai."** The researcher studied the historical background of cyber law in India and evaluated the types of cyber-crimes in India similarly the legislative framework of cyber security was covered by the researcher, the judicial perspective towards protection and prevention of cyber-crime was studied and made a comparative study of international legislative framework of USA, Isreal and India to know about positives and negatives. Studied the nature of cyber-crime in financial sector and analysed how cyber-crimes affects the financial sector in Mumbai.

After analysis of the questionnaires and personal interviews of the experts it pointed out that Information Technology is inadequate to tackle cyber-crimes in spite of to counteract the threat of cybercrimes, provisions and essential adjustments can yet be made to the current laws. and the current cyber security mechanism in India is not capable to cater with the fast pace of developing technology at the hands of cyber criminals, that could affect India's vital infrastructure like "the defense sector, financial sector, the grid lines and the corporations."

The most common mistake done by the people is that they are unaware of the cybercrime. Awareness was the major reason behind the successful rate of the cyber criminals as cyber criminals used unawareness of the citizens to commit cyber-crime. While interviewing the cyber experts they suggested that, it's the awareness which will play a vital role in the future of the cyber-crime as awareness was lacking most of the time among the citizens and this made the cyber criminals access the phone, computer, emails of the citizens for the purpose of cyber-crime. Those who fell prey to the cyber criminals were lacking technical know how or we can say the basics of mobile and computing. Basic awareness was lacking and they fell prey to cyber criminals. As pointed by out the police officials the cyber criminals are not that much educated or technically strong to hack someone's phone or computer it's the system or we can say the method which they know to commit the crime. While interacting with the police officials they said that it's the people who are greedy, needy, cyber criminals tend to access the social media sites of the citizens also to know the whereabouts of the person who is being targeted. They lure them or offer discounts, premium or offer something like lottery in form of malicious link and steal their valuable information.

The financial sector is the most important part which the cyber criminals are targeting in order to get huge sum of financial gains. As pointed out by the cyber experts there are great chances that there could be financial war between a nation and cyber criminals. The responses from the financial sector proved to be the major finding as they pointed that there is lack of awareness among the individuals, the Information Technology act is not sufficient to curb cyber-crime and the most important part was that the cyber security infrastructure is not sufficient to curb cyber-crime in the financial sector. Cyber security infrastructure is the most important part in relation to curb cybercrime as pointed out by the respondents of the financial sector cyber security measures are in place it's the awareness relating to it is missing among the citizens.

In order to curb the cyber-crime, the authorities are taking steps, creating awareness also on national TV, radio. Social media, google is also creating awareness among the citizens in order to make them aware of the cybercrime. Awareness campaigns are being organized by the financial sectors banking institutions keep cyber surakhsha pakwada in order to give information relating to cyber-crime to its customers. The most widely used search engine in India Google corporation is also creating awareness through various advertisements on the national TV so that people are aware of the cyber criminals. True caller and various telecom

partners are coming together to curb cyber-crime in relation to spam calls which the cyber criminals use on daily basis. Spam calls are the most important part of cyber-crime as this helps the cyber criminals call numerous people in order to scam them. Awareness, some sort of technical know-how with vigilance regarding cyber-crime among the citizens is the key to curb cyber-crime.

8.2 FINDINGS:

The financial sector of Mumbai as suggested by Mr. Pankaj Bafna one of the best cyber experts in Mumbai said that it's the financial that will be hit hard by the cyber criminals. The general respondents also pointed out that there is need to look into the IT act 2000 as early as possible. The law faculties where also in the favour of changes in the cyber laws and in the financial sector. The financial sector questionnaire provided us with eye opening data they admitted that cyber security is vulnerable to cyber criminals. The advocates admitted that cyber law practice is something new to the law fraternity and there is huge scope for improvement. The police officials also mentioned that people lack awareness regarding cyber-crime and how to deal with them and police authorities also are not aware how to deal with cyber-crime cases. The following are the finding of the research as follows: -

- The Indian IT Act, 2000 needs to be amended to deal with the nuances of cybersecurity. The amendment of IT act will be helpful in cyber security lapses which is there in the financial sector. Cyber security infrastructure is the key towards to curb the cyber-crime in the financial sector. Special provisions in relation to the intermediaries so that third party can held liable as compared to the main recipient and the receiver. The parties involved in the transaction should be held liable.
- The Act needs to be future proofed so as to cover emerging technologies and the challenges it brings in its wake. The cyber criminals as pointed by the cyber experts are way ahead of the in relation to technology and methods used by them in order to commit cyber-crime. The act need to future proofed as technological advancements are happening on daily basis which is not covered by the current IT act. Future prospects of cyber-crime and its methods should be covered in the amended IT act.
- Eliminate "safe-harbor" provisions that exempt intermediaries from liability. The safe harbor provision should be eliminated so that the intermediaries can be held liable for the activities which are committed on their platforms. This will create a deterrent effect on the intermediaries as of now they are not held liable.

- Keep up with the agile cyber-space; fast track amendments and roll-outs. The legislature is required to be on toes in order to be on equal footing of the cyber criminals and amendments should made a quick pace as technology will change every fortnight.
- Empower CERT and enforce stricter and substantial penalties on defaulters. The computer emergency response team should be given more responsibilities and powers in order to facilitate smooth working. The penalties which are mentioned in the current Information Technology is nothing but peanuts in relation to the crime committed by the cyber criminals. Penalties should be in the lines of companies act in crores.
- Address privacy issues in the existing IT Act. Data privacy and privacy is gaining impetus in India as data will play a major role in the coming years. Selling of data of citizens in order to facilitate the working of cyber criminals. It is the most important problem which India is facing currently.
- Learn from data breach notification laws implemented by other countries and avoid superficial changes. Data breach by hackers such as linked, dominos, Air India, razorpay these data breaches leaked millions of data ordinary citizens on the internet. Hefty fine should be imposed on both the hacker and the firm which failed to stop the attack.
- More collaboration with private players and cybersecurity experts and not leaving amendments to bureaucrats. Cyber security infrastructure of the co-operative banks should be strengthened by involving private players which are having sufficient cyber security measures.
- Amend Act to introduce ODR (Online Dispute Resolution]. Online Dispute Resolution is the most important form of dispute resolution which is gaining grounds in India during the period of covid it's the online platform which gave relief to the many. Provision relating ODR should be brought into play.
- Akin to the RBI's mandate for a bank to report a breach within six hours, CERT needs to come up with the same guidelines for other institutions to enforce cyber vigilance.
- Data Protection Law. The most important law which is pending in the parliament for the past 10years. The data protection act will make the corporations liable in case of

data breach which they are responsible for storing and keeping safe. And similarly, the use of personal and non-personal data should be used.

- Satellite Broadband Policy. Satellite Broadband the emerging nature of internet service which might be available in selected countries in relation to these provisions should be introduced in the coming years.
- Online Gaming Regulator. The IT act 2000 is lacking the regulator in relation to gaming which is gaining impetus in India. The Gaming industry has become a million-dollar industry in India similarly on this note Regulator is required.
- Doctrine to govern cyberspace. If any discrepancy arises a doctrine will help to remove the doubts in relation to the particular dispute.
- Bringing in Law for Online gambling. A different law in relation to online gambling will be more useful as online gambling such as Dream 11 is a million-dollar industry which requires a regulator as well as particular provisions in relation to its functioning.
- Law and Policy for cryptocurrency. Cryptocurrency is not recognized by the government of India as well as RBI in relation to give importance to cryptocurrency a particular law will be more advantageous.
- Policy on appointing special Courts for Technology or cybercrime. Amendments in relation to special courts for technological crimes or crimes which are not ordinary in nature which requires knowledge of hacking, coding, programing should be introduced.
- AI & fintech Policy to be revisited to make it consumer centric. The law relating to artificial Intelligence should be taken into consideration as artificial intelligence is playing a important role in relation to cyber terrorism.
- The general respondent's data collected by the researcher showed that 49% of the respondents gave their responses and admitted that cyber law i.e., "the Information Technology Act, 2000" is not able to control the cyber-crimes in India.
- The cyber experts pointed out that, awareness is the major part where one gets scammed to the cyber criminals. And people are not aware of how deal with cyber criminals as they lure them to greed and play with their mental psychology. The experts pointed out that, financial sector will be hit by the cyber criminals in the coming future. As mentioned by Mr. Pankaj Bafna there could financially war by the cyber criminals in the coming future. The educated are more vulnerable to cyber

criminals as compared to the uneducated. The rural areas in Maharashtra and the people therein are more easy targets of cyber criminals as they lack the awareness required to stop the cyber-crime. The cyber experts admitted that, there is requirement to amend "the Information Technology Act, 2000" and special courts should be introduced with qualified judges having technical qualification to understand the nature of cyber-crime. The cyber experts pointed that the financial sector cyber security infrastructure is vulnerable to the cyber criminals but safe also if used with due care while performing financial transactions. Cyber experts pointed out educated people should be aware of the financial websites and the solution provided on those websites

- The cyber experts pointed that, the laws should be stricter but still up to the individual how much he or she is aware regarding the transactions he or she is performing.
- After interviewing the police officials at the Maharashtra cyber cell Police Inspector Prashant Sir, he mentioned that awareness is lacking among citizens all over Mumbai and Maharashtra. And he specially mentioned that police officials are also not aware of how to deal with cyber-crime and cyber awareness programs are needed to be given to the police officials. The time taken for a cyber-crime to be solved in Mumbai usually take 7 days minimum and it takes 72 hours to the parties to reply and he mentioned the time span is long just to reach to a solution. The most important part he covered that, usually people who lose in between 1000 to 5000 Rs. never reach to cyber police to solve the crime. Rural areas are more prone to cyber criminals as mentioned Mr. Prashant. He pointed that, awareness and proper grievance is the first step to reach a solution to solve cyber-crime. Mr Prashant pointed out that the time taken to solve the cyber case also depends on the nature, offence and its gravity having media coverage all this also are very important factor to solve the cyber-crime.

8.3 SUGGESTIONS:

The following are the suggestions after doing the empirical research in relation to cyber-crime and cyber laws in India with reference to financial sector in Mumbai. The suggestions are of different categories such as legal, financial, Regulatory, Security Mechanism, Surveillance, scams, matrimonial frauds that also leads to financial fraud, job scam, phishing scams which leads to financial scams, link related frauds that lead to financial scams, gift card phishing scams that also leads to financial scams, how to stay secure online moreover every scam leads to financial fraud.

8.3.1 LEGISLATIVE SUGGESTIONS

Amendment of Information Technology act, 2008 on a future oriented basis in a dynamic nature. As cyber criminals are fast paced, and the technology is changing on daily basis. The Information Technology act cannot be static and rigid the regulatory bodies should be in a position to amend or alter the law on case-to-case basis or under extreme urgencies.
Separate act for critical infrastructure like USA and Israel, as the critical infrastructure is one of the most importance aspect of the country, if it's under the attack by the cyber criminals can lead to huge damage on the economy and the people also. The recent attacks on the AIIMS, International Airport of Mumbai, Electrical Grids of Mumbai, banking bodies and data leak of defense information from WhatsApp to the neighboring countries is a huge task for India to tackle with.

Cyber security mechanism and a separate act for cyber security should be introduced at the earliest to cater to the attacks of cyber criminals on the financial sector. The RBI being the body which looks after the financial sector of India and other relevant bodies such Indian National security council, CERT-In are not that sufficient to tackle the cyber security breach by cyber criminals. A separate regulatory body of cyber security should be established just look after the breaches of financial emergency with topmost priority. Separate cyber courts should be established in each district depending upon the population of the district or city. And powers should be given to the high courts to establish cyber courts in the district with consultation of lower courts as this will help speedy trial and disposal of cases at the earliest. Courts with well-known facilities is the need of the hour in the districts of Maharashtra and Mumbai at the earliest.

The courts and the Judges should be well versed with the technical know-how of cyber related crimes its modus operandi and the technical aspect of the crime. The appointment of the judges should be made based on the technical knowledge and education such as B.SC in computers or M.SC in computers so that they understand the technical aspects related to the case or the crime. This will lead to understanding of the case to a great extent. Law relating to the Artificial intelligence should be given priority as this is next part of cyber-crime, which is being introduced to help the people, but it will create huge concern in the coming future. During

the research researcher came across various instances of cyber criminals using the artificial intelligence.

Strict Punishment should be introduced in relation to section 66C, 66D, 66B, 65, 67C, 66E, current punishment is for 3yrs and 2 lakhs fine and bailable in nature. The punishment should be increased to 7yrs and fine up to 20 lakhs and it should be made non bailable in nature. As per the words of Justice Vikram Nath of supreme court the cyber-crime portal should not be merely a complaint box. It should be made comprehensive and workable in nature as its inefficiency and non-working is not providing any fruits to the public for complaints and grievance's that could be solved.

8.3.2 ENFORCEMENT SUGGESTIONS

The cyber-crime portal which is just there to collect data and do nothing else and same was taken into consideration by the supreme court in one the proceedings. The portal should be made more user friendly and rather than collection of data it should provide with solutions to the person who is lodging the compliant. And the same complaint will work throughout the process, it can be showed to every authority involved in the process. Implementation of efficient cyber-crime portal is the need of the hour. Establishment of cyber police stations at all district level in Maharashtra and nearby cities. This will cater to the rising number of disputes arising out of cyber complaints. At present Maharashtra is only having 43 cyber police stations. The numbers are very low if compared with the population and number of complaints received on day-to-day basis. The training of the police officials in relation to the functioning and working of the cyber-crime, its implementation, application of law in relation to cyber-crime. As at present the police officials lack the required skill set required to tackle cases of cyber-crime.

The nodal agencies which look after cyber-crime in relation to the financial sector. In Maharashtra at present there are just 4 Nodal agencies which looks after financial crimes. Looking at the geographical extent of Maharashtra and specially Mumbai more nodal agencies are required to curb the cyber crime in relation to financial sector. As nodal agencies are the most important body which is to be contacted in case of financial fraud. The cyber-crime units in Mumbai is around 95, it should be increased to 200 or 250 this will make the situation more advantageous for the person who has suffered cyber-crime. As less number of cyber units in

the city of Mumbai wont cater to the problems of the large number of people staying in Mumbai. The awareness of cyber crime and cyber security is lacking among the citizens and this awareness can be introduced at an early stage. If syllabus is tweaked and schools should introduce the subject of cyber crimes and cyber security in their curriculum. As UGC also have suggested to include topics related to cyber crime in each institution. Knowledge of cyber crime at an early stage can provide great impetus to curb cyber-crime.

The advocates and the judges in most of the courts in Maharashtra are lacking the required knowledge for the implementation of Information Technology and its procedural aspects. During my research the responses which I received clearly stated that advocates and judges are lacking the required knowledge for the of IT act 2000. Awareness regarding the Information technology act among the advocates should be introduced. Technical sessions should be introduced in courts and conferences delivering lectures on the procedural aspects of the Information Technology act 2000.

8.3.3 FINANCIAL SUGGESTIONS

Cyber security should be separated from the Information Technology act and a separate act should be introduced to cater with the problems of the cyber security as Information Technology act is not sufficient to curb the cyber-crime. A separate act will do wonders in relation to cyber security mechanism, methods, approach and can give focus on the financial part of the crime in general as compared to the Information Technology act which just gave us 4 sections to deal with the cyber security. Awareness Programs should be introduced by the financial authorities as this will help the uneducated and the people lacking basic knowledge regarding the cyber-crime to deal with it on the first stage of the crime. Government bodies are doing their part as to provide awareness but it's the other authorities should come forward and guide the locals about the cyber security structure and methods to be adopted to be safe online and offline from the cyber criminals.

As per the research and the respondents' answers through questionnaires a strong password should be made mandatory for all the financial transactions. So that it becomes difficult for the cyber criminals to crack the password and enter the system easily. Two step verifications should be made compulsories for all financial transaction's as it will reduce the risk of losing the money at the first stage of the OTP verification, the person who is being

cheated can have one more verification remaining in which he can study and research what is going on, in the transaction which he or she is doing. Two step verification plays an important role in the protection of finances one is having.

Cyber security provisions such as section 43, section 66, section 69 and section 70 should be given more dynamic form if new law or act is not introduced in relation to cyber security. As this will help in catering to the cyber-crime at a speedier pace and catch hold the cyber-criminal at the earliest. Special appointment of officers should be made which is specifically for the purpose of cyber-crime in relation to the financial crime and cyber security breach of any kind. The following officer will not only make the life easier of the person affected and it will reduce the gap between the crime and transfer of money to different accounts. The nodal officer appointed for banks is not that effective as compared a individual appointed for cyber-crime and cyber security. The triparty system should be stopped as if one gets affected, he or she should have direct access to the bank employees or representatives so that, the employee can directly access the account or the system of the affected person and stop the transaction. This will reduce the time of money being transferred to multiple accounts.

8.3.4 MISCELLANEOUS SUGGESTIONS

8.3.4.1 Matrimonial Frauds

Recognize of people who ask for money. Do not pay anything for visa purpose or other reason. It is not safe to discuss about your financial matters with someone you just met. People tend to target those who are divorced, widow and lure them by giving assurance of gifts or money and people tend to fall prey to them. Scanning the profiles carefully is a step can be followed to fight against matrimonial frauds one can tell a lot about a person from their online profile and the language used by the person, grammar the typing, grammatical mistakes and the most important the way of chatting. The usage of social media to verify and match them against the details in the matrimony website as most of the cyber criminals tend to use the matrimonial websites to gain advantage of widows, depressed women. In order to be safe and matrimonial frauds one can also use the method of using different personal email id for registration for chatting and communication. Reporting the profile is also one of the ways to safeguard oneself from matrimonial frauds as fake profiles tend to harass the person online. One should try to avoid reveal personal information to the person, one should be careful not to

discuss personal life/ details on matrimonial websites. Never meet the person alone, meet them in public places and also keep your friends and family members informed about it. To safeguard oneself, avoid sharing photographs if you are asked to even if you are interested in the person you are talking to. Online communication is different from face-to-face communication. Never hurry into a relationship or feel compelled to meet them immediately away. In order to catch the fraudster, one should save the chat and email communication for future reference, this can be used as evidence if any fraud activity takes place. Report Cyber Crime on Helpline 1930 OR https://cybercrime.gov.in @MumbaiPolice https://mumbaipolice.gov.in.

8.3.4.2 Gift Card Phishing Scams

In gift card scams attackers rely on impersonation and social engineering to engage in conversation with victims. After a few exchanges, victims are convincing to send money. using gift cards rather than through wire transfers. The attackers leverage authority and urgency in their requests and will frequently impersonate high-level executives, Deans, or Chairs of departments as part of the scam.

"Are you available? No calls text only 9513072xxx"

"I'm in a meeting and need help getting some Amazing Gift Cards"

If you think, an email is a phish report it immediately you could save someone else from becoming a victim. Many of receive email which seems off at that time Contact the alleged sender in a separate email or call them to ask if they emailed you. Don't use any information provided in the email.

8.3.4.3 Phishing Scams

Never open files or links in emails, messages, social media sites, etc. that you are not familiar with. Phishing/Suspicious link tends to route to different sites which are purposely made to collect sensitive information of the individual. In order to avoid phishing scams one should keep your password private at all times. Sharing of the passwords is the most common mistakes done by many people. The password should not be disclosed to anyone specially on calls or messages. One should watch out for emails requesting login credentials or other private information. Suspicious mails which tend to collect login credentials are used by the cyber criminals to collect data such as credit card, debit card, passwords etc. Avoid falling for alluring

advertisements, etc. mails, links, pdf which gives advertisement of easy money or discounts are not to be clicked on.

8.3.4.4 Part Time Job Scam

Fraudsters send phone emails and messages proposing part-time work while posing as representatives of well-known businesses. Once the victim is persuaded, the con artist demands payment in place of training, registration fees, etc. Individuals should refrain from clicking on unverified links, no matter how tempting they look, they are made in such a way that the person will click on that link or poster. Be cautious before doing any financial transaction with unknown persons. One should verify the credentials with whom one is doing the transactions.

8.3.4.5 What to Do If Your Mobile Phone Is Lost/Stolen

Firstly, report to your bank and police immediately that your phone is stolen or lost. Block the stolen sim card and get replacement of the sim card. As the stolen sim card cannot be used by the person who is in the possession of the card. One can track the phone if he is having tracking details. Note the IMEI number of your mobile phone to trace mobile phone if its stolen. Try to locate through GPS as GPS tracking will be made available in different login credentials. Change your passwords of financial apps immediately so that the person who is possession of the phone is will not be able to access those apps.

8.3.4.6 Important Check List Before Calling Cyber Helpline 1930

- Mobile number of the complainant.
- Name of the bank wallet/merchant from which the amount is debited.
- Account no./Wallet merchant, UPI ID from which the amount is debited.
- Transaction ID (12 Digit UTR Number)
- Transaction Date.
- Debit/Credit Card number in case of fraud using card credentials
- Screenshots of transaction or any other image relate to the fraud (Filed by Citizen)

8.3.4.7 Stay Secure Online

Make your passwords complex and never share them. Activate 2 Step Factor Authentication on social media. Check your privacy settings on social networking sites. Do not click on random Links or download unknown files. Always keep profile locked and private. Clear Cookies & Delete Browsing History regularly. Do not accept request from strangers. Do not share/download obscene video, images etc. Always check authenticity of app. before downloading

8.3.4.8 Identity Theft/Protect Your Personal Data

`Social networking sites' personal information posting and publication restrictions. Examine all of your social media and online accounts for signs of fraud. Monitor your financial accounts for suspicious activity on a regular basis. Beware of onlookers when using your credit/debit card and entering your PIN number. Make use of the security tools offered by all websites. Only transact with reputable businesses and websites. Send documents with password protection. Do online shopping only through official sites that uses secure payments gateway Always read and check privacy policies Take immediate action if you think your personal information has been misused.

8.3.4.9 Filing of Cyber Complaint

An apt narration of facts, as-they-happened. Prepare all the relevant annexures (mostly compromises of screenshots of chats on telegram and WhatsApp). Relevant details of accused persons, such as mobile number, email, name, address (latter details if available) and the VPA (Virtual Payment Address) of the accused. How were funds transferred to the accused (Transaction IDs). Via Bank Account: Through IMPS/NEFT/RTGS. Via Wallet: Through Phone Pe, Paytm, Amazon Pay. Via UPI: Through Google Pay. Bank statement in which the debit transaction was undertaken. Prepare the narration and upload on National Cybercrime Reporting Portal of India at https://cybercrime.gov.in Details of the Grievance Officer of the Merchant Bank/ Wallet/ UPI. Sharing the complaint with the relevant officer. Raising the dispute on the Dispute Redressal Mechanism of “the National Payment Corporation of India” at UPI Dispute Redressal Mechanism – “NPCI https://www.npci.org.in”. Good to remember that in all likelihood the cyber-complaint will be dealt with the address of the complainant, so

do have some address proof in the complainant. It helps to also report the complaint on 1930 helpline within 24-48 hours.

The following scams are the most common scams used by the cyber criminals in order to commit cyber-crime in most of the places in the country. The fresh scams such as the KYC fraud and click on link fraud is gaining popularity among the cyber criminals. If one follows the suggestions as provided there are great chances that the person won't fall for the cyber criminal's tricks as he would be aware of the tactics employed by the him.

Bibliography

A. Books

- Dr. Pramod Singh, *Laws on cybercrime*, 03, Book Enclave, 2007
- George Kostopoulos, *Cyberspace & cyber security*, CRC press Taylor & Francis Group, 2nd ed, 2018
- Babak Akhgar et al. "combatting *cyber-crime and cyber terrorism challenges, trends and priorities"* Springer, Advanced Sciences and Technologies for Security Applications /10.1007/978-3-319-38930-1/ ISSN 2363-9466
- Kenneth J Knapp, "Cyber *Security and Global Information Assurance: Threat Analysis and Response Solutions*" Information Science Reference / 978-1-60566-326-5 / 978-1-60566-327-2
- Suvarna shirke et al. "cyber security and laws" Tech knowledge publications, 2019, Mumbai.
- Henry Prunckun, "cyber weaponry issue and implications of digital arms" Advanced Sciences and Technologies for Security Applications, Springer, 978-3-319-74107-9, 10.1007/978-3-319-74107-9
- Amos N Guiora, "cyber security -Geopolitics, law and policy", Routledge 2017, 978-1-498-72911-6
- M. Gercke, "Understanding cybercrime: a guide for developing countries," International Telecommunication Union (Draft), vol. 89, p. 93, 2011
- Kharouni, L. (2012). Automating Online Banking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit Feature (Rep.).
- Hamid Jahankhani, Cyber Criminology, Springer, ISSN 1613-5113 ISSN 2363-9466 (electronic) Advanced Sciences and Technologies for Security Applications,2018.
- Dr. A Sukumar, *Cyber law*, 1st ed, ISBN: 978-93-5321-921-5, 2018
- Deepti Chopra and Keith Merrill, Cyber Cops, Cyber Criminals and the Internet, I.K. International Pvt. Ltd., 2012, New Delhi.
- Dr. R. K. Tewari and others, Computer Crime and Computer Forensics, Select Pub., Delhi, 2017
- Dr. Farooq Ahmad, Cyber Law in India - Law on the Internet, Pioneer Books, New Delhi
- R. C. Mishra, Cyber Crime impacts in the new millennium, 1st ed., Authorspress 2014

- S. V. Joga Rao, Law of Cyber Crimes and Information ‘Technology Law, Wadha & Co., 2004
- Joga Rao S.V. Law of Cyber Crimes and Information Technology Law, Wadhwa and Company, Nagpur, 2004.
- Pradhan R.K. Cyber Crime and Cyber Terrorism, Mangalam Publications, Delhi, 2010.
- Sharma Vakul, Information Technology Law and Practice, 4 ed. Universal Law Publishing, 2015
- Pillai, K.N., Principles of Criminology, T.L.L. 2013.
- Fatima Talat. *Cyber Crimes*, 2 Ed., Eastern Book Company, Lucknow, 2016.
- Bivas Chattergee, Cyber Adjudication: Alternative Remedy, Asia law House Publishing, 2015
- Bivas Chattergee, Law relating to Mobiles, Asia law House Publishing, 2015
- Anthony Reyes et al., Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, 2007
- Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes, 2012
- Brett Shavers, Cybercrime Investigation Case Studies: An Excerpt from Placing the Suspect Behind the Keyboard, 2012
- Debarati Halder, K Jaishankar. Cybercrime: An Indian Perspective (Universal Law Publishing, 2010)
- Vakul Sharma. Cyberlaw: The Indian Perspective (Universal Law Publishing, 2019).
- K Jaishankar. Cyber Crime and Digital Evidence: Materials and Cases (Taylor & Francis, 2017)
- Bimal N Patel. Cyber Crime: Law and Practice (Eastern Book Company, 2019).
- K Jaishankar. Cyber Crimes: Detective's Investigative Guide to Online Crimes (CRC Press, 2021).
- Barkha and U. Ram Mohan, Cyber Laws and Crimes, 3rd Edition, Delhi Law House
- Dr. Prasanna A., “Cyber Crimes: Laws and Practice”, IMG, Thiruvananthapuram.
- Kumar Shiva V, “Cyber Crime Prevention and Detection”, Andhra Pradesh Police Academy 20153

- Nagpal Rohas, “Cyber Crime & Digital Evidence –Indian Perspective”; Real World Cyber Crime Cases, Asian School of Cyber Crime 2010
- Singh Talwant, “Cyber Law & Information Technology”, New Delhi, India, 2011
- Gibson, W. (2019). Neuromancer (1984). In Crime and Media (pp. 86-94). Routledge.
- Gaur, L. (2022). Evolution of Cyber Laws in India. Jus Corpus LJ, 3, 670.
- Maneela. (2014). Cyber Crimes: The Indian Legal Scenario. US-China L. Rev., 11, 570.
- Chatterjee, S., & Kar, A. K. (2018). Regulation and governance of the Internet of Things in India. Digital Policy, Regulation and Governance, 20(5), 399-412.

B. Articles/Research Papers

- Proof point, “a state-of-the-art annual report on phishing”, 2020
- Risk based security,” Q3 report 2020 data breach quick view” 2020
- Acharya, Suman & Sujata. "*Impact of cyber Attacks on banking institutions in India: A study with special of safety mechanisms and preventive measures*." PalArch's Journal of Archaeology of Egypt/Egyptology 17.6 (2020): 4656-4670.
- Jyoti, Shirish Mishra & Subodh Kesharwani , “*Cybercrime: An Emerging Threat to Banks and NBFCs”,* 2 scholastic seed 15
- Harshita, “Cybercrime in Banking sector”, International Journal of Research Granthaalayah, Vol 7 issue 1 (2019) 148-161
- S. Kumudha and Aswathy Rajan, “*A Critical Analysis of Cyber Phishing and its Impact on Banking Sector*”, International Journal of Pure and Applied Mathematics Vol 119 No. 17 (2019) 1557- 1568
- Morya, Kishore K., and Mahesh Singh. "*Study of Latest Cybersecurity Threats to IT/OT and their Impact on e-Governance in India*", International Journal on Emerging Technologies 11(2): 939-947(2020).
- Virmani , Kaushik & Mathur (2020) Analysis of cyber-attacks and security intelligence: Identity theft. Indian Journal of Science and Technology 13(25): 2529-2536 https://doi.org/ 10.17485/IJST/v13i25.580.

- Rajasekharaiah, K. M., Chhaya & E. Sudarshan. "*Cyber Security Challenges and its Emerging Trends on Latest Technologies*." IOP Conference Series: Materials Science and Engineering. Vol. 981. No. 2. IOP Publishing, 2020
- Dr. Sudhir Sharma, "Cyber Security: A Legal Perspective", IJCIS. ISSN 0974-2247 Volume 9, Number 1 (2017), pp. 1-11
- Rao, Yerra Shankar, et al. "Digital Crime and its Impact in Present Society." International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol 8 Issue 1, 1-6
- Singh, Tejinder, and Nitin Pathak. "Emerging role of artificial intelligence in Indian banking sector." journal of critical reviews ISSN- 2394-5125 VOL 7, ISSUE 16, 2020 1370-1373
- Kashyap, Sunidhi, and Kuldeep Chand. "Cyber Security and Safe Computing: Need of an Hour which needs to be solved." The International journal of analytical and experimental modal analysis vol 12 issue 9 September 2020
- Prashant, Sodhi, Trivedi, Sanjeev , Analyzing the Awareness of Cyber Crime and Designing a Relevant Framework with Respect to Cyber Warfare: An Empirical Study, International Journal of Mechanical Engineering and Technology 9(2), 2018, pp. 110–124
- Neeti Gupta, "*Freedom of speech Restored- 66A of IT act Struck down"* Indian Journal of Applied Research ISSN NO 2249-555X, vol 5 issue 05th May 2015
- International Journal of Engineering Research & Technology (IJERT), Digital Crime and its Impact in Present Society
- Instituted by section 36 of the Information Technology (Amendment) Act 2008 (10 of 2009), w.e.f. 27 October
  2009, http://164.100.47.193/BillsPDFFiles/Notification/2006-96-gaz.pdf
- Report of the committee of experts on Amendments to IT Act 2000
- The committee of experts proposed to insert a new section, viz. 43(2) in the then Information Technology Act, 2000.
- The committee of experts proposed to insert a new section, viz. 67(2) in the then Information Technology Act, 2000
- Entries 1 and 2, List II, Seventh Schedule, Constitution of India.
- Cyber Security, Press Information Bureau, Government of India, December

- 52nd Report of the standing committee on IT on Cybercrime, Cyber security and Right to Privacy, February 2014.
- Pg. 125, Justice Srikrishna Committee Report on data protection: Security of the State,
- Pg. 124, Justice Srikrishna Committee Report on data protection: Security of the State,
- Indian Cyber Crime Coordination Centre (I4C) – A 7-Pronged Scheme to Fight Cyber Crime, Press Information Bureau, Government of India, July
- O.-e. I. E. G. o. Cybercrime, "Comprehensive Study on Cyber Crime," UNODC2013.
- Apoorva Bhangla and Jahanvi Tuli, A Study on Cyber Crime and its Legal Framework in India, 4 (2) IJLMH Page 493 - 504 (2021)
- S Kalpana," Cyber Crime: A Growing Threat to Indian E-Banking Sector" Journal of Emerging Technologies and Innovative Research (JETIR), December 2020, Volume 7, Issue 12,964-969
- Net Losses: Estimating the Global Cost of Cybercrime (Rep.). (2019). Intel Security
- Breaux, T. D, A distributed requirements management framework for legal compliance and accountability. Computers & Security, 28(1–2), 8–17.2009
- Brenner S. W. (et al), Approaches to Cyber Crime, Journal of High Technology Law, Vol. IV, 2004.
- Mali Prashant. Electronic Evidence and Cyber law, *CSI Communications*, 2012.
- Conway M. What is Cyberterrorism? Current History, Vol. 2, 2002
- Sarmah, Animesh, Roshmi Sarmah, and Amlan Jyoti Baruah. "A brief study on cyber-crime and cyber laws of India." International Research Journal of Engineering and Technology (IRJET) 4.6 (2017): 1633-1640.
- Ajayi, Emmanuel Femi Gbenga. "Challenges to enforcement of cyber-crimes laws and policy." Journal of Internet and Information Systems 6.1 (2016): 1-12.
- Gupta, Ruchi, Shilpi Gupta, and Clement Chiahemba M. Ajekwe. "Electronic Banking Frauds: The Case of India." Theory and Practice of Illegitimate Finance. IGI Global, 2023. 166-183.
- Soni, R. R., and Soni Neena. "An investigative study of banking cyber frauds with special reference to private and public sector banks." Research Journal of Management Sciences
- Boateng and Amanor (2014); "Phishing, Smishing & Vishing: An Assessment of Threats against Mobile Devices", Vol. 5, April 2014, pp.297-307

- Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.

- Goyal Mohit (2012); “Ethics and Cyber Crime in India”, International Journal of Engineering and Management Research, Vol. 2, Issue-1.

- Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on cyber crime and cyber laws of India. International Research Journal of Engineering and Technology (IRJET), 4(6), 1633-1640.

- Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013, September). A survey of cyber crime in India. In 2013 15th international conference on advanced computing technologies (ICACT) (pp. 1-6). IEEE

C. Acts

- The Information Technology Act of 2000
- The Information Technology Act of 2008(Amendment)
- Indian Penal Code 1860
- National cyber security policy 2013
- Indian Telegraph Act, 1855.
- National Cyber Security Strategy 2020
- The Bankers' Books Evidence Act of 1891
- Computer fraud and abuse are prohibited under the Computer Fraud and Abuse Act (CFAA)
- The Critical Infrastructure Information Act of 2002 (CII Act)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Gramm-Leach-Bliley Act
- The Electronic Communications Privacy Act (ECPA) of 1986
- Banking Regulation Act, 1949
- Indian Evidence Act, 1872
- Criminal Procedure code, 1973
- Civil Procedure code, 1908
- Indian Constitution, 1950

D. Webliography

- https://www.gartner.com/en/documents/3889055

- https://www.cybintsolutions.com/cyber-security-facts-stats
- https://enterprise.verizon.com/resources/executivebriefs/2020-dbir-executive-brief.pdf
- cmagazine.com/video-300-billion-passwords-by-2020-report-predicts/article/634848
- Kaspersky Security Bulletin 2020. Statistics
- https://www.htsyndication.com/ht-mumbai/article/beware%2C-city-recorded-more-cybercrimes-in-2020%3A-data/48244555
- Steve Morgan, "*Cybercrime to Cost the World $10.5 Trillion Annually By 2025*", Sausalito, Calif. Nov. 13, 2020 PRNewswire Cyber security ventures
- Regina Mihindkulasuriya , "*If cybercrime were a country, its economy would be bigger than India's, says US firm's report",* The Print Tech edition November 2020 7:30Pm IST.
- https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html (12 Nov 2019) dated 20 oct 2020 3:31pm.
- Robert Birtstone, "How cyber attackers are coming after in 2021", The Register, www.theregister.com/2020/12/17/attackers_are_coming_in_2021 December 18th 9:15 Pm
- Money control, "Apple *supplier Foxconn suffers ransomware attack, hackers demand $34 million in bitcoin",* Money control Technology https://www.moneycontrol.com/news/technology/apple-supplier-foxconn-suffers-ransomware-attack-hackers-demand-34-million-in-bitcoin-6206791.html 18th December 9:28Pm
- Times now News, "Credit, *debit card data of over 70 lakh Indians leaked online*", Times now news Business Industry https://www.timesnownews.com/business-economy/industry/article/credit-debit-card-data-of-over-70-lakh-indians-leaked-online/693288 December 9:40Pm
- CISO.in, "India approves game-changing framework against cyber threats", CISO Latest security IT news. https://ciso.economictimes.indiatimes.com/news/india-approves-game-changing-framework-against-cyber-threats 18th December 2020 9:53 Pm
- Vallabh Ozarker, "*Cybercrime detection in Mumbai is just 7%*", Mumbai Mirror 20th December 2020 https://mumbaimirror.indiatimes.com/mumbai/other/7-per-cent-thats-it/articleshow/79817972 21st December 2020 8:34Pm

- Hindustan Times Tech, "Hackers continue targeting remote employees in India, 36mn attacks reported till Nov", Hindustan Times Tech 20 December 2020 https://tech.hindustantimes.com/tech/news/hackers-continue-targeting-remote-employees-in-india-36mn-attacks-reported-till-nov- 8:41pm 21st December 2020
- Ajay Sarangam, "cyber security challenges In India", Jigsawacademy September 2020 https://www.jsa.com/cyber-security-challenges-in-india/ 8:54pm 21 st December 2020
- Carin Smith, "Watch *out for these financial crimes threats in 2021",* Fin 24, https://www.news24.com/fin24/companies/ict/watch-out-for-these-financial-cybercrime-threats-in-2021-20201231 22 Feb 2021 5: 28pm
- Chandra Shrikanth, "Personal *Data Protection bill/ Hackers having Field day as centre ditheres : Justice BN SriKrishna",* Money control, May 25, 2021 at 6:31am
- News18 Technology, "How *critical infrastructure cyber-attacks can change the way we live",* New18, May 22, 2021 at 5: 40 pm
- Jitesh Vachhatani, "Air *India data of 45 lakh passengers including credit cards leaked in massive breach",* Republicworld , May 21, 2021 at 11: 23pm
- HT TECH, "59*% of Indian Adults fell prey to cybercrime in the past 12 Months",* Hindustan times 19April 2021 at 9:50am
- Zee News Tech, "cybercrimes *at its peak New techniques used for financial fraud",* Zee news April 06 2021 at 11:23 pm
- The Mint Tech, "*Whatsapp new privacy policy 'exploitative and exclusionary CCI orders detailed probe",* Mint News 24 March 2021 10:50am
- Bloomberg, "India *plans a new national strategy on cybersecurity amid china hacking concerns",* Mint Tech 08 March 2021 09:54 am
- HT TECH, "Cyber threats in online education sector increased by 60% in 2020", Hindustan times 14 Feb 2021 at 5:46pm
- Express new service "Bank *swipe machines emerge as latest tool of fraud for cyber criminals in Mumbai",* The Indian Express June 25, 2021 at 7:04 am
- Shubhajit Roy, "*India in Tier 3 as cyberpower : IISS",* The Indian Express June 28 2021 at 7:20 am
- Sarthak Dogra, "*Data of over 700 million LinkedIn users exposed, it includes numbers, addresses and salary details",* India Today June 29 2021 at 12:25 pm
- India Tv, "*SBI OTP scam: Chinese hackers targeting state bank of India users offering free gifts",* India Tv News, July 08 2021 at 12:08 Pm

- https://indianexpress.com/article/india/pegasus-panel-to-probe-spying-charges-submits-its-report-to-sc
- https://indianexpress.com/article/cities/mumbai/mumbai-64-year-old-actress-falls-for-airtel-kyc-cyber-fraud-loses-rs-1-48-lakh
- https://www.moneycontrol.com/news/technology/indian-oil-companies-suffered-3-6-lakh-cyberattacks-in-six-months
- https://www.hindustantimes.com/cities/lucknow-news/cyber-fraud-case-arrest-of-wb-man-exposes-3-000-cr-online-job-racket
- https://www.business-standard.com/article/companies/hackers-steal-rs-7-3-cr-in-831-transactions-over-three-months-from-razorpay
- https://www.deccanchronicle.com/nation/crime/050522/hackers-prey-on-coop-banks-with-cheap-security-software-police
- https://timesofindia.indiatimes.com/city/nagpur/digital-payment-frauds-will-continue-unless-second-half-of-process-is-streamlined
- https://www.deccanchronicle.com/amp/nation/crime/160622/cyber-fraud-cloned-fingerprints-7-arrested-for-fraudulent-withdrawal
- https://indianexpress.com/article/cities/delhi/new-headache-for-cops-cyber-criminals-buying-personal-data-in-bulk
- https://www.hindustantimes.com/cities/mumbai-news/accounts-of-bank-in-thane-hacked-2-59cr-stolen
- https://www.soolegal.com/news/cybersecurity-india-received-sc-hacking-cyber-crimes-data
- https://www.news18.com/news/india/high-level-probe-against-army-officials-over-cyber-security-breach-on-whatsapp
- https://www.appknox.com/blog/cybersecurity-laws-in-india
- https://www.google.com/amp/s/www.jigsawacademy.com/blogs/cyber-security/types-of-cyber-crime
- https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy
- https://www.dailyexcelsior.com/impact-of-cyber-crimes-on-indian-economy
- https://www.mondaq.com/Guides/Results/16/100/all/1/India-Cybersecurity-Legal-framework
- https://www.jigsawacademy.com/cyber-security-in-india-are-we-doing-it-right

- https://www.financialexpress.com/defence/indias-tryst-with-a-new-national-cyber-security-policy-heres-what-we-need/2304053
- https://www.jigsawacademy.com/blogs/cyber-security/challenges-of-cyber-security
- https://blog.forumias.com/answereddiscuss-various-threats-and-challenges-to-cyber-security-in-india-what-initiatives-are-being-taken-by-the-government-to-enhance-cyber-security-in-india
- https://www.gatewayhouse.in/cyber-attacks-on-critical-infrastructure-is-india-ready
- https://theprint.in/opinion/how-chinese-cyber-attacks-mumbai-blackout-depict-a-new-era-of-low-cost-high-tech-warfare/614892
- www.businesstoday.in/latest/economy-politics/story/cyber-attack-from-china-behind-mumbai-power-outage-in-2020-289648-2021-03-01
- https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector
- https://www.indiatoday.in/india/story/cyber-attacks-rising-in-india-cert-in-alerts-to-over-700-entities-govt-in-lok-sabha-1833783-2021-07-28
- https://scroll.in/article/943954/what-happened-when-the-kudankulam-nuclear-plant-was-hacked-and-what-real-danger-did-it-pose
- https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones
- https://www.republicworld.com/india-news/general-news/cowin-app-hacking-reports-rise-in-indore-madhya-pradesh-police-launches-probe.html
- *Centre to revamp IT Act*, the Hindu, 26 February 2020, https://www.thehindu.com/business/Industry/centre-to-revamp-it-act/article30925140.ece
- http://kanoon.nearlaw.com/2017/10/28/information-technology-act-2000
- https://www.toppr.com/guides/business-laws-cs/cyber-laws/information-technology-act-2000
- https://www.vedantu.com/commerce/information-technology-act-2000
- https://www.legalserviceindia.com/legal/article-836-cyber-law-in-india-it-act-2000.html
- https://www.meity.gov.in/content/information-technology-act-2000

- https://timesofindia.indiatimes.com/india/supreme-court-strikes-down-section-66a-of-it-act-which-allowed-arrests-for-objectionable-content-online/articleshow/46672244
- https://www.drishtiias.com/daily-updates/daily-news-analysis/section-66a-of-the-it-act
- https://www.mondaq.com/india/telecoms-mobile-cable-communications/225328/intermediaries-under-the-information-technology-amendment-act-2008
- https://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy
- https://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008
- Procedure for blocking of websites under the Information Technology Act 2000, MeitY, https://meity.gov.in/content/it-act-notification-no-181
- Shreya Singhal vs. Union of India, (2015) 5 SC1, https://meity.gov.in/writereaddata/files/Honorable-Supreme-Court-order-dated-24th-March%202015.pdf
- Cyber Swachhta Kendra, https://www.cyberswachhtakendra.gov.in
- https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship
- *MHA's snooping order challenged in Supreme Court,* The Economic Times, 24 December 2018, https://economictimes.indiatimes.com/news/politics-and-nation/mhas-snooping-order-challenged-in-supreme-court/articleshow/67232730.cms?from=mdr
- *India's new Defence Cyber Agency*, Medianama, 15 May 2019, https://www.medianama.com/2019/05/223-indias-new-defence-cyber-agency-nidhi-singh-ccg-nlud
- https://www.mondaq.com/india/privacy-protection/257328/an-overview-of-cyber-laws-vs-cyber-crimes-in-indian-perspective
- https://corporate.cyrilamarchandblogs.com/2021/01/supreme-court-on-the-admissibility-of-electronic-evidence-under-section-65b-of-the-evidence-act/
- https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece

- https://bnwjournal.com/2020/07/17/analysis-cbi-v-arif-azim/
- https://www.lawyered.in/legal-disrupt/articles/diving-information-technology-act-2000-salient-features-and-2008-amendments-rashi-suri
- meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf.
- https://www.loc.gov/item/global-legal-monitor/2020-03-18/israel-emergency-regulations-authorize-digital-surveillance-of-coronavirus-patients-and-persons-subjected-to-home-isolation/
- https://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page
- https://www.loc.gov/item/global-legal-monitor/2007-12-02/israel-new-copyright-law
- https://www.paisabazaar.com/banking/internet-banking-e-banking/
- https://www.icicibank.com/Personal-Banking/insta-banking/internet-banking/online-banking-features.page
- https://corporatefinanceinstitute.com/resources/knowledge/finance/mobile-banking
- https://worldline.com/content/dam/worldline/documents/india/documents/worldline-india-digital-payments-report-q1-2021.pdf
- https://www.bankrate.com/banking/what-is-atm-skimming
- https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security
- https://www.blueliv.com/cyber-security-and-cyber-threat-intelligence-blog-blueliv/threat-intelligence/the-10-biggest-cyber-threats-facing-the-financial-services-industry

E. Newspaper Articles

- https://www.hindustantimes.com/cities/mumbai-news/mumbai-ranks-third-in-country-in-cybercrimes-in-2020.
- https://timesofindia.indiatimes.com/india/need-surveillance-reform-privacy-law-cyber-experts/articleshow 26 oct 2020 12:37pm.
- Bharat Panchal Cheif Risk officer, *getting cyber defenses ready,* Financial express/ inancialexpress.com/opinion/getting-cyber-defences-ready-india-needs-a-robust-cybersecurity-policy/2077314/ 15 December 2020 10:17am.

- Satya Prakash, "Information Technology legislation falls far Short" The Tribune January 2020
- Times Now, *"Facilitate academic fraternity to work on cyber security, awareness measures: UGC tells varsities"* Times Now, Education news. 03rd December 2020.
- ETNOW NEW.COM, "*Chinese launch covert cyber-attacks on India: Millions of online shoppers targeted", ET now digital 19*Dec 2020
- NDTV, "*62% Of Cybercrime Complaints in 2020 Linked to Financial Frauds: Delhi Police",* Press Trust of India 30 December 2020.
- News18 India, "*Cyber Frauds are Calling Up UP Residents for 'Vaccine Registration' to Swipe Their Aadhaar, Bank Details".* News18, https://www.news18.com/news/india/cyber-frauds-are-calling-up-up-residents-for-vaccine-registration-to-swipe-their-aadhaar-bank-details-3236567.html 22 Feb 2020 5:19 pm 2021
- Aman Nair, *"Pandemic technology takes its toll on data privacy*", Deccan Herald, June 13 2021 at 9: 18am
- Archana More, "cybercrime *101: dissecting the ongoing trend",* Pune Mirror , May 29, 2021 at 6:00am
- Ankita Chakravarti, "*leaked data of Dominos India users now available on search engine created by hacker",* India Today News May 22 2021 at 10:57 am
- Erum Salam, "*cyber-attack forces shutdown of one of the US's largest pipelines",* The Guardian May 08 2021 at 1:03pm
- Money control News, "Government *operationalizes national helpline 155260 to combat cyber-crime losses",* Money control June 17 2021 at 8:52 pm
- Suhasini Haidar, "*some states using cyberspace skill to execute cross border terror: Shringla",* The Hindu 29 June 2021 at 8:00 pm Indian standard time.
- Deccan Herald, "*India 2nd biggest target of cyber criminals in Asia Pacific in 2020: IBM",* Deccan Herald news February 24 2021 11;42pm
- Combating Copyright Online Piracy In India: Government's Initiatives And Judicial Enforcement March 2020
- M*eitY seeks ideas on IT Act revamp,* The Economic Times, 07 April

F. Case laws

- Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal & Ors 2019 SCC OnLine SC 1553
- Abdul Rahaman Kunji v. The State of West Bengal 2014 SCC OnLine Cal 18816
- M/s. Xact Studio International vs M/s. Liwona SP. Z.O.O 2018 SCC OnLine Del 9469
- S. Karunakaran v Srileka 2019 SCC OnLine Mad 1402
- Syed Asifuddin v State of Andhra Pradesh 2005 SCC OnLine AP 1100
- State (NCT of Delhi) v Navjot Sandhu (2005) 11 SCC 600
- Puneet Prakash v Suresh Kumar Singhal & Anr 2018 SCC OnLine Del 9857
- Central Electricity Regulatory Commission v National Hydroelectric Power Corporation Ltd. & Ors. (2010)
- Dr. Madhav Vishwanath Dawalbhakta v M/s. Bendale Brothers 2018 SCC OnLine Bom 2652
- UOI v. Shreya Singhal (2013) 12 SCC 73
- Shamsher Singh Verma v. Haryana State 2015 SCC OnLine SC 1242
- Syed Asifuddin and Others v. Andhra Pradesh State and Others 2005 CriLJ 4314
- Nakul Bajaj & Ors. v. Christian Louboutin SAS (2018) 253 DLT 728
- Avnish Bajaj v. Delhi State (NCT) (2008) 150 DLT 769
- Suhas Katti v. State of Tamil Nadu CC No. 4680 of 2004
- Jogesh Kwatra vs. SMC Pneumatics (India) Pvt. Ltd CM APPL. No. 33474 of 2016
- Devidas Ramachandra Tuljapurkar Vs the State of Maharashtra (2015) 6 SCC 1
- Firos vs State of Kerala on 24 May, 2006, AIR2006KER279
- R v Gold and Schifreen [1988] 2 WLR 984
- Suhas Katti v. State of Tamil Nadu C No. 4680 of 2004
- Janhit Manch & Ors. v. The Union of India PIL NO. 155 OF 2009.
- Emeka Fabian Vs State of Karnataka Crl.P. NO. 570/2016
- Adv R.Mahalakshmi vs Commissioner Of Police CRL.O.P.Nos.27389 of 2013
- State by Cybercrime Police vs. Abubakar Siddique C.C.No. 24836/2009
- Shagun and Ors vs Health W.P.(C) No.3193 of 2016
- Sandip Harshadray Munjyasara vs State of Gujarat AIRONLINE 2018 GUJ 151

- Sri Shakthi Institute of Engineering vs Anna University W.P.Nos.14136 & 16306 of 2021
- Prehari Cyber Security Facilities Pvt vs East Delhi Municipal Corporation W.P.(C) 5645/2021
- The Associated Chambers of Commerce and vs Cyber Security Integrators India Pvt O.M.P. (COMM) 390/2022.
- Matispft Cyber Security Labs Private Vs the State of Andhra Pradesh W.P.No. 8860 of 2021
- J.B. Educational Society and 2 Others vs Jawaharlal Nehru Technological W.P.Nos.25815 2021
- Cherabuddi Educational Society vs Jawaharlal Nehru Technological SLA (C) No.2440/2023
- High Court for the State of Telangana at Hyderabad
- Jawaharlal Nehru Technological Vs Crescent Educational Society Civil Appeal No 6931 of 2021
- Trusted Info Systems Private Limited vs Indian Computer Emergency Response W.P.(C) 7508/2021
- Cyber Media (India) Ltd vs M/S Cyber Intelligent Security Pvt CS No. 159/11 Additional Senior Civil Judge (South), Saket Courts, New Delhi.
- Sheeli Goyal D/O Radhyashyam Goyal vs State of Gujarat R/CR.MA/6945/2021 In The High Court of Gujarat at Ahmedabad

G. Committee Reports/Policies/ Manual

- National Cyber Security Policy -2013
- Justice BN Srikrishna Committee on Data Protection
- TK Vishwanathan committee on Cyber security
- IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to online gaming
- SEBI- High Powered Steering Committee on cyber security (HPSC-CS) and Information Systems Security Committee (ISSC)
- Cyber Security Guidelines for Government Employees manual
- Cyber hygiene for cyber space Manual

- Standing committee Report on – cyber-crime, cyber security and Right to Privacy by Ministry of communication and Information technology
- Cyber security Association of India
- IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 namely- IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023 in relation to online gaming and fake or false information about Central Government business.
- Report of the Joint committee on the Personal Data Protection Bill 2019

LIST OF APPENDICES

Questionnaires for Empirical Work

Part I: General Respondents

Q 1. Please select your age group

Q 2. Please select your gender

Q 3. How much aware you are about cyber-crime?

Q 4. How much aware you are about cyber security?

Q 5. While using the internet, how safe do you feel your information is?

Q 6. How important is it to have a strong password in your social accounts/financial apps?

Q 7. Have you ever lost your money due to cyber-crimes online shopping?

Q 8. Have you ever experienced any of these situations?

Q.9. How many times you have been article victim of a cybercrime?

Q.10 Do you agree that cyber laws of the country are able control cybercrimes?

Q. 11. How important is it to be safe online (social media, net banking, ETC) (5 is more important, 1 is least important)?

Q 12. Are cyber security measures taken by financial institutions are enough to tackle cybercrime in Mumbai?

Q 13. Should cyber laws be amended as per the situation in the financial sector and make it more deterrent towards cybercriminals?

Q.14. cybercrime and cyber security in the financial sector should be taken into priority by the legislature?

Part II: Law Faculties

Q.15 Are you aware of cyber-crime?

Q.16 Is the Current Information Technology Act 2000 is Sufficient to Curb Cyber-crime in India?

Q.17 Information Technology act 2000 requires amendments relating to cyber-crime?

Q.18 Are you aware what is cyber security under Information Technology act 2000?

Q.19 Does Information Technology act 2000 covers each aspect of cyber-Security?

Q.20 Does Information Technology act 2000 requires changes in the cyber-Security laws and a separate cyber security act should be introduced to curb cyber-crime?

Q.21 Are you aware of what is critical infrastructure under cyber-crime?

Q.22 Critical infrastructure under cyber-crime includes: -

Q.23 Does Information Technology Act 2000 covers all aspects of critical Infrastructure?

Q. 24 Do You feel a separate act is required to protect the critical Infrastructure from cyber-criminals?

Q.25 what are your suggestions on the Information Technology act & what amendments are needed in the Information Technology act 2000 to curb cyber-crimes in India?

Part III: Lawyers/Advocates

Q.26 Are you aware of cyber-crime?

Q.27 Does Practicing Advocates have Awareness regarding cyber security & data protection?

Q.28 Are there enough cyber lawyers currently in Mumbai?

Q.28 Cyber law practice is a new practice altogether for the litigating lawyers in Mumbai?

Q.29 The Prosecution and the Defense Advocates find it difficult to decide the matter before presiding judges in Mumbai due lack of knowledge related to cyber law?

Q.30 The Police officials also lack knowledge regarding the cyber law and how Information Technology Act 2000 sections to be applied why framing charges against an accused?

Q.31 The Judicial infrastructure is not prepared for deciding cyber related matters and cyber security matters due to lack of knowledge?

Q.32 Should there be amendments in the present Information Technology Act 2000 for better implementation in the litigation part?

Q.33 Information technology act, 2000 will play an important in the Coming years to educate cyber law matters in the judicial infrastructure?

Q.34 Workshop and Conferences should be organized to help Advocates to understand the importance of Information Technology act 2000 and make them understand the litigation part of cyber law?

Q.35 Cyber law practice and cyber security experts are required in each state bar council to promote its importance and to educate advocates regarding cyber law matters?

Part IV: Financial Sector

Q.36 In which financial sector do you work?

Q.37 How many years of experience do you have in the financial sector?

Q.38 How Much Percentage of financial crime gets solved?

Q.40 Which are the common cyber threats customers are aware of?

Q.41 How much percent of debit and credit frauds customers usually face?

Q.42 To whom do customers report cyber fraud incidents?

Q.43 How do you deal with financial frauds which the general people face?

Q.44 How many percent of active customers are having E Banking and Payment apps?

Q.45 Do customers recognize fake websites of the financial sectors?

Q.46 Are you aware about importance cyber security in the financial sector?

Q.47 Is the current cyber–Security Infrastructure sufficient to curb cyber-crime in the financial sector?

Q.48 Do the current methods adopted by the financial sector for prevention of cyber-crime is enough to cater to the rising problems of citizens?

Q.49 Are citizens aware of what cyber security is and its importance in the financial sector?

Q.50 How Much percent of third-party payments applications such as net banking, internet banking, UPI are vulnerable to cyber criminals?

Q.51 Do you believe People around the age of 40 to years of age are not aware of the internet or E banking, UPI and they are easy targets of cyber criminals?

Q.51 Do you feel a separate act is required to protect the financial sector from cyber criminals?

Part V: Personal Interview Cyber Experts

Q.52 What Is Your Opinion on The Current Structure of Cyber Crimes and Cyber Laws in India?

Q.53 Whether Cyber Crimes Are Affecting Financial Sector in Mumbai, What Are Your Opinions How It Can Be Tackled?

Q.54 What Is Your Opinion on The Current Cyber Act (Information Technology Act 2000) Whether It Is Capable to Cater the Rising Cyber Crimes in The Financial Sector?

Q.54 Critical Infrastructure and Its Importance, How It Can Be Strengthened?

Q.55 What Are Your Opinion Whether New Information Technology Act Should Be Introduced to Cater Cyber Crimes?

Q,56 What Are Your Views on The Cyber Security Infrastructure In Financial Sector Whether They Are Capable Of Catering Cyber Crimes?

Q.57 Lastly Your Suggestion, Comments, Opinions on Cyber Crimes, Cyber Law, And Its Impact on The Financial Sector in Mumbai

Part VI: Personal Interview Police Personnel

Q.58 How Cyber Crimes Matters Are Solved?

Q.59 What Is the Current Structure of Communication Between Banks, Telecom Operators and Police Officials After Cyber Crime Is Committed?

Q.59 Whether Cyber Crime Is Solved If Solved in How Many Days?

Q.58 Whether People Are Aware of How-To Complaint About Cyber Crime?

Q.59 What Are Your Experience with Cyber Criminals?

Q.60 What Is the Appellate Mechanism of Cyber Complaints?

Q.62 Do You Think More Cyber Cells Are Required in Each Police Station?

Q.63 Can Police Take Suo Moto Cognizance/Action Without the Order Of The Appropriate Court?

Q.64 Do You Think Citizens' Cyber Cell Should Be Introduced?

Q.65 What are your Suggestions, Opinions, How Cyber Crime in Mumbai Can Be Streamlined to Cater Cyber Crimes

LIST OF PUBLICATIONS

SCOPUS INDEXED JOURNAL

INTERNATIONAL LEGISLATIVE FRAMEWORK OF CYBERCRIMES- A COMPARATIVE STUDY OF INDIA, ISRAEL AND USA, Journal of Positive school of psychology, Volume 7, No.1, Page No. 782-800.

UGC CARE LISTED JOURNAL

THE VIRTUAL REALITY OF CYBER STALKING: A STUDY WITH SPECIAL REFERENCE TO WOMEN IN MUMBAI, Shohd Sanchar Bulletin, Vol 11 Issue 41 Page No. 299 - 303.

CYBER SECURITY IN THE INDIAN BANKING SECTOR, Journal of Scientific Research in Science and Technology/International Journal of Scientific Research in Science and technology, Volume 9, Issue 5, Page No. 391-394

DEVELOPMENT OF CURRICULUM OF SCHOOL EDUCATION WITH REFERENCE TO THE CYBER CRIMES FOR FUTURE, Indian Journal of Psychology, Book No. 002, 2024 ISSN 0019-5553

PEER REVIEWED JOURNAL

DATA PROTECTION BILL: NEED OF THE HOUR IN INDIA, Journal of Advance and Innovative Research, Volume 9, Issue 1 (III)

INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES 2021 & IT'S RELEVANCE WITH OTT PLATFORMS, International Journal of Advance and Innovative Research, Volume 9, Issue 2 (XII)

LIST OF CONFERENCES

INTERNATIONAL CONFERENCES

CYBER SECURITY IN THE INDIAN BANKING SECTOR, International Multidisciplinary E conference on Contribution of various aspects in Nation Building In association with International Journal of Scientific Research in Science and Technology, Volume 9 | Issue 5 | PG; 391-394, ISSN: 2395-6011/Online ISSN: 2395-602X (www.ijsrst.com), Paper Presented

DATA PROTECTION BILL: NEED OF THE HOUR IN INDIA, One Day National Multi-Disciplinary E-Conference on Post- Covid Revival of the Indian Economy /International Journal Of Advance And Innovative Research, Volume 9, Issue 1 (III), ISSN: 2394 – 7780, Paper Presented

INTRODUCTION OF THE POLICIES UNDER THE INFORMATION TECHNOLOGY ACT RELATED TO INTERMEDIARIES, Virtual National Conference On "Progressive India: Corporates and The Pandemic,

LIST OF WORKSHOPS

RESEARCH METHODLOGY USING STATISTICAL TOOLS, short term course from 25th May to 29th May 2021, organised by lovely Professional University.