SAFEGUARDING PERSONAL PRIVACY IN DIGITAL ERA: A STUDY ON THE RIGHT TO PRIVACY

A DISSERTATION TO BE SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE OF MASTER OF LAWS

SUBMITTED BY

MOHD. RIYAZ AHMAD
1220997022
SCHOOL OF LEGAL STUDIES

UNDER THE GUIDANCE
OF
PROF.(DR.) SUDHIR AWASTHI
SCHOOL OF LEGAL STUDIES

BBD UNIVERSITY

SESSION 2022-23

CERTIFICATE

This is to certify that the dissertation titled, "**SAFEGUARDING PERSONAL PRIVACY IN DIGITAL ERA: A STUDY ON THE RIGHT TO PRIVACY**" is the work done by **Mohd. Riyaz Ahmad** under my guidance and supervision for the partial fulfilment of the requirement for the Degree of **Master of Laws**in School of Legal Studies Babu Banarasi Das University, Lucknow, Uttar Pradesh.

I wish his success in life.

Date -------------- Prof.(Dr.) Sudhir Awasthi

Place- Lucknow

DECLARATION

Title of Dissertation **"SAFEGUARDING PERSONAL PRIVACY IN DIGITAL ERA: A STUDY ON THE RIGHT TO PRIVACY"**

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

Mohd. Riyaz Ahmad

I declare that

(a) This dissertation is submitted for assessment in partial fulfilment of the requirement for the award of degree of **Master of Laws.**

(b) I declare that this **DISSERTATION** is my original work. Wherever work from other source has been used i.e., words, data, arguments and ideas have been appropriately acknowledged.

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

(d) The work conforms to the guidelines for layout, content and style as set out in the Regulations and Guidelines.

Date : ………………

Place- Lucknow

Mohd. RiyazAhmad
LLM
Criminal & Security Law
1220997022

ACKNOWLEDGEMENT

This dissertation is the outcome of the study by the researcher. Any material used from different sources has been thoroughly acknowledged. After the successful completion of my work, I would like to thank a number of people.

I would like to give my heartfelt gratitude to Prof.(Dr.) Sudhir Awasthi, School of Legal Studies who undertook the role of being my supervisor, mentor, and guide for the successful preparation of this dissertation. This work is an outcome of an unparalleled infrastructural support that I have received from staff and employees of the School of Legal Studies. It would never have been possible to complete this study without an untiring support from my family.

Finally, I must express my very profound gratitude to my family for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this dissertation. This accomplishment would not have been possible without them. This study bears testimony to the active encouragement and guidance of a host of friends and well-wishers.

Mohd. Riyaz Ahmad
LLM
Criminal & Security Law
1220997022

Abbreviations

- $- Dollar
- £- Pound
- §- Section
- AIR- All India Reporter
- E-banking - Internet Banking
- RBI- Reserve Bank of India
- ATM- Automated Teller Machine
- NPCI- National Payments Corporation of India
- WTO - World Trade Organization
- WB - World Bank
- IMF - International Monetary Fund
- IPC - Indian penal Code
- IT act - Information Technology Act
- ATM- Automated Teller Machine
- B2B- Business to business
- B2C-Business to customer
- B2G- Business to government
- B .C.- Before Christ
- BOM- Bombay
- C- Column
- UPI - Unified Payments Interface
- NPCI - National Payments Corporation of India
- RBI - Reserve Bank of India
- e-RUPI - Electronic(Digital) Rupee
- RBI Act - Reserve Bank of India Act 1934
- NFT - Non Fungible Token
- NITI - National Institute for Transforming India
- DPIIT- Department for Promotion of Industry and Internal Trade
- MCA- Ministry of Corporate Affairs
- IBA - Indian Banks' Association
- PSS act- the Payment and Settlement systems Act 2007

- C .P .C- The Code of Civil Procedure, 1908
- Cal- Calcutta
- CBI- Central Bureau of Investigation
- CCC- Cyber Crime Cell
- CCTV- Closed Circuit Television
- CD- Compact Disk
- CD-ROM Compact Disk- Read Only Memory
- Cr LJ- Criminal Law Journal
- Cr.P.C- The Code of Criminal Procedure, 1973
- Cri.- Criminal
- CV- Civil cases (US)
- CVC- Central Vigilance Commission
- Del.- Delhi
- DOS Denial of Service
- e .g . Exempli Gratia
- E-Com- Electronic Commerce
- EFT- Electronic Fund Transfer
- ENIAC- Electronic Numerical Integrator and Computer
- ESN- Electronic Serial Number
- etc . et cetera
- EU- European Union
- FBI- Federal Bureau of Investigation
- FIR- First Information Report
- FTP- File Transfer Protocol
- G-8- Group of Eight Governments
- GIF- Graphic Interchange Format
- GPS- Global Positioning System
- HC High Court
- HTML- Hypertext Markup Language
- HTTP- Hypertext Transfer Protocol
- i .e . Id est
- Ibid- In the same place
- IBM- International Business Machine
- ICANN- Internet Corporation of Assigned Names and Numbers

- ICTs- Information Communication Technologies
- Id- Idem(the sanie)
- ID- Identity
- inc.- Incorporated
- IP- Internet Protocol
- IPC- Indian Penal Code, 1860
- ISP- Internet Service Provider
- IT- Information Technology
- ITA- Information Technology Act
- ITU- International Telecommunication Union
- LAN- Local Area Network
- LPG- Liberalisation Privatisation and Globalisation
- MIN- Mobile Identification Number
- MMS Multi Media Services
- MS-DOS- Microsoft Disk Operating System
- MSN- Microsoft Network Messenger
- NASSCOM- National Association of Software Service Companies
- NCRB- National Crime Records Bureau
- NCT- National Capital Territory
- No.- Number
- OECD- Organization for Economic and Cooperation and Development
- ONS- The Office of National Statistics
- Ors- Others
- p.no- Page number
- PC- Personal Computer
- PDF- Portable Document Format
- PIN- Personal Identification Number
- SC- Supreme Court
- SCC- Supreme Court Cases
- Sec.- Section
- SMS- Short Message Service
- Supra- Referred above
- TCP- Transmission Control Protocol
- TELNET- Telecommunication Network

- TRAI- Telecom Regulatory Authority of India
- U .O .I- Union of India
- UNCITRAL- United Nations Commission on International Trade Law
- URL- Uniform Resource Locator
- US- United States
- USA- United States of America
- USD- United States Dollar
- USSR- Union of Soviet Socialist
- v.- Versus
- Viz- Videlicet (namely)
- Vol- Volume
- W.P.- Writ Petition
- W.P.Crl.- Criminal Writ Petition
- WAN- Wide Area Network
- WAP- Wireless Application Protocol
- WIPO- World Intellectual Property Organization
- WWW- World Wide Web

TABLE OF CASES

- Ban on Chinese apps under section 69A of the IT Act, 2000,

- CBI Vs Arif Azim [(2008) 105 DRJ 721: (2008) 150 DLT 769]

- CBI v. Arif Azim (Sony Sambandh Case) (2013)

- Cyber Appeal/4/2013, Misc Application/120/2018

- Nasscom v. Ajay Sood &Others : 119 (2005) DLT 596, 2005 (30) PTC 437 Del.

- Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi &Others :

- Pune Citibank Mphasis Call Center Fraud (2005)

- Justice K.S. Puttaswamy (Retd.) &Anr. vs. Union of India &Ors.: (2017) 10 SCC 1, AIR 2017 SC 4161

- Shreya Singhal vs Union of India [2013 12 SCC73]

- State of Tamil Nadu v. SuhasKatti : C No. 4680 of 2004

- Vinod Kaushik and others v. Madhvika Joshi and others : WP(C) 160/2012, Delhi High Court,

- Yahoo Inc vs Akash Arora 1999 19 PTC 210 Delhi

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1- DIGITALIZATION IN INDIA AND ITS BENEFITS & DEMERITS-

The world's largest democracy (that is India) has been performing very well on the economic front even when many countries have still not been able to come out of the impact of Covid pandemic and from various other negative impacts of the global economic slowdown. The opportunities for India in coming years are quite bright not only because it is performing well in the economic field but India has the most young population compared to the other countries and this young population can transform the future of India as a new world leader as well. The increasing pace of digitalisation in India has not only been making the whole country get developed but various new digital inventions have started becoming global which were planned and developed in India, for example UPI which has become a popular and much demanding payment option not only in India but also in other countries as well.

The technological advancements have been bringing a never seen before transformation in India. Inspirational services are getting availed very easily by the Indians through the technological advancements and especially through the increasing usage of smartphone and internet.[1] Digital development with unexpected speed of growth and reach of digitalitalisation in every corner of India has made at least everyone to come online or use different kinds of digital methods for various day to day practices. The factors which has made a wide spread of digitalisation, smartphones and internet are the affordable cost of internet, affordable smartphones, capability of smartphones in doing various digital activities, introduction of 4G and 5G, easy steps of availing various digital services which can be operated by any person having basic knowledge to operate a digital gadget. There was a time when laptops or computers had an edge over mobile phones and smartphones due to which the reach of digital services were quite limited because all persons were not able to afford such highly priced devices or most of them were utilising the services in cyber cafes to accomplish various kinds of digital services but now the mobile phones and smartphones have become highly advanced that an individual can very easily accomplish any kind of digital works or transactions through his mobile phone or smartphones though the role of laptops and computers have also

[1] Excerpt from "A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians", a report by the Committee of Experts chaired by Justice B.N. Srikrishna, (2018), Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report. (Visited on 19th April 2023)

become so important because they have also become so advanced with the passage of time. But such advancements have brought many problematic issues and the breach data and violation of privacy are the most concerning ones.

Due to the cultural reasons, a joint family system is quite prevalent in India but the concept of urbanisation has also been influencing the growth of nuclear families especially in urban areas and the prime reason has been the migration of people from one place to another especially from the villages to the cities. But still data shows that 5.5 is the average size of a family in India. It shows that there is still a big population in India which is still conscious about the prices of the products and which favours affordable products especially it matters a lot when a consumer purchases any digital gadgets. This reason has been causing the manufacturers of digital devices to introduce affordable gadgets. The providers of the internet have also been conscious about this reason as well as the introduction of Jio has also brought revolutionary changes in providing affordable internet for the users. Before the introduction of Jio the prices of internet were very high and after the introduction of Jio not only has good speed internet has been provided to the user but the prices of internet have become so affordable as well. The combination of the affordable smartphones with cheap internet has made a big population of India move towards the digital world. This phenomenon has been causing the less use of television for entertainment purposes and it has been happening because private space has been made available by the modern gadgets where any person can get entertained from anywhere and there is no need in most of the case to gather at the same spot for watching television or for getting entertained. This activity is quite common in nuclear families where everyone has their own space to use smartphones and digital gadgets.

In the digital era mobile, smartphone, internet, etc. have become a part of life of at least every individual. The main importance of such digital devices and services has mostly grown from the need to communicate to the need to engage on social media, to the need to complete various financial transactions, to the need to store large data in small spaces, to the need to facilitate various medical, academic, transportation services, online shopping and many more.

Affordable gadgets have brought some problems as well because they can not provide proper security from various cyber misuses. Since various important data are available online hence it has become very easy for the criminals to access someone's online data just by using some technical & cyber information and if the criminals are highly advanced than they can breach even high class of cyber security measures and can cause big cyber crimes against any person or organisation. In this way the cyber security measure must be made more affordable for proving the concept of digital India more successful. The user of digital gadgets and the internet users must be made more informative about the cases of cyber crimes and they must be taught the cyber security measures for minimising the risks of cyber crimes. The affordable mobile phones and smartphones have been quite successful in causing the growth of the digital services, social media, online payments, etc. but such affordable devices have become very vulnerable for becoming the victims of cyber crimes. In the growth of cyber crimes the devices with no or insufficient cyber security measures have been quite important. It has become necessary to make it mandatory that the digital and online devices must have the needful cyber security measures, though it can increase the cost of the devices but it is a much needed step and if the cost is getting too high then the government must provide some subsidy for coupling every digital and online devices with the cyber security measures. Though, the affordable and cheap devices can be blamed for the increase in the cases of cyber crimes and breach of privacy but with this the misuse of cyber knowledge by the cyber experts and the inability of the monitoring authorities in preventing the cyber risks and their inability in tracking the cyber criminals can also not be ignored.

Consumers are immensely influenced by the growth of smartphone technology and widespread use of digitalisation. Such growth has brought various kinds of behavioural changes as well in the minds of users. Information divide is decreasing day by day and various differences between rural and urban areas are also getting shortened.

"Today we have 1.18 billion mobile connections, 700 million Internet users, and 600 million smart phones, which are increasing 25 million per quarter. India has the highest mobile data consumption rate at 12 Gigabytes or GB per user a month in the world."[2] There will be more than 100 crore internet users when the year 2030 arrives. The smartphone technology would

[2] India's growing data usage, smartphone adoption to boost Digital India initiatives: Top bureaucrat, *available at* :https://economictimes.indiatimes.com/news/india/indias-growing-data-usage-smartphone-adoption-to-boost-digital-india-initiatives-topbureaucrat/articleshow/87275402.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst (Visited on 19th April, 2023).

have become more advanced which will allow more advanced activities. Technological growth will reduce a lot of the burden of manual work done by human beings.[3]

1.1.1- ISSUE OF CYBER RISKS

Due to the reasons of comfort and time saving processes, various activities have now started being performed on the digital and online devices hence the users have to share various personal and private data on these digital & online devices. The risk is that the other people with malicious minds can acquire this personnel and private data of others by some physical means like by stealing the digital or online devices or through non-physical means such as controlling the devices and accessing the information through technological mediums like hacking. These risks result into cyber crimes if no proper measures are taken to reduce the risks. The problem is that the acquired data can be used to withdraw money from banks, to extort the person, to blackmail the persson, or for many other purposes as well.

Not only any sudden act with malicious intent can breach the personal and private rights of users but such violations can happen continuously as well like there can be many apps and softwares in the digital and online system which may continuously steal the private and personal day of the users. The users have become a product these days to enrich the owners of various apps and softwares who are making billions of dollars on the basis of personal information of users.[4]

"Users of mobile devices or so called mobile users are increasingly subject to malicious activity, mainly concerning pushing malware apps to Smartphone, tablets, or other devices using a mobile Operating System. Smart phones today store hefty amounts of data and operate over International Cellular Networks, WLANs, and Bluetooth PANs. They run a diverse set of complex Operating Systems such as iOS, BlackBerry OS, Android, and Windows Mobile. Most Smart phone also supports the Java platform for mobile devices, J2ME, with a variety of extensions. All this network connectivity and diverse rich code

[3] The impact of mobile and rapid digital adoption on how India consumes, WORLD ECONOMIC FORUM, *Available at* https://www.weforum.org/agenda/2019/01/how-mobile-is-disrupting-consumption-in-india/ (visited on 19th April, 2023).

[4]https://www.forbes.com/sites/forbes-personal-shopper/2022/02/18/best-tech-deals/?sh=6cc8f735390b (Visited on 19th April, 2023).

makes these devices more vulnerable than traditional PCs, which typically run standard operating systems for which many security products are readily available."[5]

1.1.2- RIGHT TO PRIVACY IN INDIA

In India, Right to Privacy has been acknowledged as one of the fundamental rights by virtue of Article 21. In the case of K. S Puttuswamy v. Union of India[6] it was held that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

While deciding the case the court listed a long line of jurisprudence the central deficiency in the existing jurisprudence in the court's opinion was the lack of a "doctrinal formulation" that could help decide whether Privacy is Constitutionally protected. The jurisprudence on privacy therefore changed from being valued as a right that protected other ends to being an end in itself. Along with holding that privacy as a fundamental right, the judgment also declared informational privacy to be a subset of the right to privacy.[7]

1.1.3- PRIVACY IN DIGITAL WORLD:

The Indian economy has continuously started enjoying the benefits of digital advantages especially from the last ten years. The growth of various digital services has been creating a big amount of digital data of users. "India generates about 150 Exabyte of Data annually and is amongst the fastest growing Data generating nations in the world."[8]

The activities performed on digital & online apps and softwares and the information shared on such platforms are part of digital data. Some data is created by the technology itself to identify the users and this data is also very crucial. Daya is like currency in the modern world. There have been continuous sales of such data on the dark internet. Big companies purchase this data to make their business plans and cyber criminals utilise this data to commit various crimes. In this way the users on the name of comfort and modernity have become a

[5] PawełWeichbroth and ŁukaszŁysik, Mobile Security: Threats and Best Practices, Quanzhong Li, (2020),*Available at*: https://www.hindawi.com/journals/misy/2020/8828078/. (Visited on 19th April, 2023)

[6] (2017) 10 SCC 1

[7] Anirudh Burman, "Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?" Carnegie India, 2020, *available at*: https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217 (Visited on 20th April, 2023)

[8] Loksabha, Report of the Joint Committee on the Personal Data Protection Bill, 2019.

tool for being victimised where their personal data is very easily misused without their permission.

The role of data and online services have become so important that business worth billion dollars can be created. "As technology progresses, newer applications emerge enhancing the value of the data. Uber, the world's largest taxi company, owns no vehicles, Facebook the world's most popular media owner, creates no content, Alibaba the most valuable retailer, has no inventory and Airbnb, the world's largest accommodation provider, owns no real estate."

The data of users have been helping a lot to the business in expanding their areas of business with proper accuracy but the problem is that the users are paid for the data which they are creating as well as a lot of their personal information are used even without inforning them.

"The low costs of storing and processing information and the ease of Data collection has resulted in the prevalence of long-term storage of information as well as collection of increasingly minute details about an individual which allows an extensive user profile to be created. Such information can then be used to create customized user profiles, based on their past online behaviour, which has the benefit of reducing the time required to complete a transaction."[9]

The more advanced technologies have been accessing more data of users. GPS can tell the travel records of users, fingerprint scanners can get the fingerprints, voice recording, health status, financial status, private chats, they all are at risk of being stolen and misused.

The biggest issue in this regard has been the lack of development of affordable security devices and security measures. Coupling the digital online devices with proper cyber security measures can protect the cases of cyber crimes and cases of breach of personal data.

1.2- STATEMENT OF THE PROBLEM

In the digital era, it has become very easy to steal the secret information and personal data of the users through digital and online mediums. In India, some laws have been made but they are not sufficient enough in safeguarding the privacy of the users and they lack a lot of strict

[9] Poulomi Sen, EU GDPR and Indian Data Protection Bill: A comparative study, *available at:* https://ssrn.com/abstract=3834112 (Visited on 20th April 2023)

measures in protecting the data of the users. In 2021, the rank of India was third all over the world in terms of number of cases of data breaches.[10] Hence, we need a quick legal reform to tackle these issues.[11]

Enforcement Mechanisms with regard to the online Data Protection in India are weak. The existing Indian laws are not implemented properly due to which rarely any actions are taken against cyber criminals. Hence, big legal reforms are required to protect the right to privacy in the digital era.

Big reforms in the judicial system are also required because the trial of cyber crimes and other Court proceedings in cases related to cyber crimes are very slow, as well there is a poor status of the rate of conviction in cyber crimes. From the side of judiciary, fast trials and quick convictions of the offenders can only guarantee the protection of rights to privacy.

Issues of violations of privacy and the issue of misuse of data exist all over the world.[12] Collaboration of countries on this issue may provide a strong way to solve this problem. India does not have a comprehensive legislation which deals with Data Protection and Privacy. There is a requirement to formulate robust data management policies, standards and best practices with accurate data, appropriate data access, strong data security, and privacy and ownership rights. Deploying advanced digital infrastructure for connecting and when mass data is collected, it is impossible to distinguish between personal data and non personal data, as various kind of data deal with various level of security. To avert contradiction, confusion and mismanagement, a single administration and regulatory body is necessitated.[13] This research work will help to review the law and compare it with other countries how they have been tackling the issue of Data Privacy. Data Privacy in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India and this research will be way towards it.

[10] Today Desk, India ranks third in global data breaches in 2021: Report, *available at:* https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15 Business (Visited on 20th April 2023).

[11] Today Desk, India ranks third in global data breaches in 2021: Report, *available at:* https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report-315750-2021-12-15 Business (Visited on 20th April 2023).

[12] Data Protection & Privacy Issues in India, Economics Law Practice, (2017).

[13]*Ibid.*

The growing number of cases of banking frauds and crimes related to financial gains have been seen to be committed through online mediums in recent years. It raises an issue of targeting the banking sector through cyber crimes.

Through the increasing dominance of internet banking in India targeting banking sector through cyber crimes can be very really a very easy process for criminals.
Cyber criminals seem to be very handy in duping people online and through digital mediums while the banks and authorities look very helpless in preventing the cases of loss caused by cyber crimes.

It shows a serious concern which must be solved very soon, if the prime target of the cyber criminals are banks and money of people only then the preventive measures must be be very strong to save the banks and money of people from cyber crimes.

Various findings in past years show that the banking frauds and illegal financial gains are those cases of cyber crimes which are always related to having the highest number of violations through cyber crimes.

It indicates that the prime target of cyber crimes are banks and various stakeholders related to banks and the introduction of i-banking has made the job of cyber criminal very easy.

Not only stealing money from banks but for supporting the commission of various other traditional and cyber crimes the internet banking has made the job of criminals very easy.

Criminals and wrongdoers are paying money to their partners through online modes for committing various kinds of crimes and for organising various illegal activities. It is said that online transactions can be traced very easily but the criminals have developed various methods through which they are paying money online by disguising them as someone else, by faking their locations to some other places or take the help of third parties to receive the money through internet banking for various illegal activities. In this way, it looks that the internet banking has made the job of traditional and cyber criminals very easy.

Now it is said that cyber crimes are having a great relation with the intent banking and without internet banking the case of cyber crimes would not have increases this much higher.

1.3- HYPOTHESIS

Existing laws for data protection must be implemented strictly, as well as the existing cyber laws must be reformed as soon as possible and it must be continuously updated to protect the right to privacy and to improve the status of data protection in India.

Currently too much time is taken in finishing both the investigation and trail in cyber crime cases. The pace of investigation by police in cyber crime cases must be quick. The trial of the cyber crimes must be conducted through the formation of fast track courts.

1.4- OBJECTIVES OF THE RESEARCH

Following are the objectives of this research work-

1. To analyse the importance of right to privacy and to understand the need for data protection in the digital era.
2. To find out the factors which make a user vulnerable for being targeted through cyber mediums which ultimately causes violation of privacy.
3. The aim of the research is to examine the attitude and check the extent of awareness users have regarding the data privacy while downloading the app or while using other digital & online mediums.
4. The aim is to understand and examine the importance of consent as the ground of processing of the data.
5. To examine the legal framework and judicial approach in India for protecting the right to privacy in the digital era.
6. The objective of the research is to find out if there are any lacunas in the present law in India dealing with the protection of data privacy.

1.5- RESEARCH METHODOLOGY

Doctrinal method of research has been used to complete this research work. The risk on personal privacy in the digital era has been analysed with the help of many books, previous research works, bare acts, and the help of various authentic online sources have also been taken. The concept of right to privacy has been explained with the help of many important judgments of courts and also with the help of many credible literary works of scholars. The IT Act, 2000 along with the relevant IT Rules and IT regulations have been analysed to understand the legal mechanism to protect privacy in India. The much awaited Data

Protection Bill has also been analysed to understand the plans of government to protect personal data of people.

1.6- LITERATURE REVIEW

Udayan Mukerji, R K Naroola[14](2021) has analysed the status of privacy of users in the digital world. He has analysed the data protection bill of the EU to understand the responsibilities of inyernediarues. According to him, there has to be transparency in utilisation of data of the users so that the data can be protected, it can be properly legally regulated and the right of privacy of users can be protected. He has said that the right to privacy is not totally absolute because there are some exceptions of it when data can be accessed and he has explained those situations as well.

G V S Jagannadha Rao[15](2021) has highlighted the mischievous activities happening on the internet. Various foreign service providers have been taking no action against the mischievous persons, in this regard he has discussed the foreign laws which regulate such service providers. He has explained the need for a law which can control mischievous activities, in this regard he has also analysed the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 through which various legal control on social media has been brought by the India government.

Naavi[16](2020) in terms data usage has talked about the roles of:

- IT professionals,
- Advocates,
- Privacy activists,
- Business managers,
- Government,
- Law enforcement officers.

These all people and institutions have different roles in protecting the right to privacy in the digital world. The researcher has also explained the complexities and shortcoming in the

[14] UdayanMukerji , R K Naroola : Jurisprudence of Privacy, Oak Bridge Publishing Pvt. Ltd.(2021).

[15] G V S JagannadhaRao : Ethics Code for Social Media, OTT and Digital Media Commentary on Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Asia Law House 1st Edition (2021).

[16] Naavi : Personal Data Protection Act of India (PDPA 2020): Be Aware, Be Ready and Be Compliant (Notion Press, 12 February 2020)

cyber laws. The researcher has said that there is big opportunity in the coming years for data protection officers & data auditors, hence a career in these fields will be quite interesting. The researcher has also talked about utilisation of technology for bringing cyber security measures and for protecting the right to privacy in the digital world.

THE REPORT[17](2020) by the Centre for Internet & Society's Report on digital civic space in India, has analysed the issue of monitoring of data and protection of privacy. The Indian cyber laws' capabilities in protecting privacy have also been discussed.

Anghrija Chakraborty[18](2019) has analysed:

- the European Union General Data Protection Regulation,
- the Indian Data Protection Bill 2018,
- and other data protection laws which have been developed in other countries and which are being developed.

The main focus has been on the protection of privacy, protection of personal data, protection of confidential data of the users and clients. The elements for protection which have been discussed are:

- data subject to an individual's rights,
- data handling,
- data ownership,
- data security,
- new information technologies,
- changing scenarios of business in IT sector, financial sector,
- applicability of legislation,
- sanctions, penalties and punishments in India and in other countries,
- the social and legal norms which are evolving.

The implementation of the cyber security laws has been one of the important points raised by the researcher. The researcher has talked about the effective methods of implementations which can be beneficial for corporate sectors as well as to others also.

[17] Mira Swaminathan and ArindrajitBasu, Surveillance and Data Protection: Threats to Privacy and Digital Security, The Centre for Internet & Society's (2020)

[18] AnghirijaChakraborty : Data Protection Laws Demystified (Oak Bridge Publishing Pvt Ltd, 1st Edition, October, 2019).

Bernadette Kamleitner and Vince Mitchell[19](2019) has talked about the issue of interdependence of data and sharing of data. Interdependent infringements have been seriously dealt with by the researcher. Two parties by sharing data become dependent on each other to protect the data. Realise, recognise & respect are "the 3Rs" which have been suggested as an effective measure by the researcher.

Rahul Matthan[20](2018) has said that the status of privacy has changed from ancient times to modern times. He has talked about full utilisation of modern technologies instead of creating highly strict laws to prevent the modern generation from feeling the benefits of modern technology in the name of privacy.

The Report[21](2018) was prepared to understand the capabilities of Indian organisations in protecting the privacy of digital properties. This study analysed:

- The kind of personal data accessed by the App/Website,
- Sharing of personal data with third parties,
- How much data goes beyond India,
- The effectiveness the Apps/Websites in securing personal data,
- The transparency level of the organisation with users in utilising privacy practices,
- Vulnerability of children when they use android apps

The report said that out of total Children Apps, 71% of them were accessing storage, details of phone, location. Among all the permissions which were taken for running the app, more than 50% of them were not necessary to run these apps. Most of the Apps were not taking consent and even if consent was taken then it was done without age verification to check whether the user is an adult or minor. Availability of In-App purchase options were found and most of the apps were having In-App ads. The permissions for running the apps were 45% more in the Indian android apps than in the global android apps. This figure for permission was 60% to 80% in the Indian apps providing services like online shopping, travel booking, Mobile Wallets. Most of the Indian apps were quite active in availing permissions for SMS, phone calls, microphone , contacts.

[19] Bernadette Kamleitner and Vince Mitchell, Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements, Journal of Public Policy & Marketing 2019, Vol. 38(4) 433-450

[20] Rahul Matthan, Privacy 3.0: Unlocking Our Data-Driven Future (HarperCollins, 2018)

[21] The Arrka Study, State of Data Privacy of Mobile Apps & Websites from India (2018)

The shortcomings in various literatures are that the researchers see i-banking as a very highly advanced medium of banking and they always support it by making suggestions for making its use more but they have never properly thought about the issue of internet banking's growing contribution in various crimes . They always focus on the issue of help provided to developed and modern cities through internet banking. Due to fast and easy processes provided by i-banking, the researchers always ask to increase the dominance of internet banking but they always ignore the fact that internet banking is becoming is continuously becoming an easy tool for cuber criminals either to steal money from accounts or to pay their partners the money for crime through electronic and online mediums.

It must be researched whether internet banking has been a part of various crimes in which the money transactions done by the criminals were very difficult to deduce and if it was really done Iike this then it must be concluded that the criminals have decoded the methods to hide their identities while processing internet banking. If it is found to be true then it can be clearly presumed that there are many crimes in which payments are possibly dome to criminals through i-banking. In this way i-banking can be declared a menace. Though, stopping i-banking from use can be very disastrous but it will require various upgrades and various reforms for proper and secured use.

For banking fraud related cases, it has been discussed very well by various scholars that internet banking has become vulnerable for various cyber crimes and how cyber activities are causing monetary loss to people by stealing their crucial data and money, but still it has to be found in detail whether the i-banking has provided a strong ground for committing various cyber crimes, is there a great relationship between cyber crimes and i-banking.

1.7- SIGNIFICANCE OF THE STUDY

This research work will help in understanding the risks on privacy of people in the digital era. These risks are causing people to become victims of various kinds of cyber crimes through which they lose their personal data, money and many other personal things.

By analysing the laws for protecting privacy in India the shortcomings and loopholes in laws will be explained and the need for a proper law to protect privacy in the digital world and the need for protection of personal data through proper laws will be explained.

The need for protection of data and privacy for preventing the cases of financial frauds will be highlighted. There will be a comparison between breach of data and the risks of cyber crimes in internet and digital banking. The financial losses caused due to breach of privacy will be explained with sone more data related to cyber crimes.

Connection between cyber crimes and breach of privacy will be explained and it will be emphasised how efficient and quick our police and judiciary is in solving the cases of cyber crimes.

At the end various helpful suggestions will be given to protect the privacy of people and to protect the personal & confidential data of individuals and institutions in this modern digital era with the help of strong laws.

1.8- TENTATIVE CHAPTERS

This research work will have the following six chapters:

CHAPTER 1: INTRODUCTION

In the starting of this chapter the impact of digitalisation in India and its benefits are discussed. Cyber risks as demerits of digitalisation have also been discussed. The concerns of protection of privacy of people in the digital era have been explained. In the next part the statement of problem has been discussed to protect the privacy of people in the digital era. This chapter also includes research questions, research objectives and hypotheses. Then, for conducting this research work the methodology of research has been explained. The literature works studied by the researcher have been explained under the heading literature review. After explaining the significance of this study, the researcher has given the chapters which have been planned by him to complete this research work.

CHAPTER 2: THE ISSUE OF CYBER CRIMES AND PROTECTION OF RIGHT TO PRIVACY IN INDIA

In this chapter, the concept of right to privacy is discussed and its status as a fundamental right has also been explained, in this regard the case of Puttaswamy has also been explained in which the SC had recognised the right to privacy as a fundamental right. The IT Act 2000 and the IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, have been analysed to find out the important provisions for protecting the right to privacy of people in the digital world. The need for a strong data protection law has also been discussed to protect privacy of people and to prevent the misuse of data of people, in this regard the much awaited data protection bill has been analysed which has now the Indian Government planned to introduce in the monsoon session of the Parliament in 2023 and it is named as Digital Personal Data Protection Bill, 2022.

CHAPTER 3: BREACH OF PRIVACY, CYBER CRIMES AND LOOPHOLES IN THE POLICE AND JUDICIAL SYSTEM

In this chapter the breach of privacy and its outcome in the form of cyber crimes have been analysed. In this regard, the activeness of police in the investigation of various cases of cyber crimes have been examined with the help of data provided by NCRB. Similarly the activeness of judiciary in solving the cases of cyber crimes and the activeness of judiciary in providing justice to the victims have also been examined by the utilisation of NCRB data.

CHAPTER 4: BREACH OF PRIVACY IN THE ERA OF INTERNET BANKING: A COMPARATIVE STUDY

Breach of privacy has become a very serious issue because the data stolen/accessed can be used to withdraw money from banks, to transfer money, etc. In the age of internet banking the breach of privacy and leakages/loss of data can result in a big online financial fraud or cyber fraud. In this chapter the issue of cyber fraud, online financial frauds through net banking, internet banking and digital banking have been analysed. The cases of cyber frauds, online financial frauds in India have been examined and they are compared with the cases of cyber crimes, online frauds, online financial frauds in the UK and USA.

CHAPTER 5: MISUSE OF PERSONAL DATA, CYBER CRIMES AND DECISIONS OF COURTS

In this chapter various cases of misuse of personal and confidential information of victims have been explained with the help of some case laws related to cyber crimes in which the judiciary had found the accused as guilty of cyber crimes and punishments were imposed. In this way, it has been shown that breach of privacy can result into cyber crimes and the data accessed can be used to commit various kinds of cyber crimes like cyber frauds, blackmailing, etc.

CHAPTER 6: CONCLUSION AND SUGGESTIONS

On the basis of all the important findings from this research work a conclusion has been provided. Outcome of the research has been explained in this chapter. The research questions have been explained with their answers. The hypothesis has again been discussed to find out its validity. This chapter in the end provides various helpful suggestions to protect the right of privacy and confidential data of people in the digital era. Such suggestions will be quite helpful in decreasing the cases of cyber crimes and in handling the issue of cyber risks very well also.

CHAPTER 2

THE ISSUE OF CYBER CRIMES AND PROTECTION OF RIGHT TO PRIVACY IN INDIA

2.1-INTRODUCTION

Just like other rights are important similarly the right to privacy has the same importance though in legal terms it has been recognised very recently but in the digital world this right was very necessary to be recognised for protecting the personal data and confidential information of citizens using digital and online devices or whose data is stored on the digital or online devices.

Technological usage has become an important part of the life of people using various digital and online services. The growth of technology has been making more people connect with digital and online mediums. The digital and online devices have become an affordable hub for storing various data and information. Social media has been a place to share various data and information. The financial transactions through online and digital mediums are not possible unless users have registered through their important details and confidential information, similarly there are various instances for which personal data is shared on the online and digital space. In this way, the risk of data theft has become very common because of the increasing number of cases of data violation and cyber crimes. In this way the role of cyber security laws and data protection laws become so important in protecting the right to privacy of the users.

2.2- RIGHT TO PRIVACY AND THE CASE OF PUTTASWAMY

In 2017, the right to privacy was recognised in India through the case of Justice K.S. Puttaswamy (Retd.) &Anr. vs. Union of India &Ors.[22] By the 9 Judges bench of the Indian SC the status of fundamental right was recognized in this case. It is very important to protect the dignity, autonomy & liberty and because of the proper enjoyment of fundamental freedoms in the Part III of the Indian Constitution, it was held by the Court very necessary to protect the right to privacy. According to the unanimous decision of the Court:

[22] (2017) 10 SCC 1, AIR 2017 SC 4161

> "the right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

In this way Article 21 which guarantees right to life and personal liberty includes right to privacy as well and the right to privacy is also very important to fully utilise the benefits of the fundamental freedoms provided by the Constitution. In this regard it can be said that the data theft and breach of privacy happening on the online and digital mediums are totally a violation of the fundamental right of citizens. The government must quickly trace the offenders and punish them through the laws against cyber violations. Cyber crimes are committed to steal and misuse the data of users. The organisers of online and digital apps/websites must also be treated as cyber offenders if they secretly use the data of users. The IT Act, 2000 and the IPC, 1860 has been mainly applied in the cases of cyber crimes. But India needs stronger laws against cyber crimes, especially for protecting the data of the users. The Data Protection Bill has been planned to be introduced by the government but it is pending from 2017 and still it has not been passed.

2.3- PROTECTION OF RIGHT TO PRIVACY THROUGH THE INDIAN LAWS:

Any specific law is not currently existing in India which can directly protect the citizens from breach of privacy on the digital and online platforms though whatever laws are existing in India are applied to punish the offenders. The IT Act, 2000 and various rules and regulations relating to IT Act have been very important in providing punishment to the person breaching privacy of others.

"Sensitive personal data or information of a person" has been asked to be protected according to the Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. This personal data/information includes:

- Passwords,
- Details of bank account or debit card or credit or the details of other payment instrument,
- Medical records and history,
- Sexual orientation,
- Biometric information.

According to the Rules of 2011, privacy policy has been asked to be adopted by the body corporates. Body corporate to provide policy for privacy and disclosure of information.—

"(1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;

(ii) type of personal or sensitive personal data or information collected under rule 3;

(iii) purpose of collection and usage of such information;

(iv) disclosure of information including sensitive personal data or information as provided in rule 6;

(v) reasonable security practices and procedures as provided under rule 8."[23]

This privacy policy is a kind of document which explains the plans of an organisation that how they collect data and how they use it. It gives an idea to the users how their data is treated by that organisation and what type of information is being used.

According to Section 43A in the IT Act, 2000:

"Compensation for failure to protect data.–

> Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.
>
> Explanation.–For the purposes of this section,–
>
> > (i) body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

[23] Rule 4, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

> (ii) reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
> (iii) sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit."[24]

This section says that possessing, dealing or handling of any information/data, which is personal and sensitive, by a body corporate which is not able to implement security practices, which are reasonable, due to its negligence and not able to maintain such practices due to such negligence for data protection and in such cases on the happening of wrongful loss to any person or any person gains wrongfully due to such negligence then damages will be paid by that body corporate to the person who has been affected by that wrongful loss or gain. This section is quite confusing because:

- First of all it does not impose penalties on the body corporate which is negligent in taking cyber security measures and only damages are provided to the victim even when he has been affected by the negligence of that body corporate and some wrongful gain or wrongful loss has happened,
- and secondly the maximum or minimum amount of damages have not been explained. If a big amount as damages have not been clearly explained by law then no fear of law will exist in the corporates to eliminate the negliences which exist.

Penalty can be imposed by applying section 72 of the IT Act when privacy is breached or confidentiality is breached. Section 72 provides:

[24] Section 43A, The Information Technology Act, 2000(Act No., 21 of 2000)

"Penalty for Breach of confidentiality and privacy.–

> Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both."

There are some people who can be authorised to access data according to law but not to share it with others. This section 72 does not provide the punishment for breaching privacy by the processor of data but talks about the punishment for accessing data without consent and then sharing it with others. Hence accessing data in some cases is not punished but sharing that accessed data with others is punishable. The person who accesses data is authorised by the IT Act, IT Rules or IT regulations, who has accessed data of a person without his consent then if he discloses this with any third person then the person accessing data can be punished for imprisonment upto 2 years or fine upto rupees 1 lakh or with imprisonment and fine both.

According to section 72A of the Information Technology Act, 2000:

"Punishment for disclosure of information in breach of lawful contract.–

Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both."[25]

[25] Section 72A, The Information Technology Act, 2000(Act No., 21 of 2000)

This section says that with the knowledge or with the intention if information is disclosed without taking the consent of the concerned person or by breaching a lawful contract then it is punished as an offence upto 3 years of imprisonment or fines upto Rupees 5 lakh or with the punishment of imprisonment and fine both.

2.3.1- EXCEPTIONS TO THE RIGHT TO PRIVACY

In some situations it becomes quite necessary to collect data of users and the government can collect such data under those exceptional situations. It shows that the right to privacy is not an absolute right and it is subjected to various exceptions. According to Section 69 of the IT Act, 2000:

> "Power to issue directions for interception or monitoring or decryption of any information through any computer resource.–
>
> (1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient so to do, in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
>
> (2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
>
> (3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to–
>
> (a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
>
> (b) intercept, monitor, or decrypt the information, as the case may be; or
>
> (c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine."[26]

This section 69 has provided exceptions for privacy and according to this section the government can access the data and in these cases the right to privacy can not be claimed. The reasons of accessing data and information may be for protecting:

- Sovereignty of India or integrity of India,
- For the defence of India,
- State's security,
- For safeguarding the relations of friendly nature with foreign states,
- For protecting public order,
- Concerning the above points data can be accessed for the prevention of incitement to the commission of any cognizable offence,
- Accessing data for the purpose of investigating any offence.

2.4- NEED FOR A DATA PROTECTION LAW IN INDIA

Attorney-General R. Venkataramani while appearing for the Central Government in the Whatsapp data sharing case, informed the Constitutional Bench which was headed by Justice KM Joseph, on April 11, 2023 that the new bill on the data protection is ready to be tabled in the monsoon session of Parliament. This new bill has an aim of protecting data & privacy of people and it will replace the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, which has been applicable since 2011.

2.4.1- DATA PROTECTION NEEDED BECAUSE RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

The data of people which is shared on apps and websites or on online sources, by the users, are highly misused by the organisers of those apps/websites, etc. Without the direct permission from the users various wrong things can be committed by utilising that data. like personal data of a user can be stolen, purchased or accessed by someone and on the basis of

[26] Section 69, The Information Technology Act, 2000(Act No., 21 of 2000)

that data a bank loan can be taken, especially online loans are very easy to get on the basis of such data. Any person can use the data of others for various purposes because all the essential for accomplishing these purposes are available on the databases or on the online mediums, like PAN card details, Aadhaar card details, and other personal details required for opening a bank account, getting a loan, withdrawing money from banks, booking tickets, opening social media accounts, for hiding the identity by utilising the personal data of someone else, etc. Such data is shared by the users for availing various digital/online services on the digital/online mediums and such data is stored in databases. The organisers of apps/websites either take permissions for accessing, storing and using such data or even without permissions they can also use the data of users. Due to this reason the privacy of the users are at stake and a clear law is required to prohibit the organisers or any other person to use the data of the users in any manner without their permission. Such utilisation without permission is certainly a violation of the right to privacy of the users.

In 2017, the right to privacy has already been recognised as a fundamental right in a landmark decision of the SC. The SC has also focused on protecting online personal data from fraudsters, cyber criminals or from prying eyes.

2.4.2- THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

While hearing the case related to the sharing of data by WhatsApp with Facebook, the Supreme Court was told by the Indian government that the Digital Personal Data Protection Bill, 2022 will be brought in Parliament in the Monsoon session in July, 2023. It was April 11, 2023 when the Government of India said that the new bill on data protection is ready and informed the Supreme Court about their intentions of tabling this new bill in the upcoming monsoon session of Parliament. The main intention behind drafting this new bill is to bring strong laws for safeguarding Individual privacy in the online world. If this new bill is passed from the Parliament, then various changes can occur and the first change will be related to the replacement of the rules which were notified in 2011 which were named as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules.

The definition of Data has been given in the Digital Personal Data Protection Bill 2022 as "representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means".

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 has been guiding the corporates and organisers of online services to frame and utilise various kinds of privacy policies but a strict implementation has been lacking and the penalty provisions are also very weak. In this way a strong data protection from data breach is much required and instead of policies and guidelines for data protection a strict law is highly needed which if implied strictly and if penalties are imposed quickly then the leakage of data, misuse of data can get decreased and the privacy of people can be protected. Such measures will decrease the cases of cyber crimes as well because the data which is accessed are used in committing various kinds of cyber crimes like bank frauds, identity theft, hacking, blackmailing, etc. In this way prevention of cyber crimes is also a goal of data protection law.

CHAPTER 3

BREACH OF PRIVACY, CYBER CRIMES AND LOOPHOLES IN THE POLICE AND JUDICIAL SYSTEM

3.1- INTRODUCTION

Breach of privacy is a serious issue because the data stolen or accessed can be utilised in various kinds of cyber crimes. Hence, happening of cyber crimes highly depends upon the protective measures taken to stop data from being stolen or accessed without permission. If data is stolen very easily or the utilisation of data without permission is highly existent then the number of cases of cyber crime will keep increasing as well. By preventing the data from being stolen and by preventing the organisers of apps/websites and by preventing others to use data of someone else without permission, the number of cases can be decreased and in this way the cyber risks can be managed very well as well. Protection of privacy requires quick investigation in the cases of breach of privacy, quick investigation of cyber crimes and quick justice is also needed from the side of the judiciary. In this chapter the main focus is on the activeness of police in investigation of cyber crimes and activeness of judiciary in giving justice in the case of cyber crimes. This activeness is analysed on the basis of NCRB data.

3.2- THE ISSUE OF SLOW PACE OF INVESTIGATION AS WELL AS LAZY NATURE OF TRIAL IN CYBER OFFENCES IN INDIA :

It can be said that police authorities as well the judiciary is not highly advanced in solving the cases of cyber offences as efficiently as required. The delays in filing cases of cyber offence then the slow pace of investigation followed by unsuccessful trials in courts have not been able to provide justice to the victims of cyber offences. The police is not in most cases are not very serious about the issues of breach of privacy due to which the victims whose right to privacy have been breached face a lot of difficulties in filing a report. Even if a case is filed then the investigations remain too slow. In this way the courts also get very less strong evidence against the accused and in most of the cases either the accused is set free or no trace of the accused is found or the case remains pending for a long time in that court. In other countries at least the police and judiciary have been quite active in reporting the cases and in finally deciding the outcome of the cyber related cases, but in India big reforms are required to make the police quickly report the cases and start the investigations very fast and then to very quickly file their final report to the judiciary. The judiciary also has to be ready to pursue the cases in a very fast manner because there are much data which shows that either the judiciary has taken very much time in finalising the cases or the judiciary was not able to be convicted for penalising the accused on the basis of existing evidence.

There are units like FBI & IC3[27] in the United States which are responsible for doing proper investigation in cyber crime cases. There was a 82% success rate in 2020 of IC3 in exposing the cyber crime cases in which money of victims had been lost and by following the advanced mechanism the IC3 was able to detect and recover the lost money as well. On the other hand, the Indian Police had a total 16783 cases for investigation in the year 2016 but only in 2710 such cases the charge sheet was filed in that year. In this way only in 16% cases the police was able to complete its investigation and file the chargesheet in 2016.

The problems of slow investigation are very easy to solve if the investigating police officers are highly advanced in understanding the knowledge of computer science & information technology and if the police who are investigating the cases of traditional crimes has been given the charge of investigating the cyber offences then obviously they will take much time in completing the investigations. A knowledgeable team of police authorities can very quickly collect strong evidence in the cases of cyber crimes and then can arrest or identify the accused as well. Such strong evidence will help the judiciary also to understand the seriousness of the cases and to rely on the evidence and them to punish the accuseds.

Only the knowledge and getting skilled in computer science & IT can not be sufficient because there is a big requirement of improving the infrastructural facilities as well in solving the cases of cyber crimes. Availability of computers, laptops, projectors, internet, cyber security softwares, cyber security devices, etc. are very important objects which must exist in all police stations and courtrooms. There must be experts in police stations who can trace any activities of cyber misuses. The courtrooms must be highly advanced ro examine any kind of electronic evidence. These basic necessities can increase the pace of investigation and can certainly help in very quickly finalising the trails in courts.

[27] Internet Crime Complaint Center

3.2.1-Investigation and finishing the investigation of cases of cyber crimes by police in India-

In 2016, 24187 cases of cyber crimes for investigations were dealt by Indian police while only 3712 cases were recorded by NCRB in which investigations had reached to filing of chargesheets. Here, the data related to India (provided by NCRB) has been mentioned for investigation and conclusion of investigation by police in the year 2016.

3.2.1.1- Investigation of cyber offences under IT Act- According to the "NCRB data"[28], cases in 2016 handled for investigation by police for crimes related with the IT Act are-

Table 3.1

Offences in IT Act	Cases of previous year pending investigation	Cases reported in 2016	For investigation total number of cases
Tampering computer source documents	83	78	161
Offences related to computers (Section 66 & 66B to 66E)	6673	6818	13491
Offences under sec 66	4061	3321	7382
Offences - sec. 66B	115	196	311
Offences - sec 66C	1197	1545	2742
Offences- sec. 66D	1188	1597	2785
Offences- sec. 66E	112	159	271

[28] https://ncrb.gov.in/en/crime-in-india-table-addtional-table-and-chapter-contents?page=27

Cyber terrorism under- sec. 66F	11	12	23
(Publication) (Transmission of obscene) (sexually explicit content) offences Under- sec 67 & 67A-67C	694	957	1651
Offences under sec. 67 & 67A	673	930	1603
offences- sec. 67B	6	17	23
Offences - sec. 67C	15	10	25
(Breach of confidentiality) (privacy and disclosure of information in Breach of Lawful contract)	22	35	57
Other cases	687	713	1400
Total	**8170**	**8613**	**16783**

Table 3.1 shows that a total of 16,783 cases were there for investigation in 2016 and it included the new cases of cyber crimes investigated by the police in 2016 as well the previous year cases in which investigation had still not been completed. These cases were related to various offences provided by the IT Act, 2000. It shows that pending cases before 2016 were nearabout equal to the new cases registered for investigation in 2016. It shows that Police is continuously getting a lot of cases for investigation but due to its slow approach in investigation a lot of cases become pending.

3.2.1.2- Conclusion of investigation by police under the IT Act-

In the same year 2016, the police had concluded the investigation of cyber crimes related to the IT Act-

Table 3.2-

Sl.No.	**Offences in the IT Act**	**Cases in which chargesheets were submitted**
1	Tampering computer source documents	32
2	Offences related to computers (Section 66 & 66B to 66E)	2018
3	Offences under sec 66	1453
4	Offences - sec. 66B	52
5	Offences - sec 66C	267
6	Offences- sec. 66D	205
7	Offences- sec. 66E	41
8	Cyber terrorism under- sec. 66F	6
9	(Publication) (Transmission of obscene) (sexually explicit content) offences Under- sec 67 & 67A-67C	409

10	Offences under sec. 67 & 67A	400
11	offences- sec. 67B	6
12	Offences - sec. 67C	3
13	(Breach of confidentiality) (privacy and disclosure of information in Breach of Lawful contract)	16
14	Other cases	229
15	**Total**	**2710**

Table 3.2 talks about the number of investigations which were completed by police in 2016 when it was investigating the cases of cyber crimes under the IT Act, 2000. There were only 2710 cases of cyber crimes in which police had filed chargesheet in 2016 while Table 3.1 shows that there were a total 16783 cases in which police were doing investigation concerning various kinds of cyber crimes under the IT Act, 2000. It shows that the success rate of police in completing the investigation and filing the chargesheet was only nearabout 15%. It shows that police is very slow and due to lack of technological knowledge and due to less experience in the IT field the Indian police is highly incapable in quickly finishing the investigations.

3.2.1.3- Police Investigation in 2016 for cyber offences under IPC-

Table 3.3-

Offences in IPC	**Cases of previous year pending investigation**	**Cases reported in 2016**	**For investigation total number of cases**
1- Data theft	101	86	187
2- Criminal Breach of Trust / Fraud	46	56	102
- Credit / Debit card	12	26	38
- Others	34	30	64
3- Cheating	2373	2329	4702
4- Forgery	102	83	183
5- Counterfeiting	9	10	19
6- Fabrication / Destruction of Electronic records for evidence	4	6	10
7- Others	970	950	1920
Total	**3605**	**3518**	**7123**

The cases concerning cyber crimes booked under the IPC which were investigated by police in 2016 have been mentioned in Table 3.3. It shows that a total 7123 cases were investigated by the police in which new cases in 2016 were 3518 but the pending cases were higher than the new cases for investigation. With 3605 cases of previous years and 3518 cases in 2016, it can be said that police get a big number of cases for investigation for cyber crimes under IPC as well. Pending cases are a big burden on investigation. More number of pending cases than new cases is a serious issue.

3.2.1.4- Conclusion of investigations by police in 2016, under the cyber crimes in IPC-

Table 3.4-

Offence in IPC	**Cases in which chargesheets were submitted**
1- Data theft	22
2- Criminal Breach of Trust / Fraud	12
- Credit / Debit card	4
- Others	8
3- Cheating	355
4- Forgery	16
5- Counterfeiting	12
6- Fabrication / Destruction of Electronic records for evidence	4
7- Others	438
Total	**859**

Table 3.4 shows that the police was able to complete the investigation on 859 cases only in 2016 which were related to the cyber crimes booked in IPC. 859 cases in which chargesheets were filed are very less than the total cases which police were investigating in 2016 under IPC for the cases concerning cyber crimes. In Table 3.3 it was found that police was investigating 7123 cases in 2016, but with the chargesheet filed only in 859 cases the success rate of police is found to be near about 12% only.

3.2.1.5- Police investigation for cyber crimes in Special and local laws in 2016-

Table 3.5-

Cyber Offences under Special & Local Laws	**Cases of previous year pending investigation**	**Cases reported in 2016**	**For investigation total number of cases**
Copyright Act, 1957	81	181	262
Trade Marks Act, 1999	0	**2**	2
Other special & local laws	14	3	17
Total	**95**	**186**	**281**

3.2.1.6- Conclusion of police investigation in 2016 for cases of cyber crimes under special and local laws-

Table 3.6-

Cyber Offences under Special & Local Laws	**Cases in which chargesheets were submitted**
Copyright Act, 1957	136
Trade Marks Act, 1999	0
Other special & local laws	7
Total	**143**

Table 3.5 gives the number of cases for investigation done by Police under various special and local laws. Table 3.6 shows that the Police in 2016 was able to file chargesheets in only 143 cases when it had investigated a total 281 cases.

Here police has a success rate of newbout 50% which shows that the rights of Copyright holders, trade marks holders, etc. are taken very seriously by the police. Also the owners of trademarks, copyrights are mostly rich and influential persons, which is also a reason for the activeness of police in cyber crimes related to such cases. Though compared to the investigation in IT Act and IPC the success rate of police is much higher in investigation of cyber cases concerning special and local laws, But still it is not quite satisfactory. Copyright violation in this digital world is a big issue and quick investigation in such cases are highly required.

3.2.2- Handling of cyber crime cases by Courts in India - According to NCRB data, total 10164 had come for trial in 2016 but only 201 convictions had happened, rest of the cases were either discharged, acquitted, disposed offor they remained pending in 2016.

3.2.2.1- In 2016, Trial by courts in cases related to the IT Act-

Table 3.7-

Offences in IT Act	**Cases from previous years of Pending trial**	**Cases sent for trial in 2016**	**Total cases for trial**	**Compounded cases**
Tampering computer source documents	70	32	102	0
Offences related to computers (Section 66 & 66B to 66E)	3123	2018	5141	33

Offences under sec 66	2521	1453	3974	21
Offences - sec. 66B	72	52	124	0
Offences - sec 66C	276	267	543	12
Offences - sec 66D	199	205	404	0
Offences - sec 66E	55	41	96	0
Cyber terrorism under- sec. 66F	1	6	7	0
(Publication) (Transmission of obscene) (sexually explicit content) offences Under-sec 67 & 67A-67C	605	409	1014	3
Offences under sec. 67 & 67A	590	400	990	3
offences- sec. 67B	11	6	17	0
Offences - sec. 67C	4	3	7	0

(Breach of confidentiality) (privacy and disclosure of information in Breach of Lawful contract)	10	16	26	2
Other cases	400	229	629	0
Total	**4209**	**2710**	**6919**	**38**

In Table 3.7, the total number of cyber crime cases under the IT Act, 2000 tried by the court in 2016 are mentioned. Concerning cyber crimes in 2016 there were a total 6919 cases for trial and nearabout 60% cases for the trial were the case still pending before 2016. In 2016, 2710 cases for trial were brought before the courts. It shows that a lot of cases under the IT Act concerning cyber crimes were pending and it shows the issue of slow trial in the Indian courts in solving cyber crime cases.

3.2.2.2- Conclusion of trial in 2016 by courts in cases related to the IT Act-

Table 3.8-

Offences in IT Act	**Cases convicted**	**Cases acquitted or discharged**	**Cases disposed off by court**	**Cases remained pending**
Tampering computer source documents	1	15	16	86
Offences related to computers (Section 66 & 66B to 66E)	134	306	473	4668

Offences under sec 66	119	244	384	3590
Offences - sec. 66B	1	3	4	120
Offences - sec. 66C	5	26	43	500
Offences - sec. 66D	9	24	33	371
Offences - sec. 66E	0	9	9	87
Cyber terrorism under- sec. 66F	0	0	0	7
(Publication) (Transmission of obscene) (sexually explicit content) offences Under-sec 67 & 67A-67C	10	46	59	955
Offences under sec. 67 & 67A	9	45	57	933
Offences - sec. 67B	1	1	2	15
Offences - sec. 67C	0	0	0	7

(Breach of confidentiality) (privacy and disclosure of information in Breach of Lawful contract)	0	1	3	23
Other cases	14	25	39	590
Total	**159**	**393**	**590**	**6329**

Table 3.8 shows that only in 159 cases out of the total 6919 cases mentioned in Table 3.7, the accused were convicted and 6329 cases still remained pending. In 2016, only in just more than 2% cases convictions were given by the court out of total 6919 cases for trial under the IT Act. It shows that the judiciary is very slow in delivering justice when only in 2% cases conviction is granted and nearabout 92% case remained pending. It shows that police were also not able to collect strong evidence against the accused due to which a quick conviction was not possible. The 2% success shows that the judiciary has to take some quick approach in solving the cases of cyber crimes.

3.2.2.3- In 2016, trial by court in cases related to IPC-

Table 3.9-

Offence in IPC	**Cases from previous years of Pending trial**	**Cases sent for trial in 2016**	**Total cases for trial**	**Compounded cases**
1- Data theft	26	22	48	0
2- Criminal Breach of Trust / Fraud	44	12	56	0

- Credit / Debit card	12	4	16	0
- Others	32	8	40	0
3- Cheating	540	355	895	0
4- Forgery	42	16	58	0
5-Counterfeiting	28	12	40	0
6- Fabrication / Destruction of Electronic records for evidence	1	4	5	0
7- Others	927	438	1365	1
Total	**1608**	**859**	**2467**	**1**

Total 2467 cases for trial under IPC have been shown by Table 3.9 concerning cyber crimes. The number of new cases for trial were nearabout half of the pending cases from previous years. The judiciary is quite slow in solving the cyber crime cases under IPC as well because a big number of cases are pending here as well.

3.2.2.4- Conclusion of trial in 2016, in cases related to IPC by the courts-

Table 3.10-

Offence in IPC	**Cases convicted**	**Cases acquitted or discharged**	**Cases disposed off by court**	**Cases remained pending**
1- Data theft	0	6	6	42

2- Criminal Breach of Trust / Fraud	0	1	1	55
- Credit / Debit card	0	0	0	16
- Others	0	1	1	39
3- Cheating	4	28	32	863
4- Forgery	0	3	3	55
5-Counterfeiting	0	1	1	39
6- Fabrication / Destruction of Electronic records for evidence	0	0	0	5
7- Others	9	28	38	1327
Total	**13**	**67**	**81**	**2386**

Only in 13 cases of cyber crimes under IPC, convictions were granted as shown by Table 3.10. Table 3.9 showed that total 2467 cases were there for trial but conviction happened in only 13 cases which was just bedaabot 0.50% of total number of cases. 2386 cases still remained pending, meaning the judiciary needed more time to solve these cases. In this way the slow trial is seriously a big problem. The wait for justice is quite long and due to this fear people fear to approach police and judiciary and instead of that they keep tolerating the cyber crimes

3.2.2.5-Trial of cases by court in cyber crimes related to special and local laws in 2016-

Table 3.11-

Cyber Offences under Special & Laws	**Cases from previous years of Pending trial**	**Cases sent for trial in 2016**	**Total cases for trial**	**Compounded cases**
Copyright Act, 1957	611	136	747	1
Trade Marks Act, 1999	0	0	0	0
Other special & local laws	24	7	31	0
Total	**635**	**143**	**778**	**1**

3.2.2.6-CONCLUSION OF TRIAL BY COURTS IN 2016, IN CASES OF CYBER CRIMES RELATED TO SPECIAL AND LOCAL LAWS-

Table 3.12-

Cyber Offences under Special & Laws	**Cases convicted**	**Cases acquitted or discharged**	**Cases disposed off by court**	**Cases remained pending**
Copyright Act, 1957	29	82	112	635
Trade Marks Act, 1999	0	0	0	0
Other special & local laws	0	0	0	31
Total	**29**	**82**	**112**	**666**

Total 635 cases were there for trial before court under special and local laws as shown by Table 3.11, in 2016. Out of these total cases only in 29 cases convention happened which was just 5% of the total cases and pending cases which needed more time to be solved remained 666 as shown by Table 3.12.

3.3- SUBEX HAD A REPORT TO COMPARE WRONGFUL CYBER RELATED ACTIVITIES IN THE WORLD, RELEASED IN 2020-

3 months in 2019, India had become the most cyber-attacked country, this was said by a report of Subex[29], a firm in Bengaluru.

Release date of report was 27 February 2020, and it told that in 2019, majorly the US had faced many cyber-targets but India got top rank in April 2019, May 2019 and June 2019.

Report brought the information that countries like the US, UK, India, Ukraine, Singapore, UAE, Japan, Nigeria, Spain & South Korea and Spain had been made targets of cyber attacks in large numbers in 2019 compared to the rest of the countries.

Cyber-attacks which were applied to target India in 2019 mostly had its origin from Slovenia then in Ukraine, then in Czech Republic, and China & Mexico.

Country from where India was targeted and no. of cyber attacks-

- Slovenia : 74,988
- Ukraine : 55,772
- Czech Republic : 53,609
- China : 50,000
- Mexico : 35,201

Target no 1 were the industries of Oil & gas in India for cyber attacks. Common targets of most of the cyber attacks in India were sectors of crucial infrastructure and it mostly targeted banking, then defence then manufacturing, and rest of the sectors. according to the report. Oil and gas industries were the most targeted by these attacks.

[29] https://theprint.in/tech/india-was-the-most-cyber-attacked-country-in-the-world-for-three-months-in-2019/374622/

Subex report also found many targets which were inflicted from India on other countries.

- For cyber attacks targeted Countries from India & no. of attacks
    - Iran targeted most : 5,700
    - Vietnam : 4,150

3.4- SOME BIG CASES OF CYBER ATTACKS IN INDIA-

1. Cosmos Bank Cyber Attack, Pune -

Year: 2018
Target : Cosmos bank
Location of bank: Pune

- Targeted things-
    - Rs 94.42 crore from the Cosmos co-operative bank ltd,
    - information of visa holders & debit card holders,
    - bank's ATM server.

28 countries were also targeted in this attack.

2. ATM System of Canara Bank -

Year: mid-2018
Victim- Canara Bank ATM servers
Loss: near about 20 lakh rupees swiped out from many consumer's accounts.

Reason- details of ATM of near about 300 users were acquired by cyber attackers- 50 of them are estimated as victims. To steal the information of debit cardholder's hackers used skimming devices.

3. Hacking of UIDAI Aadhar Software-

Year - beginning of 2018

Loss- various information and secret information were released online, like

- Aadhar details,

- PAN number, mobile number,
- bank account numbers,
- Key personal info of individual card holders,
- IFSC codes, etc.
- Selling of Aadhar cards started, photocopies of that had also been sold, it became like a commodity to sell.

4. Hacking on Indian Healthcare Websites

Year : 2019

Victim: the healthcare websites of India

Loss:

- hacking of Indian website
- Info. of 68 lakhs patients & doctors

5. SIM Swap Scam

Year of arrest of accused people: August 2018 location of arrest : Navi Mumbai

Mode of crime: blocking SIM cards by accessing SIM card details, details were used for stealing money from bank : used for hacking also.

3.5- COMMENTS

Modern technologies have grown in an uncontrolled manner which has become a prime reason for increasing the cases of cyber misuse and in violating the right to privacy of the individuals. One big example in this regard is the uncontrolled growth of the affordable mobile phones and smartphones which lack proper cyber security measures and which are quite vulnerable for many cyber offences. The easy connectivity of the whole world through various online devices have made the jobs of cyber criminals living outside India very easy. In this regard a proper extradition policy is required to start cases against such transboundary cyber criminals and to punish them by bringing them to India. In this regard the role of international laws has to be very crucial. All countries must unite together to frame a universal laws against breach of privacy which is violated through the digital and online mediums and they must agree to extradite the cyber offenders who violated the right to privacy of the victims living in other countries. The current system has no such proper facility to get easy access to the cyber offenders living in other countries who have violated the rights of the victims living in other countries. The Indian IT Act has talked about persecuting the cyber offenders living in other countries but in reality the execution of this measure has been quite rare even when India has suffered many cyber attacks from the cyber offenders living in various foreign countries.

People using digital and online services must have the knowledge of the capabilities of police in investigation of cyber offences, it will warm the people that the Indian police is currently not highly capable in quickly finishing the investigation in the case of cyber crimes and if these users also become victims of cyber crimes then they must also have to face such situations and wait for a long time to get justice. By knowing these, the users will tend towards the utilisation of more cyber security measures and they will take care of their personal data as much possible as it can be from their side.

The same information about the judiciary must also be possessed by the people and they must know that the Indian judiciary is quite slow in quickly solving the disputes in the cases concerning cyber crimes. Delayed justice prevents other people to approach courts and for cybercrimes also people may not like to approach courts if slow justice is provided by judiciary. If the cases of cyber crimes have to be prevented then the judiciary must be very quick in disseminating justice. Quick investigation with quick dissemination of justice in cyber crimes will decrease the cases of cyber crimes and more and more victims will approach with their concerns to the police and judiciary. Such approach will protect the right to privacy of the people as well.

Police must utilise modern technologies and experienced cyber experts for conducting quick investigation of cases of cyber crimes. A separate court must be formed to deal only with the cases of cyber crimes where the judges and lawyers must have adequate information and a good experience of the cyber world.

CHAPTER 4

BREACH OF PRIVACY IN THE ERA OF INTERNET BANKING: A COMPARATIVE STUDY

4.1- INTRODUCTION

Breach of privacy has become a very serious issue because the data stolen/accessed can be used to withdraw money from banks, to transfer money, etc. In the age of internet banking the breach of privacy and leakages/loss of data can result in a big online financial fraud or cyber fraud. In this chapter the issue of cyber fraud, online financial frauds through net banking, internet banking and digital banking have been analysed. The cases of cyber frauds, online financial frauds in India have been examined and they are compared with the cases of cyber crimes, online frauds, online financial frauds in the UK and USA.

4.2- LEAKAGE/LOSS OF CONFIDENTIAL DATA AS PRIME REASONS FOR CYBER CRIMES

The idea of law suggests that people are helpless without legal protective measures so a standard of law is required to ensure them. After applying this we may state that PC's are powerless so standard of law is required to secure and protect them against digital wrongdoing. Following are some reasons.

- Loss of proof
- Negligence
- Complex
- Easy to access
- Capacity to store information in little place.

Indian people are moving beyond just searches, social networks, and even more sophisticated practices, including online shopping and banking. India is in the wake of a digital revolution. Through financial product transactions, already 70% of urban consumers are digitally driven, which means that during the purchasing process of a financial product they use at least one digital platform.

With the continuous computerized drive in India, the quantity of clients deciding on the internet banking is relied upon to twofold to arrive at 150 million imprints by 2020, from the current 45 million dynamic urban internet banking clients in India, as indicated by a report drafted by Facebook and The Boston Consulting Group (BCG).

In a report, named “ENCASHING ON DIGITAL: Financial Services in 2020″, the two firms have featured the rising impact of computerization in monetary administrations and the change required to benefit as much as possible from this transformation. “India couldn’t be progressively prepared for an advanced upset in money related administrations with government meditations on one hand and developing purchaser mindfulness on the other.

4.3- BANKING AND INTERNET BANKING

In every nation’s economy, the banking system still plays a major role. It is important for every nation because it serves all facets of society’s credit needs. India’s growth potential is focused on its strong banking structure.

The absorption of IT in the banking sector has transformed the way the banking sector works. Banks had to opt for this recent update to survive in the current globalized world. Some banking today takes place as you snack coffee or make a big call. At your doorstep are ATMs. Banking services 24×7 are open. More plastic cards than paper currency are in your pocket.

Internet banking or E-banking is the term that connotes and includes the whole circle of innovation activities that have occurred in the financial business. Internet banking is a conventional term utilizing electronic stations through phone, cell phones, Internet, and so on for conveyance of banking administrations and items.

Internet banking as the conveyance of bank’s data and administrations by banks to clients through various conveyance stages that can be utilized with various terminal gadgets, for example, a PC and a cell phone with program or work area programming, phone or advanced TV.

Internet banking is characterized by Barron’s Dictionary (2006) as “A type of banking where assets are moved through a trade of electronic signals between money related foundations, instead of trade of money, checks, or other debatable instruments”.

Numerous years prior, under the arrangement of conventional financial when a client needed to open a ledger, the individual must be available at the parts of the bank. Customary finance offers individuals an individual’s association. Fixed calendar, badly arranged areas, and constrained monetary items offer are a portion of the disadvantages of conventional banks.

For internet banking, the most effortless approach to open a sparing record is by connecting to a current record. Business exchanges can be completed by only a “tick”. With no verbal correspondences and no long line at the counter, the clients despite everything can deal with any records by remaining at home.

Internet banking is progressively advantageous and offers 24 hours in 7 days of banking administration and greater adaptability as diverged from that of Internet banking.

4.3.1- ACCENTS OF INTERNET BANKING

Banking functions are conducted through the Internet.

- This eliminates the typical regional barriers since consumers can be served in various jurisdictions.
- In all times as well as on the day, including vacations and Sundays, e-banking enhances bank transactions.
- It offers a variety of additional distribution platforms for both the client and the banker that are more efficient and cost-effective.
- It is based on science and technology that saves bankers and customers time and energy, i.e. using electronic devices.
- Its specific characteristics lie in maintaining transaction stability, client confidentiality, and transaction transparency.

4.3.2-- IS INTERNET BANKING BENEFICIAL FOR THE ECONOMY?

- **Comfort**

  - This is the absolute most significant advantage that exceeds any deficiency of Internet Banking. Making exchanges and installments directly from the solace of home or office at the snap of a catch without venturing out is an office none might want to forego.

  - Monitoring accounts through the Internet is a lot quicker and advantageous when contrasted with heading off to the bank for the equivalent. Indeed, even non-value-based offices like requesting checkbooks Internet-based, refreshing records, enquiring about loan fees of different monetary items and so forth become a lot less difficult on the Internet.

- **Better Rates**

  The banks remain to pick up fundamentally by the utilization of Internet banking as it infers lesser physical exertion from their end. The need to get bigger spaces for workplaces and utilize more staff to manage the clients is essentially diminished making it monetarily gainful to the banks.

  This implies a part of investment funds accumulated can be given to the clients as far as higher rates on stores and lower rates on credits. To empower Internet banking most banks offer least or no store represents internet banking and lower punishments on early withdrawal of Fixed Deposits.

- **Administrations**

  Technology has made it very advantageous for the bank just as the client to access to a large group of awesome administrations by basically signing in. These administrations incorporate budgetary arranging capacities, useful planning and gauging apparatuses, advance number crunchers, speculation investigation devices, and value exchanging stages which are accessible as basic applications on the bank’s site. Moreover, most banks likewise give the office of online tax documents and assessment readiness.

- **Versatility**

Internet banking has above and beyond over the most recent couple of years as portable Internet banking which agrees on boundless portability to the client who would now be able to deal with budgetary exchanges even while progressing.

- **Condition well disposed**

Another significant advantage of the idea of Internet banking is that it is useful for the earth as it chops down the utilization of paper, lessens contamination as individuals don’t need to travel genuinely, and furthermore doesn’t include discharges. Anyway, the current pattern of solely utilizing the online mode to make a wide range of exchanges has a couple of entanglements that may demonstrate expensive over the long haul except if made preparations for from the earliest starting point.

Net Banking is an electronic payment system, a service offered by banks/financial institutions. It allows an individual to undertake different kinds of transactions from the comfort of their home, through the internet. The development of the internet and technology has been enormous and has ventured into the field of banking. ICICI Bank was the first Indian Bank to facilitate Internet Banking, which was also then referred to as “Convenience Banking.”

Though India has been digitized for quite some time now, it has taken a significant leap in the last year during the COVID-19. Digital appearance has grown considerably in the forms of payments, online meetings, video conferences, and webinars, etc.

During these times, we have seen a sharp rise in the number of frauds, white-collar crimes, phishing, scams, etc.; while reducing the use of technology may not seem like a viable option, the only workable recourse is following the precautionary measures, being alert and vigilant, so we are in a safe place.

This part dwells upon the cyber risks associated with Net Banking, how the legislation is recognizing technology and making amendments to the existing laws; and suggests some of the solutions that may curb the cyber-crimes.

4.4- NET BANKING IN INDIA

As mentioned earlier, ICICI Bank began facilitating online banking services in 1996, followed by some other banks. On the opposite hand, the general public sector banks were reluctant to adopt internet banking practices. While net banking is not a separate business but an ancillary service provided by the banks/financial institutions; the depository financial institution of India took the lead in adapting to technology and taking banking to the doorsteps of its customers. Some banks blame it on the shortage of laws and regulations for them to go online while others are comfortable and not willing to switch from traditional banking methodology.

It has always been a concern for the banks that if they provide a net banking facility, how they going to be regulated; in the absence of proper laws, will they have autonomy in their affairs or will they be under the radar of the Reserve Bank of India (RBI).

The RBI had welcomed suggestions from the industry and adopted recommendations of the "Working Group on Internet Banking," which examined three driving forces like Technology and its allied security issues, legal issues, and regulatory and supervisory issues. The RBI then gave some independence to the banks, while ensuring that for some issues, the banks strictly follow the provisions of the RBI.

The Indian government has been promoting "Digital India" to quite a far-reaching extent. This campaign has been initiated to provide the citizens with services through the mode of internet and thereby increasing the scope of connectivity throughout the country.

To promote the use of internet banking technology, the Ministry of Finance implemented Public Financial Management Systems (earlier known as Central Plan Scheme Monitoring System), which is an element of the digital India campaign. The primary objective of Public Financial Management Systems is to establish an efficient fund flow system and establish a proper accounting network. Further, it has widened the scope of online payments amongst users.

4.4.1- DRAWBACKS OF NET BANKING IN INDIA

There are many forms of cyber frauds in the banking industry; almost every day we read headlines about people falling prey to the internet’s wrong-doers, losing their money while making payments, or availing other transactional services over the internet. Privacy and security of the customers are one of the biggest drawbacks of net banking.

It cannot be denied that despite having specific statutes in place, like the Information and Technology Act, 2000 (IT Act) and Indian Penal Code, 1860 (IPC) for curbing cybercrimes, wrong-doing by fraudsters concerning net banking is increasing rapidly.

There is a lacuna in the legal system and the administration for tackling these crimes and adjudicating the wrong-doer. It has been over a decade and yet we as a nation are not able to curb or even reduce the frequency of these crimes.

The reason being that there is a gap between the training methodology provided; the corporate houses are easily able to hire good analysts to protect data and secure their channels, however, on the other hand, the government and other small banks lack these resources.

Security of net banking transfers becomes a major concern. The transactions made over the internet are flexible, effective but at the same time, can be untraceable, made anonymously, and due to lack of effective audit, facilitate immediate movement of money. Identifying and avoiding unauthorized and illegal activities becomes a major apprehension for the banking sector.

Application of money laundering laws could also be inadequate for other types of electronic payment such that banks are exposed to the vulnerability of money laundering.

Even after undertaking preventive measures like Know Your Customer (KYC) and Biometric Verification, the security and privacy concerns are major roadblocks for effective net banking in India.

4.4.2- LEGAL OUTLOOK ON SHORTENING THE EVILS ASSOCIATED WITH NET BANKING

Internet banking fraud can be defined as a mala fide illegal act by any individual to illegally obtain sensitive data or finances from banks/financial institutions via the internet. The IT Act primarily governs the process of net banking.

Cyber frauds include phishing, malware attacks, identity theft, debit/credit card frauds, embezzlement, frauds relating to loans, fraud by forgery, etc. The substantive and procedural laws and rules governing the areas of banking, internet information technology are effective mechanisms to prevent such internet banking frauds. To counter such crimes, the IT Act has incorporated certain legal provisions creating legal rights and their corresponding duties to the bankers and the customer. Failure to adhere to such provisions would result in penal provisions under the Act.

Apart from the relevant provisions of the IPC, the IT Act also provides punitive provisions for identity theft and cheating through technology under Section 66C and 66D of the IT Act along with a remedial right by way of compensation and penalty for breach of data under Section 43A and 72 of the same Act.

The Act imposes a legal duty that the bankers protect the sensitive personal data in the system which the banks/financial institutions own, hold, and operate. Any negligence would result in the payment of compensation for the victims. Vide its language, the legislation vide Section 43A and Section 72 of the IT Act, has laid down penalizing measures against the bank in the event of failure to maintain the confidentiality of its customers, in the event of Legal outlook on shortening the evils associated with net banking

The Act comes down heavily on online fraudsters by the virtue of provisions Section 66C and 66D of the IT Act. Both the provision punishes acts like online frauds, computer attacks, and other digital frauds. The provisions of the IT Act that deal with net banking are: attacks, and other digital frauds.

It is pertinent to measure here that the government of India to further insulate the mechanism for protection of personal data has tabled a bill called the "Personal Data Protection Bill 2019" and the same is under a consultative process. The bill aims at protecting the privacy of individuals relating to personal data under the guidance of a regulatory body concerning the data protection authority of India.

Privacy is regarded as a Fundamental right by extending the scope of Article 21 by the Hon'ble Supreme Court in Puttoswamy's case. Post this case, privacy was considered an element of the right to life and the banks/financial institutions found it difficult to identify their online customers as cards issued by the institution and storing of sensitive personal data could not be made mandatory. The internet banking service accepts the requests for the opening of accounts and has made the procedure very simple, faster, and easier.

Some of the options to be kept in check by the banks/financial institutions as well as the customers to be safe against these crimes are:

To install good antivirus software for the computer, tab, laptop and to protect the servers. This protects the devices and data from internet threats, viruses, and malware. One must always scan any external drive for viruses, before inserting it into the device. Another precaution to be undertaken is to download any software, application, anti-virus, etc. only from a genuine and determining source.

One must also keep in check that they enter into net banking transactions through their device or devices of someone known to the individual. Using a third party's electronic device for banking should be avoided. If used, it is to be checked that the credentials do not get saved on the server, and to clear the history and caches is important. Using credentials that are hard for people to guess.

Also, it is always best to use a different password for banking than one would usually use for social media, shopping, etc. It is also advisable to use different passwords for different banks.

The prosecuting agencies have set up dedicated cybercrime cells across all the districts in India for effective redressal of the grievances, however, each Bank also should incorporate their redressal cell, that could identify internet banking frauds happening to their banks and can at regular intervals, forward such reports and complaints to the cyber cell.

One must avoid opening links sent from undetermined sources. Choosing the correct website is important – many fake websites on the internet look like internet banking sites, if one falls for a fake one, an individual's credentials are jeopardized and they can be a victim of a phishing attack.

4.5- CYBER CRIMES, CYBER FRAUD AND NET BANKING

If a fraud related to net banking or ATM transactions, or any other online transaction happens, you have to raise a complaint. But, before filing a written complaint with the bank or the card issuer, the victim must have following documents-

- Bank statement of the last six months of the concerned bank.
- Make a copy of SMSs received related to the alleged transactions.
- Take copy of your ID proof and address proof as shown in the bank records.
- Lodge a complaint in your nearest police station explaining the complete incidence along with the above documents.
- There are several fake apps being floating around in the cyber world. In case of any financial fraud committed through an app, in addition to the above mentioned documents, also furnish the screenshot of the malicious app and the location from where it was downloaded.
- Filing Complaint-

  The complaint can be filed in the nearest police station. if any of the police officer does not lodge an FIR then a direct complaint can be made to the magistrate.

Loss due to cyber crimes according to information given in the Parliament-

Table 4.1

FY	**Loss** **ATM/Debit Card, Credit Card and Internet Banking**,	**Amount involved in cyber crimes**
FY 19-20	Rs 58.61cr	Rs 194.39cr
FY 20-21	Rs 63.40cr	Rs 195.80 cr

Table 4.1 shows that the amount of loss is very big and it is continuously increasing. At least one third of amount related to loss caused by cyber crimes are related to ATM/Debit Card, Credit Card and Internet Banking,

Table 4.1 is related with reported cases of cuber crimes. There can be many cases which are still not reported. Though, those unreported cases may be related to some small losses but still it must be reported so that real number of cyber crimes can be identified.

4.5.1- PHISHING AND E-BANKING

A victim of phishing can become a victim of hacking or identity theft because the information gathered on the victim can be used in many unlawful ways. Although identity theft is mainly associated with online shopping, the act of payment being made for online purchasing of goods or services can be considered a banking transaction.

Identity theft is described as the acquisition of sufficient information about a victim which enables the attacker to use the funds in the victim’s account to make payments for goods and services. It can include personal information such as credit card numbers, phone numbers and email addresses.

Credit card theft and usage, falsified loans, mortgage fraud, medical benefit fraud, and theft of funds in financial accounts are some of the identity theft attacks.

4.5.2- IDENTITY THEFT

Identity theft is believed to be the most common cybercrime being done to individuals. It was found that 61% of all cybercrime victims reported misuse of their credit card, 33% reported misuse of savings or chequing accounts and the others reported that their wireless account or telephone have been misused.

The four categories of identity theft, These are:

- Financial identity theft – Using another's identity to obtain goods and services
- Identity cloning – Using another's information to assume his or her identity in daily life
- Business identity theft – Using another's business name to obtain credit
- Criminal identity theft – Posing as another when apprehended for a crime.

4.5.3- HACKING

Hacking is considered a destination for a phishing attacker. It is the illegal breaking into a computer system by deliberately passing through security measures with the aim of stealing information that is stored on the computer or network.

These cyberattacks are easily executed by using a Trojan horse virus. These attacks are usually committed for profit or for bragging purposes. The actual cost of hacking is difficult to quantify and many companies hide the fact that they have been attacked.

Hackers are generally described as white, black and grey hats. White hat hackers are scoped out of this study because they are hackers working for the good of system security. They are usually employed by organizations to keep data safe from bad hackers by finding areas of vulnerabilities. They are sometimes referred to as 'ethical' hackers. This study is concerned about the impact of bad hackers.

The majority of hackers are black hat hackers. These hackers intrude into systems in an unauthorized manner with malicious intentions. They usually steal, exploit and sell information and in general are motivated by personal gain.

Grey hackers are those who hack mainly for fun. Their motives at times are unclear and it is expected that they can change their behavior quite easily. Both black and grey hat hackers are incorporated into the proposed research model as indicator variables for the 'Hacker' construct.

4.5.4- INSTRUCTION BY RBI TO INFORM THE CASES OF FRAUD[30]

Instructions have been issued by RBI for quickly informing the bank in incidents of frauds. For 0 liability of customer in card related frauds and financial frauds related to internet banking, if it has been informed to bank by the victim within 3 working days of information's receipt in the context of e-transaction from bank which was not permitted by him. On following this measure the Bank has to go for crediting that amount in the victim's account."

If 4 to 7 working days are taken by the consumers for informing the bank, the highest liability of consumer will not go beyond Rs 25,000 & it will be ranging between to Rs 5,000 to Rs 25,000. But if the report has been made after 7 working days, the liability of consumers will depend on the policy approved by the bank's board."

- **Within 90 days the complaints related to such frauds are asked to resolve**.

- Awareness is spread by banks and safety tips are calculated and help is taken from other social media handles also, like the account of social media.

- Awareness through e-baat programme (started by RBI) also makes people to understand the issues related to frauds and methods for its eradication.

- Annually the review of frauds will be done by banks, a note in this regard will be put by by banks before their directors.

[30] https://www.rbi.org.in/commonman/English/Scripts/PressReleases.aspx?Id=2441

- There will be shown the amount recovered also.

- Special Committee of the Board for monitoring and follow up of cases of frauds (SCBF) involving amounts of Rs 1 crore a and above, which, inter alia, monitors progress of CBI/Police investigation and recovery position in such fraud accounts.

4.6- FINANCIAL GAINS AS ONE OF THE MAIN REASONS FOR TARGETING E-BANKING-

The motives behind various reported cyber crime cases in 2020[31]-

Table 4.2

Motives for which cyber crimes were committed	No. of cybercrimes
Extortion	295
Financial gain/Greed	3855
Personal revenge/Settling scores	304
Motives of Blackmailing	293
Steal information for Espionage	22
For spreading piracy	185
For developing own business/interest	170
Sale purchase of illegal drugs/items	14
Disrupt public services	33
Inciting hate crimes against country	12
Inciting hate crimes against community	205
Political Motives	47
Sexual exploitation	588
Insult to modesty of a women	606
Fraud/illegal gain	1119
Prank/ Satisfaction of gaining control	214
Causing disrepute	387
Srxualpsuchiatric illness viz. perversion	12
Emotional motives like Anger, Revenge	223
Others	3008

[31] jetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005 ISSN: 2581-4621

Table 5.1 clearly shows that the cyber crimes in 2020 had a high number of cases of financial gains and greed which were total 3855 cases. The cases of fraud and illegal gains were also having the second highest number of cases related to cyber crimes in 2020 as Table 5.1 shows that there were 1119 such cases related to cyber crimes. It clearly shows that the cyber criminals want to target the money kept by people in banks and other places and when this money can be accessed through online mediums then it becomes very easy for cyber criminals to trace and steal it.

The cases explained in Table 5 1 explains a lot of key details related to prevention of cyber crimes. Now it has been clearly shown that banking fraud and financial gains are the prime reasons behind cyber crimes then the authorities must take actions against it.

4.6.1- PREVENTION OF CYBER CRIMES WILL PREVENT CRIMES RELATED TO I-BANKING ALSO

Digital medium & cyber world can not be limited to single boundaries, because it has connected the entire world together in such a way that we all have started perceiving ourselves as members of one nation. But it has caused some problems also which has been primarily witnessed as the increasing cases of cybercrimes and India is also not spared from this menace. In this way bad results are seen in the form of cyber crimes with constant growth in technology. Constantly new kinds of methods are being used by criminals for committing crimes and once the authorities prepare themselves for tackling those methods, the criminals move towards another new form of method, hence the tools and methods of cyber crimes are so dynamic which makes it quite hard to prevent. Hence cyber crime must be handled with serious concers as other traditional crimes are controlled likrrapes, murder, kidnapping, theft ets.

When a brutal crime happens, the authorities have many times banned the tool through which crimes were committed like

- banning the drugs which were consumed to victims for torturing or killing them,
- Banning dangerous weapons like country made guns, dangerous knives etc,
- Banning chemical substances which are so dangerous for use,

- Permanently banning many other tools and methods through which traditional crimes were committed,
- Banning the offender permanently from entering into society by giving him life imprisonment or giving the offender capital punishment for ending his life and removing him permanently from society which aslo sets an example for non commission of same kinds of crimes again by other people,
- Even in many areas alcohol is also banned because its consumption assist a lot in commission of various crimes, State of Bihar is a prime example of this,

But in cases of cybercrime suggestion are given like-

- Ban the internet permanently and it will stop the cases of cyber crimes permanently,
- Ban digital and online devices as well as ban computers, laptops, mobile phones and smartphones, -because if there is no mediums for cyber crimes then obviously cases will stop happening.

But, in a digital world and moving with plan of "digital India", the bans of electronic and digital mediums can not be approved anymore, if we have to live in a modern society then we have to support and go for maximum use of modern gadgets and technologies.

Hence prevention, propers surveillance, proper care and inquiry are better solutions than banning modern technologies.
Here, maximum use of technology for preventing cyber crimes by authorities, can also be a good measure.

Online studies for children are making it important to provide them with mobile phones, tablets, computers and many other kinds of digital gadgets. This transformation must happen with proper care and surveillance because these gadgets can be used for victimization of these kids.

New internet users are getting added everyday in India but if these users are unaware of the protective measures then they can also become victims of cybercrimes hence guidelines are issued by various authorities and service providers for due care, but these protective guidelines are so confusing and twisted which makes it normal to depend on non reliable sources. Hence the security measures must be delivered in simple languages as well as the technology must be upgraded in such a way that most of the security steps can be taken by device itself.

4.7- SOME DATA ALL OVER WORLD RELATED TO I-BANKING, MODERN BANKING AND CYBER CRIMES-

- **Some data related to USA[32]-**

  - People, who preferred online banking and did not like to physically visit banks, were nearabout 80%.

  - Nearabout 65% citizens of the USA were found to be using online banking in 2021.

  - On an average, every bank user in America had 5.3 bank accounts.

  - Among all respondents 76% of them admitted for using mobile banking app.(Forbes)

  - With each passing day cybercrime attacks are getting more frequent, dangerous and sophisticated. In 2016, the Federal Bureau of Investigation (FBI) - Internet Crime Complaint Center received 1,408,849 complaints and a reported loss of $4.63 billion. In 2016, the older folks (i.e. age group over 60 years old) suffer the most loss with 55,043 reported cases at a total loss of $339,474,918. The number one cybercrime attack in 2016 was business email compromise/email account compromise (BEC/EAC) with a total loss of $360,513,961. This was followed by identity theft, credit card fraud, phishing and hacking at $58,917,398, $48,187,993, $31,679,451 and $55,500 respectively.

- **Data related to UK[33]-**

[32] https://dataprot.net/statistics/mobile-banking-statistics/

the figures in the UK are as follows -

- Till January 2021, the popularity of bank accounts which are "digital only" has made 14 million Britishers to have it. And within 5 years it will be held by 23 million Brits.

- Online banking was used by 76% of the citizens of the UK in year 2020.
- Among all British adults, 50% of them were found to be using mobile banking in the year 2019.

- Mobile banking is used by 83% of businesses which are small & medium.
- Adoption rate as 71% was found in the UK for FinTechs.

- The strong reason for turning towards digital only banks by customers was "Convenience".

- But in 2020, banking fraud in online modes resulted in the loss of £159.7 million.

- **Some data and findings related various other countries[34]-**

    - Worldwide there are 73% people who use online banking for a minimum of 1 time in 1 month.

    - In India in FY21, the number of digital transactions were nearabout 40 billion which was calculated as Rupees 5,554 and in FY22 it was calculated as Rupees 7,422, which showed a highly +ve growth of 33%.

    - Payment devices which were wearable, had the $10.35 billion worldwide market size in 2020.

[33] https://dataprot.net/statistics/mobile-banking-statistics/
[34] https://dataprot.net/statistics/mobile-banking-statistics/

- Banking Trojans were used for attacking 625,364 PC users in 2020.

- Banks have confidence of people in protecting consumers' data, 95% people confirmed this.

- Among all people who are older than 54, only 12% were found to be using mobile payment services.

- Visiting banks became necessary for 56% of people who during online payments were redirected to physically visit banks.

- Active online users banking were found to be higher than 800 million in far east & China in the year 2020.

- Awareness of financial situations have increased for 62% consumers due to mobile banking.

- There have been many other digitalisation and online banking related findings

4.8- EFFORTS FOR SOLVING THE PROBLEM

In an effort to overcome cybercrime a multi-stakeholder approach is needed. This would involve governments, legal institutions, the private sector and other social organizations.

It is explained that an improved understanding of cybercrime would contribute to better measures and awareness in preventing and combating cybercrime. In an attempt to combat cybercrime, financial institutions utilize a wide variety of techniques.

Authentication can be classified into three categories:

- knowledge-based authentication, which speaks to information the consumer is expected to know such as password, personal details;

- token-based authentication, based on a physical token such as a credit or debit card or an actual security token and biometrics (fingerprints, retina scans or signatures) .

- Education can help victims to be aware of cybercrime like phishing.

It is said that the education is a very important factor in combating cybercrime and that persons need to be educated on how to prevent cybercrime, how cybercrime works and the harmful effects of cybercrime in the society.

The report also highlights that the private sector has outpaced the government in its recognition of the importance of cyber security.

Cybercrime has developed into an industry in which attackers are now operating internationally. This growth is due mainly to the fact that cyberattacks can be conducted with a high degree of anonymity. As a result, the likelihood of being able to identify the perpetrator is very low.

In addition, victims usually blame themselves for being attacked, only 3% don't think it will happen to them and 80% do not believe that these criminals will be brought to justice. These startling statistics result in a reluctance to adopt e-commerce in the banking sector. This reluctance can lead to missed opportunities in an Internet-connected world.

Furthermore, it was discovered that the more confident Internet users are, the less they perceived being attacked by cybercriminals, which by extension can increase the likelihood of adopting e-commerce.

Studies have discovered that banks engage in e-banking to keep abreast of technological development, lower transaction cost, achieve greater efficiency, enhance bank-customer relationship, improve customer satisfaction, and to gain competitive advantage.

Electronic banking has offered a useful and efficient way of remotely handling financial transactions and also that e-commerce has increased product availability while decreasing trading cost.

So non-adoption can have a negative impact on firm’s operations. In the midst of these potential benefits there remains the issue of security, fear and uncertainty by online consumers and ultimately business owners.

These issues can limit or retard the utilization of e-commerce services. Numerous instances of hacking and phishing attacks being taken place in India. These attacks (i.e. phishing and hacking) can deter a lot of consumers from employing the use of electronic mediums for carrying out their banking transactions.

Phishing is the act of sending fake messages to the victim, often in the disguise of bank notifications or emails promising monetary gains and romantic relationships, luring the victim into handing over sensitive information such as account number and password, or install malware on the victim’s system.

It is a type of spam that seeks to lure targeted victims to disclose certain information like usernames and passwords, which can then be used by the attacker to gain access to further banking information or can assist in stealing the victim’s identity.

Phishing activities are popular on websites in which individuals are required to enter their credit card information. Websites such as banking and pay online are prone to these activities. The attackers operate copies of genuine bank websites and encourage potential victims to log on to their bank accounts.

At this point sensitive information such as bank account numbers, passwords and the answers to security questions can be copied, saved and stored. Attackers typically perform these activities by sending emails under the disguise that these emails are coming from their authentic bank. Upon retrieval of such information, the attackers commit various cybercrimes.

Some major categories of phishing are clone and spear phishing. Spear phishing is a technique in which a specific victim is targeted. Basic information is known about the potential victim prior to the attack.

Potential victim could receive an email from a would-be friend, relative or financial institution which prompt the victim to provide certain confidential information or perform certain task.

In these instances, because the email is coming from a friend or relative, there is a high level of trust. As a result, the likelihood of success of these attacks is very high. On the other hand, clone phishing is a case where "a legitimate previously sent email containing an attachment or link has had its content and recipient address (es) taken and used to create a cloned email.

4.9- COMMENTS

This chapter found various points related to understanding and identifying the security issues when dealing with Internet banking services.

The criminals of this advanced age endeavor to commit these new crimes with the support of computers through Internet by abusing cyber space.

Cybercrime is becoming a greater threat as a result. Cybercrime comprises its own set of unique attractive features that have gradually started outweighing the traditional crimes.

The extent of anonymity, global victim reach and swift results are amongst the few that cybercriminals find most attractive. Unaware consumers are easily deceived due to lack of insight into the latest attack methodologies and identified preventive measures. Engagement of expert in cyber security professionals is a step further to develop quicker and better cybercrime investigation results.

As estimated by NASSCOM's Cyber security Task Force, India needs 1 million trained cyber security professionals by 2025.[35]

[35] https://www.dsci.in/content/cyber-security/cyber-security-task-force

CHAPTER 5

MISUSE OF PERSONAL DATA, CYBER CRIMES AND DECISIONS OF COURTS

- **SONY.SAMBANDH.COM CASE**

The punishment of the accused had resulted into the first case for punishment for cyber crime in India. This case shows that how personal and confidential data by accessing without permission the wrongdoers can misuse that data. Such access of data is done with the motive of committing various cyber crimes. Hence the Indian government, law enforcement authorities must become very serious to protect the right to privacy in the digital era. Access to digital and online data without permission must be stopped and wrongdoers must be severely punished.

Website www.sony.sambandh.com was a website of Sony India Ltd through which NRIs were sending various products to people living in India and this website was used for making payments as well. The "CBI vs Arif Azim"[36] case, was a case in which misuse of personal data had happened and the accused Arif Azim was punished who was an employee in a call centre and had collected data of users which they were using for payments. By accessing card details, Azim ordered some goods, this happened in May 2002. The owner of the card refused to pay when he came to know that a television set and headphone has been ordered which is to be delivered in Noida to Arif Azim. Sony registered this case with CBI and a report was lodged u/s 428, 429, 420 of the IPC. Arif Azim pleaded guilty, it was his first conviction, he was 24 years old so instead of giving any strict punishment the court released him on 1 year probation.

This case shows a lot of loopholes and shortcomings as well because punishment was given in this case in 2013 which was a case of 2002, also the court followed lenient approach in providing punishment which would have the repercussion of increasing the confidence of other cyber criminals.

- **BAN ON CHINESE APPS**

[36] CBI vs Arif Azim :(2008) 105 DRJ 721, (2008) 150 DLT 769

Most of the Chinese apps are known for maliciously collecting the data of users. Section 69A gives powers to the government to block the apps, websites etc on the basis of reasons mentioned in this section. For the sake of national interests, Chinese apps were banned in 2020 on 29th June(59 apps) and then on 24th November (43 aaps). TikTok was also banned through this step of the government. 54 apps were again banned on 14th February 2022. This section 69A has been constitutionally approved in the case of Shreya Singhal.[37]

- **VINOD KAUSHIK AND ANR vs MADHVIKA JOSHI AND ORS.**

In this case[38]: section 43 was violated by Madhvika Joshi but the court did not give punishment. The petitioners' emails were accessed by Nadvika Joshi which was a violation of Section 43 but no punishment was given by the court because the data was not misused and was collected for using them as evidence against petitioners in the case of 498A of IPC.

According to Delhi HC:
"In the present case, the petitioners evidently have not lead any evidence to show as to what damage they have suffered on account of the retrieval of their e-mails and chat sessions by respondent No. 1. These e-mails and chat sessions have been used by respondent No. 1 in her case lodged against the petitioners under Section 498A IPC. Admittedly, this information has not been made public by respondent No. 1 to malign the petitioners or to hurt their business or reputation. The information has been provided only to the police authorities or to the Court."[39]

"The petitioners cannot have any grievance because the respondent No.1 has lead in evidence of the materials collected by her in support of her case by breaching Section 43 of the I.T. Act."[40]

[37]Shreya Singhal vs Union of India AIR 2015 SC.1523.

[38] Vinod Kaushik and Anr vs Madhvika Joshi and Ors : WP(C) 160/2012

[39] http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=21184&yr=2012

[40] http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=21184&yr=2012

"The claim for compensation would not arise merely on account of the breach of Section 43. The claim would have to be established like in Civil Court, by making requisite averments with regard to the damage suffered, and thereafter by leading evidence in support thereof, to show that one or the other prohibited activities enumerated in Section 43 of the IT Act have resulted in the sufferance of damages by the person concerned."[41]

- **AVINASH BAJAJ vs STATE [NCT] OF DELHI:**

  "Avinash Bajaj vs State [NCT] of Delhi"[42] was a case related with section 67 of IT Act and section 292 of the IPC, in which the petitioner was not punished because he had not uploaded a pornographic video on an online sale platform (Bazee Company). Petitioner was the managing director of that company and because the platform was a third party platform and someone else uploaded that video for sale, hence he was released by the court. This website, on registration allowed goods and services to be sold and purchases and someone uploaded a pornographic video which got purchased by many consumers within 2-3 days and later it was removed by the company.

- **Shreya Singhal vs Union of India**

  In the case of Shreya Singhal,[43] section 79 which is related to exempting an intermediary, was read down by the SC, the same happened with rule 3(4) of intermediary guidelines. Order of the court or getting orders from government authority were declared the reasons for removing the contents by online intermediaries. Section 79 contains protections to make an intermediary not liable for 3rd party info., data etc which is either made available by Intermediary or intermediaries hosts that info. or data. Many occurrences have been witnessed when intermediaries had knowledge of their platform being used for malignant, immortal or unlawful activities, but they managed to protect themselves because of the exemption under sec. 79.

[41] Vinod Kaushik and Anr vs Madhvika Joshi and Ors : WP(C)160/2012 http://delhihighcourt.nic.in/dhcqrydisp_o.asp?pn=21184&yr=2012

[42] Avinash Bajaj vs State [NCT] of Delhi [(2008) 150 DLT 769]

[43] Shreya Singhal vs Union of India AIR 2015 SC.1523.

CHAPTER 6

CONCLUSION AND SUGGESTIONS

The lack of proper data protection law in India has been found as the biggest threat for the right to privacy in the digital era. Also the slow investigation by police in cyber crime cases and the issue of pending cyber crime case in judiciary are some of the most concerning issues. A strong data protection law must be quickly introduced and the police and judicial system must be reformed to quickly solve the cases of cyber crimes.

In Arif Azim cases[44] the court was not quite serious in proving big punishment for collecting the data of someone without his permission and the using that data for committing fraud. In Vinod Kaushik case[45] the court said misuse and harm is necessary to provide punishment and only collection of data without permission is not necessary for punishment. These approaches show that the judiciary has to rethink about its approach in dealing with cases of breach of privacy but first of all strict laws must be made for data protection.

Decentralisation of the data can be one of the best measures to prevent data leaks. Every individual and institution must be informed if anyone wants to get their data and without the permission of these individuals and institutions no one must be allowed to use that data.

A database which stores the data is not quite safe. An encrypted smart card can be the best medium which will be kept by a person and which can have capabilities of storing data.

Such technologies must be developed which can quickly send notifications to the person or institutions whose data is breached and or such technologies must be capable of quickly sending notifications if someone tries to breach the data or steal the data.

Tge existing technolgies fir sending notifivationsmusy mist be made more pipular so thatvoeopke can beconeawre if cyber security mechnisms.

Tge user also mist taje all cyber security measures and tgeu must not compromise tgeir privacy by ourchinf cheap devies or by viditingsusoicious pages, apos, websites.

[44] CBI vs Arif Azim :(2008) 105 DRJ 721, (2008) 150 DLT 769

[45] Vinod Kaushik and Anr vs Madhvika Joshi and Ors : WP(C) 160/2012

The law must be made to penalise the users as well who don't take proper cyber security measures. Such privision is quite important because initiatives against cyber crimes will work positively only when users also become aware of their duties for preventing cyber crimes.

The institutions providing online services, digital services must take the section 43A of the IT Act very serious and they musu quickly implement the cyber security measures and they must keep updating such measures.

- No separation was found between cyber crimes and online loss caused while using e-banking. Loss caused through e-banking has been found to have a big connection with cyber crimes.

1. Majority of the cybercrimes in i-banking sector have resulted out of hacking and identity theft.
2. Banks are being targeted over and over again because all the reserves in the form of cash are held with the banks.
3. The software can be used for detecting frauds in maximum cases is either outdated or very time consuming.
4. The number of cases resolved by the cyber cell has remained consistently low for the last four years, with only a 20 per cent success rate.

- Chapter 3 showed many cases in which i-banking was not used as a target but it was used as a supportive thing to conduct various crimes, especially cyber crimes. In various traditional and cyber crimes it was seen that criminals and wrong doers are not hesitating anymore to transact money through i-banking. The cyber criminals seem to have developed various measures through which they can use i-banking for various payments without being identified or without being traceable. This issue must be checked by authorities very seriously, if criminal are paying money to their partners through i-banking by using various technologies which make them untraceable then the challenge of preventing this kind of misuse arises very seriously and authorities must prevent the use of internet banking in cases where real identities and locations of users are not very clear.

- The i-banking frauds and use of i-banking by criminals and cyber criminals in quickly paying and receiving money by hiding their identities for various crimes proves a clear relationship between i-banking and cyber crimes.
- I-banking if not advanced with proper security measures then it will keep becoming a subject of continuous target through cyber crimes.

Information and communication Technology has become an integral part of our day to day life. With the cheap availability of broadband and smart phones, almost everyone has access to the cyber space, connecting virtually at millions of online users across the globe. Increasing use of cyber space has also made us vulnerable to cybercrime threats.

A minor laps/ negligence in managing our digital life can open doors for cybercrimes and hence can lead to financial loss. So, we must be vigilant and careful while connecting digitally to the outside world whether for financial transactions, social networking, playing games or searching things on the internet etc.

This research work provides an overview of cyber crimes in E- banking sector and general tips to prevent themselves from becoming a victim of cybercrime.

Banks in India have migrated to core banking platforms and have moved transactions to payment cards (debit and credit cards) and to electronic channels like ATMs, Internet Banking and Mobile Banking.

The banking industry has enjoyed the ride of emerging technology to undergo significant changes and has witnessed expansion of its services and strives to provide better customer facility through technology with the swift expansion of computer and internet technologies, on the other hand, there have been risks involved in it as well.

Technology risks not only have a direct impact on a bank as operational risks but can also exacerbate other risks like credit risks and market risks.

> Given the increasing reliance of customers on electronic delivery channels to conduct transactions, any security related issues have the potential to undermine public confidence in the use of e-banking channels and lead to reputation risks to the banks.

Electronic Banking or e-banking refers to a system where banking activities are carried out using informational and computer technology over human resource. In comparison to traditional banking services, in e-banking there is no physical interaction between the bank and the customers.

E-banking is the delivery of bank’s information and services by banks to customers via different delivery platforms that can be used with different terminal devices such as personal computer and a mobile phone with browser or desktop software, telephone or digital television.

In present scenario, Indian banking sector cannot avoid banking activities carried out through electronic medium but Cyber crime is more serious offence than the real life crimes, in order to overcome this problem the victims should report these cases to the nearest police station and cyber fraud council in banks.

In order to stop these issues, the legislature should keep a track on the working system of banks and law implementation should strict to monitor such wrongdoings and moreover banks should educate the customers regarding the awareness of cyber crimes often.

OTHER IMPORTANT SUGGESTIONS

1. Data protection law must be quickly introduced.
2. Police and judiciary must be reformed with the introduction of various cyber experts in police system and with a special court for solving cyber crimes only with judges experts in cyber field.
3. The first problem is that there is no specific law for internet-banking in India. It is always advised to visit IT Act, RBI's regulations, IPC and many other laws and legal instruments for tackling the cases of cyber crimes and for dealing with other issues related to i-banking. But now, with the growing dominance of i-banking there is an urgent need of passing a law from Parliament which must explain all the details related to i-banking. The new law must explain
    - all the requirements for accessing i-banking
    - it must mention all the security measures which can be very necessary for properly utilizing i-banking and for preventing the cases of frauds and misuse
    - The penalty provisions must be there to make the banks responsible if they take less proper measures for stopping the cases of misuse of i-banking
    - **Penalties for users:** the users of i-banking/banking consumers must also be penalised if they take very less protective measures as advised in this new law or as advised by the banks and government. This measure of penalty is very necessary because many people take very less protective measures and when they become victims of cyber crimes then they always blame banks, preventive authorities and government. The fear of penalty will make the users to take all protective measures regularly.
    - it must explain all the punitive measures in cases of misuse and cyber crimes.

4. The relation between cyber crimes and internet banking can not be ended at all but the cases of violations can be minimised, hence authorities must be always ready to take all those syrict steps for minimising the cases of violations.
5. The authorities and banks must take such measures through which no one must become able to hide their identities for sending and receiving money in i-banking and this phenomenon of hiding identities must be researched more properly to identify whether criminals are using it in a high number or not. If criminals are using such technologies which can make them receive or send money without being traced then it can result as a big threat for India. In that case, i-banking can be declared as an easy medium for supporting various crimes through which criminals can get their payments very easily. More research for this issue is required.
6. The technologies used in i-banking must be constantly upgraded, it must be always presumed that the cyber criminals must be using very high quality technologies than the technologies used by banks and preventive authorities. This presumption will always make the authorities to enhance the current technologies to tackle the issue of cyber crimes.
7. Gaining money through unauthorised online and digital mediums & processes have been found to be the prime reasons for targeting i-banking through cyber crimes, hence all such mediums which can give access for duping a person must be strengthened and they must be made full proof from any cyber attacks..
8. Internet banking users should use strong passwords and different user name combinations for different sites and accounts.
9. The law enforcement should be very rigid, and updated from time to time to keep a track of such crimes.
10. There should be fast track mobile courts to solve these cases, to meet the grievances and build confidence among the public.
11. The government should also keep a track on the operating network activities with the help of Big Data Banks.
12. Punishments and penalties must be exercised systematically in order to minimize the impact of these issues and penalize the attackers.
13. Awareness Programs should be initiated in order to inform the public about the ongoing scenario and upcoming threats.

14. The public must provide information about these cases to the Cyber Crime Branch in the matters related rather than just referring it to the banks, so as to ensure fast and strict actions.
15. In school curriculum the lesson for tackling cyber frauds, misuse of the internet and for dealing with various other types of cyber crimes must be added so that the children can tackle the situation related to these issues very well in future. Also the awareness provided like this will not make the students involved in any wrong practices related to cyber crimes.

BIBLIOGRAPHY

Bare Act

- Digital Personal Data Protection Bill, 2022
- Data Protection Bill
- Information technology Act, 2000,
- Information Technology (Intermediary guidelines and digital media ethics code)2021
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- Indian Telegraph (Amendment) Act, 2003
- Indian Penal Code,1860
- Copyright Act, 1957
- Patent Act, 1970

List of Reports

- NCRB Reports
- United Nation commission
- The Council of Europe Convention
- The European Commission
- Asian of South East Asian Nations
- Asia Pacific Economic Corporation

SECONDARY SOURCES:

Books:

- Andrew Grant-Adamson, Cyber Crime, Mason Crest Publishers, 2003

- ADB. (2011). Poverty in India. Retrieved 2019, from www.adb.org:https://www.adb.org/countries/india/poverty
- Assael, (1981). Consumer Behaviour and Marketing Action. 3rd Edition, PWSPublication Company, Boston.
- David Bowen, Viruses, Worms and Other Nastiness, Protecting yourself online; Department of Inter disciplinary Studies, 2003
- Davar, (1986). Law and Practice of Banking. Progressive Corporation Private Ltd,Bombay.
- Desai & Vasant, (1993). Principles of Bank Management. Himalaya Publication, Bombay.
- Desai & Vasant, (2005). Indian Financial System. Himalaya Publication, Bombay.
- Dudeja VD, Crimes in Cyberspace Scams and Frauds (Issues and Remedies) Commonwealth Publishers, New Delhi, 2003
- Eric S. Raymond: A brief History of Hackerdom (2000)
- Green & Salkind, (2002). Using SPSS for the Macintosh and Windows: Analyzing and Understanding Data. Prentice Hall Professional Technical Reference, New Jersey.
- John Townsend, Cyber Crime, Rain tree, 2004.
- Laura E. Quarantiello, Cyber Crime: How to protect yourself from Computer Criminals, Tiare publications, 1996.
- Kothari, (2004). Research methodology: methods and techniques. 2/E. New Age International Publishers, New Delhi.
- Machiraju, (2008). Modern Commercial Banking. New age International Publication, New Delhi.
- Muraleedhran, (2009). Modern Banking: Theory and Practice. PHI Learning Pvt Ltd, New Delhi.
- NageswararaoKaturi, (2007). Indian Commercial Banking: The New Dynamics. ICFAI University Press, Hydrabad.
- Somashekar, (2009). Banking. New age international Pvt Ltd, New Delhi.
- Santhanam, (1994). Banking Theory, Law & Practice. Margham Publication, Chennai.

- Smith RG, Grabosky PN and Urbas GF 2004, Cyber criminals on trial, Cambridge University Press.
- Stambaugh, Hetal, Electronic Crime needs assessment for state and local law enforcement, National Institute of Justice Report, Washington DC, US Department of Justice.
- Tan, Koon. Phishing and Spamming via IM Internet storm Centre. December 5th, 2006.
- Vladimir Golubev, International cooperation in fighting cybercrime; Computer Crime research Centre.
- Verma & Agarwal, (1987). Indian Financial System. Educational Publishers, New Delhi.
- Vikas Srivastave, (2011). Financing Infrastructure Projects by Indian Banks. National Institute of Bank Management, Pune.

Articles:

- Adam and McLaughlin, Charles. "Malware: What it is and How to prevent it" Ars Technical, 2004, http://all.net/CID/Attack/papers/Salami2html.
- Aderucci, Scott. Salami Fraud, www.all.net/CID/Attack/Papers/Salami.html.
- B.Michael Hale, Salami Attacks, http://all.net/CID/Attack/papers/Salami2.html.
- Buskin J, The Web Dirty Secret, Wall Street Journal, Available: Proquest: ABI/Inform Global, 2000
- Carter D L and A J Katz, "Computer Crime: An Emerging challenges for law enforcement", FBI Law rules bulletin http://www.fbi.gov/leb/dec961.txt
- Carter David L Computer Crime Categories, How Techno Criminals Operate, FBI Law Enforcement Bulletin, July, 1995
- Deepak Jandon, (2002). Performance variance and efficiency parameters of the Indian public sector banks. IJRCM, Vol: 1 (2), 29-41.

- Donald, (2012). The determinants of bank loan recovery rates. Journal of Banking and Finance, Vol: 36 (4), 87-96.
- Francisco Perez, (1998). Product mix of the Spanish banking firms do competition clubs exist. Working paper series documents de trabayoEc, 2,135-149.
- Ganesan, (2009). A secured hybrid architecture models for internet banking. Journal of Internet Banking and Commerce, Vol: 14 (1), 97-109.
- Gupta, (2008). Dynamics of productive efficiency of Indian banks. International Journal of Operation Research, Vol: 5 (2), 63-72.
- International Journal of Engineering Technology and Management Sciences, 2 Volume No.5 March – 2021
- Janatul& Lal, (2009). E-banking and customer satisfaction in Delhi – An Analysis. Journal of Management, Vol: 2 (1), 213-221.
- Jayaraman Munusamy, (2010). Service quality delivery and its impact on customer satisfaction in the banking sector in Malaysia. International Journal of Innovation Management and Technology, Vol: 1 (4), 41-50.
- Joshua, (2011). Usage patterns of electronic banking services by urban educated customers – glimpses from India. Journal of Internet Banking and Commerce, Vol: 16 (1), 67-78.

Electronic Sources:

Websites

- http://cybercrime.planetindia.net/worms.html
- http://etd.rau.ac.za/thesis/available/etd-05252005-120227/resticted/AppendixA.pdf
- http://webzone.k3.mah.se/k3jolo/HackerCultures/Origins.html
- http://www.asianlaws.org/Cyber-law/library/cc/what_cc.html
- http://www.cert.org/advisories/CA-1997-28.html
- http://www.cert.org/tech_tips/e-mail_bombing_spamming.html
- http://www.cyberpolicebangalore.nic.in/cybercrimes.html

- http://www.financialexpress.com/news/Cyber-crimes-cost-Indian-firms-Rs-58-lakh-in-2009/588864/
- http://www.lse.ac.uk/itservices/help/spamming&spoofing.html
- http://www.mailbroadcast.com/community/e-mail.broadcast.faq/46.e-mail.spoofing.html
- http://www.nrps.com/community/comprev.asp
- http://www.uncitral.org/english/texts/electom/
- http://www/fbi.gov/quickfacts.html
- http://www/trai.gov.in
- http://cybercrime.planetindia.net/cybercrime_cell.html
- Kabay, ME Salami Fraud, www.nwfusion.com/newsletters/sec/2002/01467137.html
- Love, David, Cyber Terrorism: Is it a Serious Threat to Commercial Organization? www.crime-research.org/news/2003/04/Mess0204.html
- ME Kabay, Logic bombs, Part 1, Network World Security Newsletter.
- Meaning of logic bomb, http://en.wikipedia.orf/wiki/logic_bomb
- Ollmann, Gunter, The Phishing Guide: Understanding And Preventing Phishing Attacks: Technical Info, 2006
- Rohas Nagpal, Asian School of Cyber Law http://www.asianlaws.org/longpress/esecurity.html
- Samuel Jay Keyser, "Where the Sun shines, there Hack they" http://www.hacks.mit.edu/Hacks/books/articles/where_the_sun_shines.html
- The Computer Ethics Institute, a leader in the field, has compromised a guideline to help computer users in their ethical decisions. They have called this guideline "The Ten Commandments" http://www.computerethicsinstitute.org/images/TheTenCommandmentsofCompu terethics.pdf
- http://www.rbi.org.in
- http://www.iba.org.in
- http://www.banknetindia.com
- http://www.iamai,in

- http://www.ideasrepec.co
- http://www.arraydev.com
- http://www.directessays.com
- http://www.idrbt.ac.in
- http://eprocure.gov.in/cppp/sites/default/files/eproc/itact2000.pdf
- http://en.wikipedia.org/wiki/Banking_in_India#History
- http://en.wikipedia.org/wiki/IDBI_Bank
- http://www.mbaknol.com/business-finance/tandon-committee-report-on-working-capital-norms and-recommendations/
- http://www.articlesbase.com/customer-service-articles/bank-computerisation-in-indian-banks-5346071.html
- http://en.wikipedia.org/wiki/Regional_Rural_Bank
- http://articles.timesofindia.indiatimes.com/2006-08-12/open-space/27790559_1_atm-india-credit
- http://wiki.answers.com/Q/Which_was_the_first_Indian_Bank_to_introduce_credit_card
- http://wiki.answers.com/Q/When_first_ATM_launched_in_india_and_by_which_b ank
- http://en.wikipedia.org/wiki/Kisan_Credit_Card
- http://www.dnb.co.in/bfsisectorinindia/BankC6.asp
- http://law.indiainfo.com/cyber law/ecommerce-act.html#1
- http://www.reliancecommodities.co.in/Details-Anti-Money-Laundering-Process/objectives
- http://rbidocs.rbi.org.in/rdocs/RTGS/PDFs/RTGSF082013.pdf
- http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
- http://www.us-cert.gov/ncas/tips/ST04-015
- http://www.pcmag.com/encyclopedia/term/57067/vishing
- http://www.nigerianspam.com/Phishing-Types.html
- http://www.infoworld.com/t/malware/cisco-linkedin-users-hammere-malicious-malware-883
- http://searchmidmarketsecurity.techtarget.com/definition/network-scanning
- http://en.wikipedia.org/wiki/Money_laundering

- http://watchdogs.gamepedia.com/ATM_HackingChrome-
- extension://efaidnbmnnnibpcajpcglclefindmkaj/viewer.html?pdfurl=ttps%3A%2F%2Fepisteme.net.in%2Fcontent%2F73%2F3820%2Fattachments%2F6-UPI.pdf&clen=327360&chunk=true
- https://www.npci.org.in/what-we-do/upi/product-overview
- https://en.wikipedia.org/wiki/Unified_Payments_Interface#:~:text=s%20of%20July%202021%2C%20UPI,all%20retail%20payment%20in%20India.
- jetms.in Issue: 2 Volume No.5 March – 2021 DOI: 10.46647/ijetms.2021.v05i02.005 ISSN: 2581-4621

NEWSPAPERS:

Following national and local dailies were reads for the news related cyber crimes and cyber laws as well as the development in the banking industry.

- I) The Hindu,
- II) The Times of India,
- III) The Indian Express,
- IV) The Tribune,
- V) The Hindustan Times
- VI) Economic times
- VII) Nav Bharat
- VIII) Dainik Bhaskar
- IX) Chronicle
- E) MAGZINES
- I) Lawyer’s Update,
- II) Practical Lawyer,
- III) Lawyer’s Collective,
- IV) RBI Bulletin (Monthly)
- V) RBI Legal News and views(Quarterly)
- VI) IBA Bulletin
- VII) Bank Quest (IBA Quarterly)
- VIII) e-track (PNB house magazine)

- IX) MahabankMonthly(Bank of Maharashtra Monthly)
- X) Mahabank Pragati (Bank of Maharashtra Quarterly)
- XI) Banking Chintan Anuchintan(RBI Hindi)