

CYBER CRIME IN INDIA : “A CRITICAL STUDY WITH SPECIAL REFERENCE TO BUNDELKHAND REGION IN UTTAR PRADESH”

A Thesis

**Submitted towards the Requirement for the Award of Degree of
DOCTOR OF PHILOSOPHY
IN**

LAW

(Under the Faculty of Law)

Researcher

Ms. Shefali Bajpai

Enrollment No.:161522016283

Under the Supervision of

Dr. Harday Veer

Faculty of Law



2026

**FACULTY OF LAW,
P. K. UNIVERSITY, SHIVPURI (M.P.)**

VILLAGE - THANRA, POST - DINARA, NH-27, SHIVPURI (M.P.) PIN- 473665

Website: www.pkuniversity.edu.in



P.K.UNIVERSITY
SHIVPURI (M.P.)

(University established under section 2f of UGC act 1956 vide mp government act no 17 of 2015)

DECLARATION BY THE CANDIDATE

I declare that the thesis entitled “**Cyber Crime in India : A Critical Study With Special Reference to Bundelkhand Region in Uttar Pradesh**” is my own work conducted under the supervision of **Dr. Harday Veer** (Supervisor) at P.K. University, Shivpuri (M.P.).

Approved by Research Degree Committee. I have put more than 240 days of attendance with Supervisor at the center.

I further declare that to the best of my knowledge the thesis does not contain any part of any work which has been submitted for the award of any degree either in this University or in any other University.

Without proper citation.

Date :

Place :

Shefali Bajpai
Ph.D. in Law
Enrollment No. 161522016283



P.K.UNIVERSITY
SHIVPURI (M.P.)

(University established under section 2f of UGC act 1956 vide mp government act no 17 of 2015)

CERTIFICATE OF THE SUPERVISOR

This is to certify that the work entitled “**Cyber Crime in India : A Critical Study With Special Reference to Bundelkhand Region in Uttar Pradesh**” is a piece of research work done by **Shefali Bajpai** under my Guidance and Supervision for the degree of Doctor of Philosophy in Law, P.K University (M.P) India.

I certify that the candidate has put an attendance of more than 240day with me. To the best of my knowledge and belief the thesis:-

I – Embodies the work of the candidate herself/

II – Has duly been completed.

III – Fulfill the requirement of the ordinance relating to the Ph.D. degree of the University.

Signature of the Supervisor

Dr. Harday Veer

Associate Professor

Faculty of Law

P.K. University



P.K.UNIVERSITY
SHIVPURI (M.P.)

(University established under section 2f of UGC act 1956 vide mp government act no 17 of 2015)

FORWARDING LETTER OF HEAD OF INSTITUTION

The Ph.D. thesis entitled **“Cyber Crime in India : A Critical Study
With Special Reference to Bundelkhand Region in Uttar Pradesh”**
Submitted by **Shefali Bajpai**, is forwarded to the P.K. University in six copies.
The candidate has paid the necessary fees and there are no dues outstanding
against her.

Name

Seal

Date:

Place: P.K. University, Shivpuri (M.P.)

(Signature of Head of Institution Where the
Candidate was registered for Ph.D degree)

Signature of the Supervisor

Date

Place: P.K. University, Shivpuri (M.P.)



P.K.UNIVERSITY
SHIVPURI (M.P.)

(University established under section 2f of UGC act 1956 vide mp government act no 17 of 2015)

COPYRIGHT TRANSFER CERTIFICATE

Title of the Thesis: **“Cyber Crime in India : A Critical Study With Special Reference to Bundelkhand Region in Uttar Pradesh”**

Candidate's Name: ***Shefali Bajpai***

COPYRIGHT TRANSFER

The undersigned hereby assigns to the P.K. University, Shivpuri all copyrights that exist in and for the above thesis submitted for the award of the Ph.D. degree.

Date:

Shefali Bajpai
Ph.D. in Law
Enrollment No. 161522016283

Note: However, the author may reproduce/publish or authorize others to reproduce, material extracted verbatim from the thesis or derivative of the thesis for authors personal use provided that the source and the University copyright notice are indic.

ACKNOWLEDGEMENT

This Ph.D. journey has been a profound and transformative experience filled with intellectual challenges, moments of doubt, growth, and, ultimately, accomplishment.

The completion of this thesis would not have been possible without the support, guidance, and encouragement of many individuals, each of whom played an important role in shaping this journey. With heartfelt gratitude, I wish to express my sincere thanks to all who have contributed to my academic and personal development during these formative years.

First for most I would like to thank almighty god for perseverance, courage and strength bestowed on me to undertake this project.

Furthermore, I extend my sincere thanks to the **Shri Jagdeesh Prasad Sharma, Hon'ble Chancellor**, P.K. University, Shivpuri (M.P.) for providing me necessary infrastructure and facilities that were essential during my research work.

My profound sense of gratitude, faith, and awe also to **Prof. (Dr.) Yogesh Chandra Dubey, Hon'ble Vice Chancellor**, P.K. University, Shivpuri, (M.P.), **Professor (Dr.) Mukesh Chansoria, Hon'ble Pro VC**, P.K. University, Shivpuri, (M.P.) for his generous and valuable support throughout my research work.

I take this pleasant opportunity to express my deep sense of gratitude and reverence to his holiness **Dr. Jitendra Kumar Mishra**, Director (Admin), P.K. University, Shivpuri (M.P.) **Prof. (Dr.) Jitendra Kumar Malik**, Registrar, P.K. University, Shivpuri (M.P.) for his constant encouragement and providing me with the required facilities that enabled me to complete my research work.

For most, I extend my deepest appreciation to my esteemed Supervisor, **Dr. Harday Veer**, (HOD), **Dr. Digvijay Singh**, (Principal), **Dr. Rohitas Meena** (Associate Professor), **Mr. Gauri Dutt Tiwari**, (Assistant Professor), **Miss Rani Prajapati**, (Assistant Professor), **Miss Erum Naiyar**, (Assistant Professor), **Miss Dimple Vayash** (Assistant Professor) Faculty of Law, P.K. University, Shivpuri (M.P.), without whom this work would not have come to fruition. His wisdom, patience, and insight have guided me from the very beginning of my research work. Your unwavering support, constructive criticism, and encouragement have been instrumental in shaping not only this research work but also my academic identity.

I would like to extend my gratitude and deep appreciation to respected **Prof. (Dr.) Ashish Vishwakarma**, Dean Research & I/c Ph.D cell, P.K. University, Shivpuri (M.P.). "I also extend my deepest appreciation and thanks for his valuable support and encouragement throughout my research work.

I express my gratitude and thanks to **Dr. Aiman Fatima**, Dean Academics, P.K University, Shivpuri (M.P.).

I also extend my deepest appreciation and thanks to all, Faculty members of law, P.K University, Shivpuri (M.P.) for his valuable support and encouragement throughout my research work.

To the members of my Research Advisory Committee, and Research Cell, thank you for your valuable inputs at various stages of the project. Your questions, suggestions, and recommendations helped in my work.

I also express my gratitude to **Miss. Nisha Yadav**, Librarian, P.K University, Shivpuri (M.P.) along with **Mr. Anand Kumar**, Assistant Librarian, and **Mr. Ashish Gupta** supporting staff of Research cell and other staff of P.K University.

I am also thankful to **Mr. Alok Kahre**, and **Mr. Purushottam** J.T. Cell of P.K University, Shivpuri (M.P.). I would also like to acknowledge external examiners whose detailed review and constructive criticism during the final stage of this journey helped me view my work from a fresh perspective and improve its scholarly merit.

I am profoundly grateful to P.K University, Shivpuri, (M.P.) and the Faculty of Law for providing an intellectually stimulating environment and the resources needed to pursue my research.

I am profoundly grateful to my mother **Mrs. Meena Bajpai** and my father **Mr. Shanti Sawroop Bajpai**, my son **Harsh** for their unwavering support, love, and encouragement during this challenging yet fulfilling journey. Their belief in me has been my greatest strength. My thanks and best wishes go to my friends for their inspiration.

I wish to acknowledge and extend my special thanks to all who have helped me immensely in writing my thesis and have provided continuous moral support.

At last, I thank all those who, some or other way, helped in my research work but somehow missed a mention.

Date:

Place: P.K. University

(Shefali Bajpai)

Enrollment Number- 161522016283



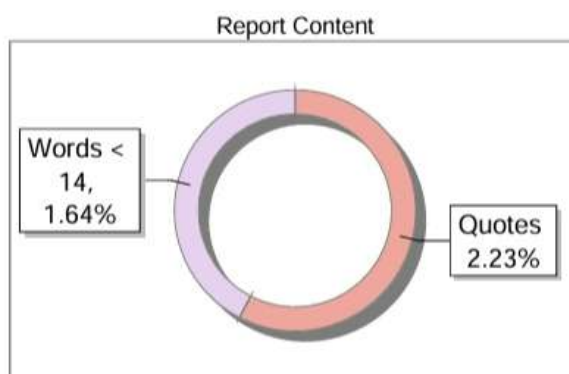
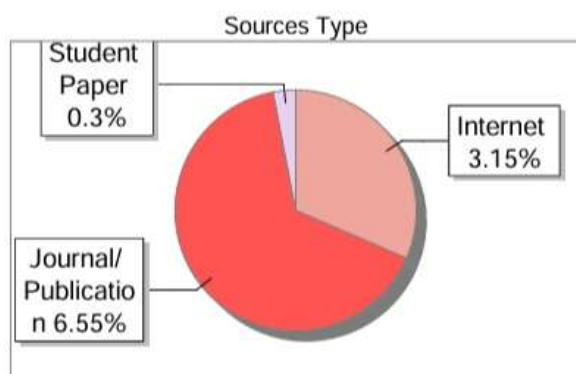
The Report is Generated by DrillBit Plagiarism Detection Software

Submission Information

Author Name	Shefali Bajpai
Title	CYBER CRIME IN INDIA : "A CRITICAL STUDYWITH SPECIAL REFERENCE TO BUNDELKHAND REGION IN UTTAR PRADESH"
Paper/Submission ID	5181356
Submitted by	library.pku@gmail.com
Submission Date	2026-01-24 12:16:55
Total Pages, Total Words	191, 49496
Document type	Thesis Chapter

Result Information

Similarity **10 %**



Exclude Information

Quotes	Not Excluded
References/Bibliography	Not Excluded
Source: Excluded < 14 Words	Not Excluded
Excluded Source	3 %
Excluded Phrases	Not Excluded

Database Selection

Language	English
Student Papers	Yes
Journals & publishers	Yes
Internet or Web	Yes
Institution Repository	Yes

A Unique QR Code use to View/Download/Share Pdf File





P.K.UNIVERSITY
SHIVPURI (M.P.)

University Established Under
section 2F of UGC ACT 1956 Vide MP Government Act No 17 of 2015

CENTRAL LIBRARY

Ref. No. PKU/C.LIB /2026/PLAG. CERT./244

Date: 03.02.2026

CERTIFICATE OF PLAGIARISM REPORT

1. Name of the Research Scholar : Shefali Bajpai
2. Course of Study : Doctor of Philosophy (Ph.D.)
3. Title of the Thesis : Cyber Crime in India: "A Critical Study with Special Reference to Bundelkhand Region in Uttar Pradesh"
4. Name of the Supervisor : Dr. Harday Veer
5. Department : Law
6. Subject : Law
7. Acceptable Maximum Limit : 10% (As per UGC Norms)
8. Percentage of Similarity of Contents Identified : 10%
9. Software Used : Drillbit
10. Date of Verification : 24.01.2026


(Librarian, Central Library)
P.K. University, Shivpuri (M.P.)
P.K. University
Shivpuri (M.P.)

ADD: VIL: THANRA, TEHSIL: KARERA, NH-27, DIST: SHIVPURI (M.P.) -473665
MOB: 7241115902, Email: library.pku@gmail.com

ABSTRACT

The rapid advancement of information and communication technology and the expansion of the digital ecosystem have transformed cyber crime into a complex, multidimensional, and transnational phenomenon. In a developing country like India, where digital inclusion is increasingly promoted as a catalyst for economic growth and governance reform, cyber crime has emerged as a significant challenge to legal frameworks, administrative mechanisms, and social structures. The widespread use of the internet, smart phones, digital payment systems, e-governance platforms, and social media has enhanced efficiency and accessibility, but it has simultaneously escalated vulnerabilities to cyber offences such as online financial fraud, identity theft, phishing, data breaches, cyber harassment, and misuse of digital platforms. This study undertakes a critical examination of cyber crime in India, with special reference to the Bundelkhand region of Uttar Pradesh, a socio-economically backward and digitally transitioning area.

The research is premised on the understanding that cyber crime is not merely a technological issue but is deeply embedded in broader socio-economic, educational, and institutional contexts. Bundelkhand, historically characterized by poverty, low literacy levels, unemployment, and inadequate infrastructure, has increasingly become susceptible to cyber crime due to the rapid penetration of smartphones and digital financial services without a commensurate rise in cyber awareness and security preparedness. The study observes a growing incidence of cyber offences in the region, particularly online banking frauds, digital payment scams, fraudulent calls, and social media-related crimes. It also highlights the pervasive problem of underreporting of cyber crime in rural and semi-urban areas, which obscures the actual magnitude of the problem and weakens effective policy responses.

This study critically evaluates the existing legal and regulatory framework governing cyber crime in India, with particular emphasis on the Information Technology Act, 2000 and its subsequent amendments. It examines the adequacy of these laws in addressing emerging forms of cyber crime and assesses their implementation at the regional level. The research further analyzes the role and capacity of law enforcement agencies, cyber crime cells, and judicial institutions in the Bundelkhand region, identifying key challenges such as limited technical expertise, inadequate infrastructure, lack of specialized training, procedural delays, and weak coordination between enforcement agencies.

The methodology adopted in this study is primarily doctrinal, analytical, and descriptive in nature. It relies on secondary sources including National Crime Records Bureau (NCRB) data, government reports, judicial pronouncements, academic literature, and policy documents. Where relevant, regional statistics and illustrative case studies from Bundelkhand have been incorporated to provide empirical support to the analysis.

The study concludes that addressing cyber crime in India requires more than legislative intervention alone. There is an urgent need for region-specific, multi-layered strategies that emphasize digital literacy, public awareness, institutional capacity building, and effective enforcement mechanisms. Special focus on underdeveloped regions such as Bundelkhand is essential to ensure inclusive cyber security, strengthen access to justice, and bridge the gap between cyber law in theory and its practical implementation. The findings of this research aim to contribute meaningfully to academic discourse and policy formulation on cyber crime control in India.

CONTENTS

CHAPTER– I **01-15**

INTRODUCTION

1.1	AN OVERVIEW	01-03
1.2	OBJECTIVE OF THE RESEARCH	03-04
1.3	NEED OF RESEARCH & STUDY	04
1.4	SCOPE THE RESEARCH	04-05
1.5	RESEARCH MYTHOLOGY	05
1.6	SIGNIFICANCE OF THE STUDY	06
1.7	HYPOTHESIS	07
1.8	RESEARCH DESING AND METHODOLOGY	07-08
1.9	REVIEW OF LITERATURE	08-15

CHAPTER–II **16-50**

CONCEPTUAL ANALYSIS OF CYBER CRIME ON SELECTIVE AREA

2.1	CYBER CRIME	16-30
2.2	CAUSES OF CYBER-CRIME	30-37
2.3	HOW TOERADICATE CYBER-CRIME	37-38
2.4	WHO ARE INVOLVED	38-39
2.5	CYBER CRIME	39-41
2.6	DEMAND OF CYBER LAW	41-43
2.7	CYBER CRIMINAL	43-45
2.8	STAGES OF CYBER CRIME	45-46
2.9	CYBER & E-COMMERCE	46
2.10	CONCEPTUAL ANALYSIS OF CYBER CRIME	47-49
2.11	CYBER SPACE AND CYBER WORLD	49-50

CHAPTER–III **51-68**

CYBER LAWS IN INDIANS CENARIO

3.1	COMPUTER AND INTERNET	51-63
3.2	CYBER CRIME IN INDIAN SCENARIO	63-68

CHAPTER – IV **69-116**

CYBER CRIME COMPARATIVE STUDIES IN OTHER COUNTRIES

4.1	INTRODUCTION	69-70
4.2	COMPARATIVE ANALYSIS OF CYBER LAWS	70-73
4.3	CYBER LAWS IN CHINA	73-79
4.4	CYBER LAWS IN PAKISTAN	79-92
4.5	CYBER LAWS IN JAPAN	92-104
4.6	CYBER LAWS IN BANGLADESH	104-107
4.7	CYBER CRIME LAWS IN NEPAL	107-111
4.8	CYBER CRIME LAWS IN VIETNAM	111-116

CHAPTER– V **117-144**

JUDICIAL INTERPRETATION IN CYBER CRIME

5.1	JUDGMENT IN BRIEF	118-144
-----	-------------------	---------

CHAPTER–VI **145-193**

ACRITICAL EVALUATION OF CYBER LAWS IN BUNDELKHAND REGION OF UTTAR PRADESH

6.1	INTRODUCTION	145-146
6.2	ACRITICAL EVALUATION OF CYBER LAWS	146
6.3	A ANALITICAL STUDY IN BUNDELKHAND REGION OF UTTAR PRADESH	146-178
6.4	CYBER CRIME–AN EMPIRICAL STUDY	179-193

CHAPTER–VII **194-198**

CONCLUSION AND SUGGESTION

7.1	CONCLUSION	194-195
-----	------------	---------

List of Tables & Graphs

Table & Graphs No.	Description	Page No.
1.	Types of cyber crime in Jhansi district	148
2.	Types of Cyber Crime in Lalitpur District	156
3.	Types of Cyber Crime in Jalaun District	159-160
4.	Types of Cyber Crime in Banda District	164-165
5.	Types of Cyber Crime in Mahoba District	170
6.	Types of Cyber Crime in Hamirpur District	174
7.	Types of Cyber Crime in Chitrakoot District	177
8.	Cyber crime update of recants years at that region of Bundelkhand of U.P.	182
9.	Age Distribution of arrested suspects in Cyber Crime.	183
10.	Victim of Cyber crime per Education level.	184
11.	(A) The most prevalent forms of Cyber crimes in the region of Bundelkhand (U.P.)	185
12.	(B) The most prevalent forms of Cyber crimes in the region of Bundelkhand (U.P.)	186
13.	Demonstrate the awareness about cyber crime by the respondents.	188
14.	Demonstrate any of the below mentioned situation experienced by the respondents.	189

15.	Mention how many time respondents have been a victim of cyber crime.	190
16.	Demonstrate that the respondents thinks that the laws in effect are able to control cyber criminals.	191

ABBREVIATION

AD	Advertisement
AI	Artificial Intelligence
AIR	All India Reporter
APR	Appeal
APP	Assistant Public Prosecutor
ATM	Automated Teller Machine
BomCR	Bombay Cases Reporter
BSNL	Bharat Sanchar Nigam Limited
C. No.	Case Number
CBI	Central Bureau of Investigation
CCTV	Closed Circuit Television
CDR	Call Detail Record
CD	Compact Disc
CDMA	Code Division Multiple Access
CERT-IN	Indian Computer Emergency Response Team
Co.	Company
COB	Central Oversight Body
CPC	Code of Civil Procedure
CJI	Chief Justice of India
Cri LJ	Criminal Law Journal

Crl. App.	Criminal Appeal
CR. C.	Criminal Case
Crl. Rev.	Criminal Revision
Cr PC	Criminal Procedure Code
CS (COMM)	Civil Suir (Commercial)
CVV	Card Verification Value
DCL	Digital Command Language
DLT	Delhi Law Times
DRJ	Delhi Reported Journal
DVD	Digital Versatile Disc or Digital Video Disc.
E-Commerce	Electronic Commerce
E-Mail	Electronic Mail
FIR	First Information Report
FTP	File Transfer Protocol
HD	Hard Disc
HON'BLE	Honourable
IB	Intelligence Bureau
ICANN	Internet Corporation for Assigned Names & Number
IEA	Indian Evidence Act
IT	Information Technology
IP Address	Internet Protocol Address
IP Rights	Intellectual Property Right
IPC	Indian Penal Code
KLT	Kerala Law Times
LAN	Local Area Network
Ltd.	Limited
MA	Miscellaneous Application
MLA	Member of Legislative Assembly
MMS	Multimedia Message Service

MP	Member of Parliament
MS-Word	Microsoft Word
MTNL	Mahanagar Telephone Nigam Limited
NCT	National Capital Territory
NEFT	National Electronic Funds Transfer
No.	Number
Ors.	Others
OTP	One Time Password
OTT	Over The Top
PC	Personal Computer
PIL	Public Interest Litigation
POSCO	Protection of Children from Sexual Offences Act
POTA	Prevention of Terrorism Act
Re.	Reply
Retd.	Retired
R.I.	Rigorous Imprisonment
RTGS	Real Time Gross Settlement
SC	Supreme Court
SCC	Supreme Court Cases
SCR	Supreme Court Reporter
SEC	Section
SI	Simple Imprisonment
SIM	Subscriber Identity Module
SLP	Special Leave Petition
SMS	Short Message Service
SCC	Supreme Court Cases
UDRP	Uniform Dispute Resolution Process
UK	United Kingdom
UOI	Union of India

UIDAI	Unique Identification Authority of India
USA	United States of America
USB	Universal Serial Bus
USD	United States Dollar
V	Versus
VHS	Video Home System
VPN	Virtual Private Network
WAN	Wide Area Network
WIPO	World Intellectual Property Organization
WLL	Wireless Local Loop
WP	Writ Petition
WWW	World Wide Web

LIST OF CASES

S.No.	Case Name	Pg. No.
1.	United States v. Neal Scott Kramer 701F, 2d 1340, 1983 USAPP. LEXIS 9138, 12Fed.R.	64
2.	R.M. Malkani v. State of Maharastra AIR 1973 SC 157 Cri LJ 228	118
3.	R v. Lothan (2001)EWCA Crim 2264	120
4.	Ziyauddin Burbanuddin Bukbari v. Brij Moban Ramdas Mehra & Ors. AIR 1975 SC 1778: (1976) 2 SCC 17: SCR 453	120
5.	State of Maharashtra v. Dr. Praful B. Desai AIR 2003 SC 2053: (2003) 8 SCC 180: 2003 Cri LJ 2033	121

6.	State of Tamil Nadu v. Subas Katti CC No. 4680 of 204	122
7.	State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru (2005) 11 SCC 600: AIR 2005 SC 3820: (6) Scale 177: 2005 Cri LJ 3950	122
8.	P.R. Transport Agency v. Union of India AIR 2006 All 23: (1) AWC 504	123
9.	K.K. Velusamy v. N. Pulanisamy (2011) 11 SCC 275	125
10.	A.R. Priyasamy v. C. Kanakayath AIR 1973 SCC (cri) 399	125
11.	SMC Pneumatics (India) Pvt. Ltd. v. Shri Jogesh Kwatra Original Suit No. 1279 of 2001 Dist. Court (Del)	126
12.	Rajesh Hariprasad Tripathi v. State of Gujarat Crl. Misc., No. 10858 of 2014 (Guj HC)	126
13.	Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke (2015) 3 SCC 123: 2 SCC (Cri) 19	126
14.	Tomaso Bruno and anr. V. State of Uttar Pradesh (2015) 7 SCC 178: 3 SCC (Cri) 54	127
15.	Shajeeb Khan v. State of Kerala B.A. 8074 of 2015 HC	128
16.	Kalandi Charan Lenke v. State of Odisha 2017 (I) OLR 543	128
17.	Shanat Babu Digwmani v. Govt. of NCT Delhi case, AIR 2015 11 SC (573)	128
18.	Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1	129
19.	Anwar v. Basheer AIR 2014)10 SCC 473	131
20.	AZZ Infraservice Ltd v. Quippo Infrastructure Ltd. SLP(C) No. 8636 of 2021	131
21.	Sattai Durai Murgan v. The Inspector of Police Crl OP (MD) No. 9381 of 2021	132

22.	M/s DRS Logistic Ltd. & Another v. Google India Private Limited & Anr. CS (Comm.) 1 of 2017 & Las. 21153	133
23.	Amway India Enterprise Pvt. Ltd. and Anr. v. M/s. LMT Technologies Pvt. Ltd. and Anr. 206 (2019) DLT 680 CS(OS) 410/2013	133
24.	Harsh Kadam @ Hitendra Kumar v. State of U.P. Case under Section 482/378/407, No. 5244 of 2021 (All HC)	134
25.	Shreya Singhal vs. Union of India (AIR 2015 SC 1523)	135
26.	State v. Salman Ansari Cyber Case No. 21 of 2021, Jamtara Dist. Court	135
27.	Payel Bishwas v. Commissioner of Police WP (MD) No. 22667 of 2021 (Mad HC)	137
28.	Ashlesh Biradar v. State of West Bengal WPA (P) 104 of 2022 (Cal HC)	138
29.	Anuradha Bhasin v. union of India AIR 2020 SC1308	138
30.	Shiv Kumar v. State of Bihar Criminal Misc. No. 3807 of 2020 (Pat HC)	138
31.	Lalita Kumari vs State of U.P. AIR 2014, SC 187	139
32.	Justice K.S. Puttasamy (Retd.) v. Union of India – AIR 2017 SC 4161: (2017) 10 Scale 1: (2017) 10 SCC 1	139
33.	Nishant Ray vs. State of U.P. AIR 2024 ALJ472	141
34.	Devashish rai vs. state of U.P. AIR 2025 LHC (Crino 3/2025)	142
35.	Deepak Singh v. State Of U.P. And 3 Others AIR 2025 HC	142
36.	Anoop Uttam v. State Of Up And 3 Others AIR 2024 HC	142
37.	Shivam Gupta @ Krishna v. State of U.P. AIR 2024 HC	143
38.	Jai Maa Aadi Shakti v. Union Of India And 3 Others AIR	143

	2025 HC	
39.	Imran Khan v. State of U.P. and Another AIR 2025 Dist. Court	143
40.	Tarun Kayal v. State Of U.P. And 3 Others AIR 2025 Dist. Court	143
41.	Ashok Kumar Srivastava v. State of U.P. And 3 Others AIR 2022 Dist. Court	143
42.	Akash Verma v. State of U.P. AIR 2025 Dist. Court	144
43.	Sujit Kumar v. State of U.P. and Another AIR 2025 Dist. Court	144

CHAPTER-I

INTRODUCTION

1.1 AN OVERVIEW

The fact that dishonest people have persisted in committing crimes via the use of computers over the past 20 years has captivated and horrified people alike. There has to be swift action in passing legislation to safeguard cyber space and its users because this phenomena has recently grown more complex and unprecedented. The system has become so advanced that it can be used to perpetrate murder and other forms of mayhem. An article from January 2002 in the Indian Express states that the first cyber murder in the US occurred seven years ago, when an underworld don was admitted to the hospital for a routine operation. A computer expert that his rival goon hired hacked into the hospital's system and changed his prescriptions. An innocent nurse gave him the doctor's fake prescription, and the patient died.¹

An evil known as cyber crime has its roots in our ever reliant reliance on computers in today's society. Cyber crime has taken on more ominous overtones in this day and age when computers power everything from home appliances to nuclear power stations. One of the most recent high-profile cyber crimes involved the theft of \$10 million from Citibank and its subsequent transfer to an account in Switzerland. The assault was carried out by a group of Russian hackers headed by the famous hacker Vladimir Kevin. The security systems of the bank were breached by the group. The accusation is that Vladimir broke into Citibank systems while he was at work at the Russian computer firm AO Saturn in St. Petersburg. While en route to Switzerland, he was apprehended at Heathrow Airport.²

Cyber crime is the subject of this study, which aims to define the term, investigate its causes, propose solutions, examine the perpetrators, and explain

¹ NCRB (National Crime Records Bureau), "Crime in India Report 2022", Ministry of Home Affairs, Government of India

² "A byte out of history: 10\$million hack "federal bureau of investigation 2014

why cyber crime is so pervasive with their help, we will examine the most effective methods for identifying fraudulent email and, finally, provide suggestions for reducing the alarming rise in cyber crime and the number of fraudsters involved.³

The issue of crime is caused by economic and social factors. Since common crimes such as stealing and burglary, up to more serious crimes such as espionage and treason, the idea of human wrong has continued to prevail in the history of humanity. This can be proven by various mythological stories and writings. Crime, regardless of the nature, has adverse consequences on all members of the society. The sharp growth of the internet and the digitization of business processes has caused the cyber crimes in developing countries to explode. Cyber crime refers to the application of computers and networks in crime. There is the possibility that the computer was targeted or it was used in a crime. Cyber crime is capable of jeopardizing the safety and financial conditions of a person. When confidential information has been intercepted or leaked legally or otherwise, this brings about a lot of privacy issues pertaining to criminality. Both the state and non-state actors commit espionage, money theft, and other types of transnational cyber crime across the globe. Cyber warfare is sometimes referred to as cyber crimes which involve activities of more than a single nation-state and cross the international boundaries. Cyber crime as Warren Buffett says is the most significant issue with mankind and it is real threats to humanity.⁴

The term “cyber crime” refers to any illegal act that makes use of computers, other networked devices, or networks in any way. While the vast majority of cyber crimes aim to enrich the perpetrators, a small percentage target computers or gadgets specifically with the intent to harm or disable them. Malware, unlawful information, photos, and other stuff can be spread through computers and networks by others. When perpetrated, some cyber crimes infect computers with viruses that then infect other computers and, in extreme cases, whole networks. Cyber crime has a significant impact on the economy. Ransom

³ Information Technology Act, 2000 (as amended in 2008), Government of India.

⁴ Indian Penal Code, 1860 – Section-65,66,66C,66D,67,72

ware 2 assaults, email and online fraud, identity theft, and efforts to steal financial account, credit card, or other payment card information are all examples of cyber crime. Hackers could target the theft and resale of confidential information pertaining to individuals or corporations. Cyber crimes are projected to increase in frequency in 2021 as a result of the pandemic's impact on distant workers. Consequently, safeguarding backup data becomes even more crucial.⁵

1.2 OBJECTIVE OF THE RESEARCH

The purpose of the research will be to research on cyber crime as another aspect of the Earth medical welfare and propose majors to commit this Threat, due to the fact that the internet is already a part of everyday life and that currently a network of million of computers distributed throughout the countries and because it is communication trades that enable a person to communicate with the vast majority of the population, as well as the selective audience and that Information Technology has been the most influential change agent of the past century and will continue to do so undoubtedly.⁶

The scholar has made the attempt to work the present in the quest of the remedy that would assist in managing and curing the Cyber crimes the rational discussed to the entire situation of the level and nature of Cyber crimes and the individual who perpetrates this crime in the law to heal these crimes. the scholar will also work towards strongly in the analysis of the various respective of the IT Act 2018 Amendment Act 2008 and also the bill and the potential means and basis to overcome them⁷. These will also be the research objectives –

- To examine the rule for cyber crime
- To make compression between various area.
- To find out the challenges faced by people at time of complain.
- To examine the role of authorities with the people.

⁵ Rohit Bansal, "Cyber Crime Trends in India: An Analytical Study", Journal of Cyber Security Studies, Vol. 8, No. 3, 2021

⁶ Pavan Duggal, "Cyber Law in India", Universal Law Publishing, 2019.

⁷ "Shreya Singhal v. Union of India", AIR 2015 SC 1523.

- To discuss the measures taken the government and other agencies for the cyber crime problem.

1.3 NEED OF RESEARCH & STUDY

A robust and efficient regulatory framework is required to further fortify the legal framework, which is essential to the expansion of electronic commerce. The field of cyber law encompasses all of these regulatory frameworks and laws. Since the internet, WWW, and Cyber space are integral to nearly every facet of modern life, cyber law is crucial. A cyber legal perspective should be considered for any online activity or response.⁸

The National Digital and 2000, neither. Cyber crime is not outlined in Safety Policy of 2013 or any other Indian law. In a very simple definition therefore, cyber crime involves the combination of conventional crime coupled with the application of. computers. Put simply, of a computer is referred to as a cyber-crime. Any crime regardless of its level of seriousness and nature can be categorized as a cyber crime in the event that the offender utilizes (or abuses) a computer to commit a crime or in the event that the victim is stored in the computer with important information. Under the I.T. Act, any item, such as a computer, computer network, data and information, required to commit a cyber crime, is considered.⁹

1.4 SCOPE THE RESEARCH

Besides the legal instructor, who is already decisive to the prosperity of electronic commerce, the electronic commerce has proposed an idea of pipe brand within effective regulatory apparatus. All these controlling mechanisms and legal systems fall under the jurisdiction of the Cyber Law. Cyber law is vital since it governs almost all forms of transactions or any activity that occurs on or within the internet, WWW, or cyber space. Every online action and response is legal and cyber legal. India has no laws defining cyber crime such as the IT Act

⁸ Reserve Bank of India, "Annual Report on Digital Frauds and Financial Cyber Crimes, 2022".

⁹ Arvind Singh, "Cyber Crime and Youth in Uttar Pradesh: A Sociological Perspective", International Journal of Social Sciences, Vol. 15, Issue 2, 2022

of 2000, Security Policy of 2013 and any other law. Cyber crime can be defined as any crime or transgression of computer and crime.”

Theft or pick pocketing is just like that which can be taken under the scrutiny of the border control of computer crime, and thus can weep a computer. The term cyber crime is used to refer to the commission of crimes with the use of computers and the information they hold by criminals either knowingly or unknowingly. Data, information, and any other elements essential to the commission of a cyber crime are defined in the IT Act. These would constitute the merger addition to the literature on the subject of cyber crime targeting youth, which is lacking in both overview and analysis. research to determine stakeholders' online habits, level of familiarity with online fraud, and prior knowledge; creation of online learning resources to incorporate into course modules; creation of hybrid regulations By introducing educational modules to certain domains, we can encourage participant engagement.¹⁰

1.5 RESEARCH MYTHOLOGY

The research methodology of proposed research work shall be non doctoral analytical or critical study, critical analysis of the stationary assessments that the IT Act 2000 as well as analysis of various statute operating in the field shall be made the judicial pronouncements of various Courts in India as well as the under the prominent jurisdiction of that area truly examine by the researcher in the instant study the present history shall collect collide and analyze different condition of the crime also the judicial decision of very sport beside this study shall encompass different reports books Law Journal and Statues of legist of various country article Publication in other material concert with its Ambit with the nature and types of the cyber crime at the Bundelkhand region of Uttar Pradesh¹¹.

¹⁰ Ministry of Electronics and Information Technology, Government of India, “Cyber Security Policy, 2020”.

¹¹ Rachna Gupta, “Cyber Crime in Rural India: Challenges and Awareness”, Economic and Political Weekly, Vol. 57, No. 11, 2022

1.6 SIGNIFICANCE OF THE STUDY

“Cyber Crime In India : A Critical Study With Special Reference to Bundelkhand Region In Uttar Pradesh”

The expansion of Electronic Commerce has suggested the necessity of pipe brand in effective regulatory machines which would go beyond the legal instructor so inhuman to the success of Electronic Commerce. All these controlling machines significant 8 due to the fact that it touches nearly all anticipations of transaction and activity and on the touching the internet, World Wide Web And cyber space. All activities and responses within the cyber space have certain legal and cyber legal dimensions. Cyber crime is not specified in the IT Act 2000, neither in the national Cyber security policy 2013 nor in any other regulation in India. A cyber crime can be defined as simply the combination of crime and computer or in other words any crime or weeping in which a computer is involved or abused by a fraudster even something as simple as stealing or pick pocketing is a computer network data information and any other data (as necessary) that falls under the borders of a cyber crime. These shell will be the little contribution in the field of the proposed work.

- Overview and analysis of critical areas of cyber crime related to children and teenagers,
- Preliminary research which aims to identify the previous knowledge, behavior in crime
- Virtual world, and awareness of Internet frauds, development of e learning materials to be included in the educational modules,
- Development of blended regulation.
- In order to achieve active involvement of participants, implementation of educational modules in selected areas

1.7 HYPOTHESIS

On the basis of mentioned objectives the present study aims at the test of following hypothesis :

1. There would be no significant difference between male and female/age group/education on cyber crime
2. There would be no significant difference between rural and urban are as on the crime and a relationship exists between the various age groups of the respondents and the awareness of cyber crime among them.
3. Statement to prove, cyber-crime prevention needs effectives laws, regulation, legislation, leadership and development of IPC in the areas of criminal justice with the help and efficiency of law enforcement authorities by providing and educating the mass whether it is governmental or private spheres to lessen such attacks and broaden the ambit of cyber-crime

1.8 RESEARCH DESING AND METHODOLOGY

1-Area of Study- the study would be conducted at Jalaun, Jhansi, Lalitpur, Banda, Mahoba, Hamirpur and Chitrakoot on social media use, money frauds, identity theft.

2-Data Type

A- Primary Data

- Interviews
- Questionnaire (online/offline)
- Data collection ,tabulation, analysis shall be done
- Simple size will be conduct later as per guidance of supervisor

B-Secondary Data

- Data from news
- Various journals

- Books
- Online data from various source

3-Research Tool

- Primary data—interviews and questionnaire
- Secondary data—cases, journals, publications

4- Sample Size

- Decided later on the basis of population

5-Sampling Tool

- Random sampling or probability sampling or any other way

1.9 REVIEW OF LITERATURE

A brief review of literature on cyber crime in India

- **Shruti Sunil Ajankar, Aditi Rajesh Nimodiya et.al. (2021)**¹² written a review of the risks of cyber attacks and protection against the unauthorized exploitation of system, networks and technologies they mainly focused on some of the techniques and perspectives on transforming the cyber security

- **Mohamed Amine Ben Farah, Elochukwu Ukwanu et.al. (2022)**¹³ were presented a classification of cyber attacks within the context of the state of the art in the maritime industry this research confirmed that the dramatic proliferations of cyber crime was fueled by increased levels of integration of new enabling technologies such as lot and big Data.

- **David ward, Paul Wooderson et.al (2021)**¹⁴ were presented an overview of standard development which help manufacturers keep up with changing technology and cyber attack method. They defined cyber security and its applies to automotive cyber physical system.

¹² International Journal of Scientific Research in Science and Technology, V- 8, Issue 6, Page Numbers: 464–472

¹³ Information 2022, 13(3), 146; <https://doi.org/10.3390/info13030146>

¹⁴ Automotive Cybersecurity: An Introduction to ISO/SAE 21434, SAE International, Dec. 15, 2021

▪ **Sanjeev Kumar** held in the **cyber crime in India Trends and prevention**¹⁵ a paper published in May 2021 edition there are many nutrients arise at the time of log down due to the people spend online everyday and increase relaying on the Internet to access service according to him the lockdown has exposed the weak cyber law and need to Reform Nation within the IT Act 2000 because it does not include much of the opposite expects.

▪ **Shweta Kumari Barnawal** published a **survey report on the cyber crime growing like seriously in Jamtara**¹⁶ in May 2019 edition according to the survey she said the cyber crime is increasing every year due to the lack of cyber safety and it effect our life this is the need of going economy how do it cyber space secured and protect Shweta Kumari Barnawal published a survey report on the cyber crime growing like seriously in Jamtara in May 2019 edition according to the survey she said the cyber crime is increasing every year due to the lack of cyber security and it effect our life this is the need of going economy how do it cyber space secured and protect.

▪ **Apurva Bhangel and Jeet Tulsi** written a paper a study on **cyber crime and its legal Framework in India**¹⁷ in international journal of law management and humanity 2021 edition the focus on the need of investments of law especially on the cyber crime with the reference to women and says to take preventive measures for cyber crime related to the women.

▪ **Sri Talwant Singh**¹⁸ the session judge of Delhi wrote a research paper on **cyber crime information technology** he provide the definition of Cyber crime according to the United Nations and compared it with the IT Act 2000 ,and focused the difficulties to registered a cyber crime to the police and said the poor rate of Cyber crime conviction in the country is also a reason of increasing the cyber crime.

¹⁵ <https://doi.org/10.17605/OSF.IO/HC4RZ>

¹⁶ International Journal of Research in Engineering, Science and Management Volume-1, Issue-12, December-2018 www.ijresm.com | ISSN (Online): 2581-5792

¹⁷ International Journal of Law Management & Humanities, Vol 4 Issue 2, pp. 493–504 (2021). DOI: 10.1732/IJLMH.26089.

¹⁸ cyberlaw - an overview. By. Talwant singh. Addl. Distt. & sessions judge: delhi. talwant@yahoo.com.

▪ **Justice Yatindra Singh's book cyber laws law on internet 6th edition** deals with all new Trends and long regulate the cyber law in India with description of its nature.

▪ **Dr Jyoti Rattna's book cyber laws and information technology 8th edition 2020** days with the specifically IT Act 2000 in the other subordinate laws relating the cyber crime justice with the specification of the cyber security in forensics.

▪ **Adv. Prashant mali's book cyber law \$cyber crime simplified** is all about cyber crime and cyber laws with the punishment and remedies as per Indian laws this book also served a awareness and regards to cyber law and cyber crime in the society.¹⁹

▪ **A.Sarmah** ²⁰ gives a paper in IRJET in June 2017 edition A brief study on cyber crime and cyber laws of India says there is need of spread the content of cyber crime among the common people because these crime never be acknowledged. If the criminal won't get punishment for their deed they will never stop.

▪ **Pune Citibank Mphasi S Call Center Fraud**²¹ The US customers of Citibank were bilked out of Rs 1.5 crores by a few former workers of the business process outsourcing (BPO) division of M Phasis Ltd, Msourc E. "Data Protection" was just one of several issues brought up by this cyber crime case. With "Unauthorized Access" to the clients' "Electronic Account Space" the criminal clearly achieved his goal. "Cyber Crimes" is the proper category to assign it to. Since any Information Processing Code (IPC) offence involving the use of "Electronic Documents" can be deemed as a crime involving the use of "Written Documents," IT Act-2000 is flexible enough to handle the components of crime that are not covered by IT Act-2000 but are covered by other statutes. Along with the clause in IT Act-2000, the terms "cheating," "conspiracy," "breach

¹⁹ UP Police Cyber Crime Department, "Annual Report on Cyber Crimes in Uttar Pradesh, 2023".

²⁰ International Research Journal of Engineering and Technology (IRJET) Volume: 04 Issue: 06 | June - 2017 www.irjet.net

²¹ Pune Citibank vs. MphasiS Call Center AIR (2005)

of trust,” etc., are thus appropriate in the aforementioned scenario. Both Section 66 and Section 43 of the IT Act-2000 acknowledge the crime. Consequently, it is possible to initiate the “Adjudication Process” to seek compensation from the perpetrators up to a maximum of Rs 1 million per victim, in addition to fines and jail time.

- **The Bank NSP Case-²²** The engagement and subsequent marriage of a bank management trainee is one of the most high-profile examples of cyber crime. The case involved Bank NSP. The couple used the workplace computers to send several emails. She sent letters to the boy's overseas clients using phonepe identities like “Indian bar associations” after the couple broke up. This was done by her using the computer at the bank. It is the boy's the business sued the bank after losing a significant number of customers. The emails sent through the bank's system were found to be the responsibility of the bank

- **Andhra Pradesh Tax Case ²³** Department officers obtained laptops used by an accused businessman from Andhra Pradesh in one of the several cyber fraud cases in India, exposing his dubious practices. Investigators from the Vigilance Department apprehended the proprietor of a plastics company and retrieved 22 million rupees in cash from his residence. Within a week, they expected him to provide an explanation for the missing funds. The accused assumed his crime would go unnoticed until he supplied 6,000 vouchers as proof of trade legitimacy; nevertheless, upon closer examination of the vouchers and the contents of his computers, it became clear that they were all created after the raids. The accused allegedly used computerized vouchers and phonepe ones to hide their true business activities, run five companies under the false impression of being one, and avoid paying taxes.²⁴

- **Bazee.com case²⁵** In December 2004, the CEO of Bazee.com was apprehended due to the sale of a CD containing explicit material on the website.

²² NSP Associates Pvt. Ltd .VS syndicate bank SA/34/ AIR 2019

²³ A. V. S. Narasimha Rao And Others vs The State Of Andhra Pradesh AIR 1969 SCC (1) 839

²⁴ “Phishing and Online Banking Frauds in India”, CERT-In (Indian Computer Emergency Response Team) Report, 2022

²⁵ Avnish Bajaj v. State (NCT of Delhi), AIR 2005

The CD was also peddled in Delhi's marketplaces. Responding swiftly were the police forces from both Mumbai and Delhi. A further bail hearing was held for the CEO. Because of this, the topic of how we differentiate between ISPs and content providers arose. The accused must prove that he was the one providing the service, not the content. Concerning the proper way for law enforcement to deal with instances of cyber crime, it also brings up numerous points.

▪ **Dr. Ishita Chatterjee (2022), Law on Information Technology, Published by Central Law Publications.** “The Information Technology Act 2000” This in-depth examination of a key statute in India that regulates online transactions and other forms of cyber crime is published by the law and justice publication company. An examination of the context that prompted the creation of the IT Act is the first section of this book. Bringing attention to the necessity of a legislative framework to tackle the obstacles posed by India's fast-paced IT development. Careful examination of the IT Act 2000's contents, purposes, and applications is provided in each section, illuminating the legal consequences, sequencing of these violations, and enforcement and prosecution mechanisms. Regulatory entities like the cyber appellate tribunal and the controller of certified authorities (CCA) are defined in it. Among the laws covered are the copyright Act and the Indian penal code, which are discussed in relation to the IT Act 2000. Current concerns including data privacy, cyber security, and the governance of digital platforms are addressed in the 2023 editions, which reflect the changing nature of computing and cyber law by including new revisions to the IT Act 2000 and the consequences they have for stakeholders. With in-depth research and practical insights, it is a crucial resource for comprehending the intricacies of cyber law in India. It is an excellent tool for navigating the vast landscape of IT law²⁶.

▪ **Rohit Arvind Jain Cyber Crime & Laws (2018), Published by Evincepub Publishing,** Offers a comprehensive review of the statutes and rules

²⁶ “Cyber Crime Awareness Among Rural Populations in Bundelkhand”, Research Paper, Banaras Hindu University, 2023.

governing cyber crime. With cyber risks on the rise and the necessity for strong legal remedies, cyber law is becoming more important. Examines the judicial and law enforcement branches' responsibilities in the fight against cyber crime. Contains instances and case studies that demonstrate the practical consequences of various offences. Discusses the legal procedures involved in prosecuting cyber offenders and looks at the difficulties encountered by law enforcement in investigating cyber crimes, such as jurisdictional issues and technological complexity. Examines legislation and enforcement strategies for cyber crime in various nations, drawing attention to the need for global cooperation to combat cyber crime that crosses national borders. Describes the changing character of cyber threats and new trends in cyber crime²⁷. Identifies the importance of regularly revising legal frameworks to account for evolving threats.²⁸

- **Satish Chandra (2017), Cyber Law in India, Published by ABS Books,** Gives a comprehensive analysis of the Indian legal framework governing cyber space. In light of the exponential growth of both cyber space and cyber-related problems, it discusses the rising significance of cyber law. To shed light on the legislative provisions controlling cyber operations in India, it dissects the IT Act 2000 and its revisions. Investigates the function of several regulatory agencies in the enforcement of cyber legislation. Emphasizes real-life examples and case studies to show how these crimes affected people and companies. Looks at the difficulties of data protection in the internet era, with an emphasis on the necessity of strong privacy regulations. Discusses copyright, trademarks, and patents as they pertain to the internet and the confluence of cyber law with intellectual property. Intellectual property rights enforcement in the digital era is the subject of this book. Examines the current state of cyber law and speculates on its future directions and difficulties.²⁹

- **Dr. J.P. Mishra (2014), An Introduction to Cyber Law, Published by Central Law Publications.** Serves as a comprehensive guide to understanding

²⁷ "Impact of Cyber Crime on Digital India Initiatives", NITI Aayog Report, 2022.

²⁸ Madhurima Sen, "The Role of Social Media in Cyber Crimes", Journal of Media and Law, 2022.

²⁹ The Role of AI and Machine Learning in Cyber Crime Detection, IEEE Research Paper, 2021.

the legal frameworks governing cyber space. It addresses the repaid evolution of technology and its implication for law and society. This book also examines laws related to data protection, emphasize the importance of safeguarding personal information. Analyses how traditional intellectual property laws apply to digital content and issues related to copy right, trademarks and patents in cyber space. It provides an overview of National and International regulations affecting cyber law. The role of organizations like the United Nations in shaping cyber law policies.³⁰

▪ **Dr. Bhagyashree A. Desphande (2019), Text Book on Cyber Law, Published by Central Law Publications.** Provides a comprehensive examination of the legal principles governing cyber activities. It introduces the basic concepts of cyber law, including definitions and the significance of legal frameworks in the digital environment and evolution of cyber law in response to technological advancements.³¹ It covers various regulations related to data protection, privacy and electronic transactions with the discussion of the legal resource available for victim of cyber crimes. It addresses contemporary issues such as the impact of artificial intelligence, block chain technology and the internet of things (LOT) on cyber law, discusses frameworks to keep pace with rapid technological changes the need for adaptive legal.³²

▪ **“Landmark Judgement on cyber crime and cyber laws”** Offers an in depth analysis of significant legal rulings that have shaped the landscape of cyber law. It have details landmark cases that have set precedents in cyber law, discussing their implications for future legal interpretations.³³ Each case is analyzed in terms of its legal reasoning, outcomes, and impact on cyber crime legislation.³⁴ It explores the existing legal frame works governing cyber crimes, including the IT Act 2000 and other relevant laws. Discusses the challenges faced

³⁰ Bundelkhand Cyber Crime Cell Report, 2022.

³¹ Indian Evidence Act, 1872 – Amendments related to Electronic Evidence.

³² Surabhi Sharma, “Cyber Bullying in Rural India: An Unseen Threat”, Journal of Digital Law, Vol. 12, Issue 1, 2023.

³³ Puttaswamy v. Union of India”, AIR2017 SC – Right to Privacy and Cyber Law Implications.

³⁴ “Dark Web and Its Influence on Cyber Crime in India”, Centre for Internet and Society Report, 2023.

by the judiciary in adapting traditional legal principles to the digital context. It highlight low landmark judgments have addressed these issues and the legal remedies available to victims. Examines the broader implications of judicial decisions on policy making and legislative reforms in cyber law.³⁵ Discusses the need for updated laws to address emerging technologies and cyber threats with encourages ongoing dialogue among legal scholars, practitioners and technologists to foster a more robust legal framework.³⁶

³⁵ Deepak Verma, "Challenges in Cyber Policing in Rural India", *International Journal of Cyber Law*, Vol. 14, No. 3, 2022

³⁶ Uttar Pradesh Cyber Crime Helpline Data, 2023.

CHAPTER–II

CONCEPTUAL ANALYSIS OF CYBER CRIME ON SELECTIVE AREA

2.1 CYBER CRIME

“From most terrestrial crimes, cyber crime differs in four ways: it is easy to learn how to commit, it requires few resources relative to the possible harm caused, it can be committed in a the authority without being physically present in it, and fourthly, it is often not clearly illegal,” states McConnell International, defining cyber crime as any harmful act devoted from or against a computer or network.³⁷

“Cyber crime (machines crime) is any illegal behavior directed by means of electronic activity that targets security of computer networks and the data processed by them,” said the director of the Computer Crime Investigation Centre (CCRC) in an interview on April 27, 2004. Essentially, cyber crime refers to criminal activity that takes place in an online environment, where data pertaining to real-life entities, such as people, places, things, events, or processes, is stored and transmitted across various networks, both local and global.

First of all, it would be prudent to define what is meant by cyber crime and distinguish it with conventional crime in a manner that is universally acceptable. Indian Penal Code handles traditional types of crimes that may occur in the cyber space such as stealing, lies, forgery, defamation and injury. Cyber crimes have also been caused by the abuse of computers and are treated by Information Technology Act of 2000. New age crimes in many forms are born out of acts punishable under the Computer Technology Act.³⁸

The Indian penalties code already addresses many cyber crimes such as e-mail spoofing, cyber defamation, writing threatening emails etc. and as such, they

³⁷ National Crime Records Bureau (NCRB), “Crime in India Report 2022”, Ministry of Home Affairs, Government of India.

³⁸ Information Technology Act, 2000 (Amendment 2008), Government of India.

are not to be defined. In its simplest definition, cyber crime refers to crime in which the computer is used as an instrument or as an object or both precise.”

Now we'll take a look at the ways in which the computer is used for illegal purposes. Typically, this type of action entails utilize computers to alter a traditional crime. Here are a few scenarios:

Financial Crimes

A site claimed to sell Alphonso the mangoes at a discard price, citing a recent incidence, as an example of this. Other examples include credit card fraud, money laundering, and deception.³⁹

A site claimed to sell Alphonso the mangoes at a discard price, citing a recent incidence, as an example of this. Other examples include credit card fraud, money laundering, and deception.

Cyber Pornography

All of the following would be considered pornographic: websites that host explicit content; pornographic periodicals that use computers for publication and printing; and the Internet for the downloading and transmission of explicit content. The Army's Bal Bharati School case is one of several recent cases in India involving cyber pornography. All of a student's classmates picked on him because he had a pockmarked face at the Air Force Bal Bharati School in Delhi. The relentless mockery finally drove him to action, and he planned to exact revenge. He created a website using a free web hosting provider, scanned pictures of his teachers and classmates, and then merged them with naked photos. Nothing happened until the father of any of the class girls who had appeared on the website voiced his objection and filed a police report.⁴⁰

Another instance was a Swiss couple who, in Mumbai, would round up children from slums and subject them to sexually explicit picture shoots. They

³⁹ Indian Penal Code, 1860 – Sections 66, 67, 420, and other provisions related to cyber crime.

⁴⁰ Rohit Bansal, “Cyber Crime Trends in India: An Analytical Study”, Journal of Cyber Security Studies, Vol. 8, No. 3, 2021.

would thereafter post these images to websites catering specifically to pedophiles. Couple apprehended by Mumbai police for porno graphic material.

Sale of Illegal Articles

Some examples of this kind of online trade include the sale of illegal substances, firearms, and even animals through classified ads, online auctions, and even email. For instance, there are rumors that some Indian auction houses are peddling cocaine under the name “honey.”⁴¹

Online Gambling

Online gambling is available on millions of websites, all of which are hosted on servers located abroad. Many such websites may be fronts for illegal money laundering operations, according to certain reports.⁴²

Intellectual Property Crimes

Some examples of these crimes include stealing computer code, infringing on trademarks, copyright violations, and software piracy.

E-mail Spoofing

A faked email is one that uses a false sender address but is actually from another account. e.g. You can reach Pooja at pooja@aianlaws.org. Sameer, her adversary, creates a fake identity for her email and uses it to send vulgar messages to everyone she knows. Friends of Pooja's could take offence and relationships could be damaged irreparably if the emails really came from her. Money can potentially be lost due to email spoofing. A young American man made a billion dollars in one instance by spreading rumors about certain firms that he had short sold. Shares brokers and investors were led to believe that the companies were in dire straits when they received bogus e-mails claiming to be from news sources like Reuters. Thousands of people lost a lot of money since share values never recovered to pre-disclosure levels.

⁴¹ Pavan Duggal, “Cyber Law in India”, Universal Law Publishing, 2019.

⁴² The threat from the internet :Cyberiar ECONOMIST ,july 2010,at 50

Forgery

It is possible to create counterfeit money, postage, revenue stamps, mark sheets, etc., with the use of modern printing and scanning technology. It is not uncommon to see touts outside of several colleges in India offering to sell fake credentials or mark sheets. A combination of computers, top-notch scanners, and printers goes into their creation. Actually, student gangs are making a killing off of this scam, which involves paying thousands of rupees for credentials that seem fake but are actually quite real.⁴³

Cyber Defamation

When one person has defamation to commit, this is referred to as online slander such as publishing some false information about another person on a web site or sending a chain e-mail to all the acquaintances of that person.”

The young woman known only as Surekha (all names have been changed) was recently engaged to the man known as Suraj. Even though it was an arranged marriage, she was overjoyed because of her felling for Suraj. He gave the impression of being friendly and accommodating. Then, she noticed that Suraj appeared anxious and even slightly distressed the day they crossed paths. Discussing her interests did not pique his attention. When she probed further, he revealed that Surekha's character had been the target of nasty e-mails sent to his family. They brought up affairs that she has had before. He informed her that his parents' feelings of justified sadness were palpable, and that they were contemplating ending the engagement as well. Thankfully, Suraj won over his parents and other household elders to contact the police rather than accepting the mail's malicious claims.⁴⁴

It was found out during the investigation that Surekha's stepfather was the one sending such emails. His goal in sending these emails was to end the marriage. Before the girl was married, he was the legal guardian of her property; once she got married, he would have lost custody of it.

⁴³ “Shreya Singhal v. Union of India”, AIR 2015 SC 1523.

⁴⁴ A Interpol Report on Global Cyber Crime Trends, 2022.

In the United States, there was another high-profile instance of online defamation. A woman's whole social circle was inundated with sexually explicit emails that seemed to come from her inbox. Among her friends, the woman in issue was getting a terrible rap because of these emails. This woman was a staunch opponent of porn. Actually, a group of crowd werw unhappy with her opinions and furious that she opposed them had resolved to retaliate against her by employing such deceitful tactics. Furthermore, they posted web pages smearing her character and sent defamatory emails to her friends and family in addition to sending counterfeit obscene emails.

Cyber Stalking

Stalking is defined as “pursuing stealthily” in the Oxford English Dictionary. By repeatedly emailing the victim, joining the chat rooms they visit, posting messages (often threatening) on bulletin boards they frequent, etc., cyber stalkers follow their victims wherever they go online.

In light of the foregoing, it is reasonable to assume that cyber crime involves the intentional manipulation, tampering, or destruction of computer data or networks. It entails using a computer to conduct a criminal or executing a crime against computer systems.⁴⁵

Crypto Jacking

When computer hackers illegally access the computer of a different individual to extract crypto currency, such action is referred to as crypto jacking and is closely linked to crypto currency. A web site may be compromised or the victim may be duped to do a dangerous click in order to gain access. To this, they also utilize web adverts which incorporate the use of the java script code.⁴⁶

Meaning and Concept of Cyber Law

Internet law, or cyber law, is another name for this field. Cyber law's concept and meaning encompasses the following: what is cyber law, why is cyber

⁴⁵ CERT-In (Indian Computer Emergency Response Team), “Annual Cyber Security Report 2022”.

⁴⁶ Reserve Bank of India, “Report on Financial and Banking Cyber Frauds”, 2022.

law necessary, rules of computer law and its realm of application. These subjects are covered in

(i) Meaning of Cyber Law

The branch of law that governs matters pertaining to the Internet is known as cyber law. Cyber space and their corresponding legal difficulties. Freedom of speech, internet access and use, and online privacy are just a few of the many subtopics that fall under the umbrella of cyber law.

Everything having to do with computers, software, hardware, and information systems (IS) as well as the Internet falls under the purview of cyber law.

Techo Pedia explains cyber law as

Information access, solitude, communication, intellectual property (IP), and freedom of speech in relation to the use of internet-based websites, e-mail, phones, computers, software, and hardware, including data storage devices, are all protected by cyber law, which aims to prevent or lessen the impact of cyber criminal activities.

Cyber law refers to that area of general law that deals with issues governing the cyber space, the internet and other related technology. The issues covered by cyber law are very broad and in addition to privacy of the online world, freedom of speech, as well as access and use of and by the Internet are also a part of the cyberspace. The internet law or simply the law is more commonly referred to as cyber law.⁴⁷

Definition of Cyber Law –

One of the most dynamic and constantly evolving branches of law in the contemporary time is the field of cyber law that involves criminal and civil laws dealing with Internet-based behavior and transactions.

⁴⁷ Lok Sabha Debates on Cyber Crimes and Digital Security, 2023.

Moreover, this area of law deals with issues of the purpose and delivery of communications, as well as the communication, which involve, though are not limited to the following: the protection of proprietary information, the freedom of expression, and provision of public record.

1. **M.A.A. Alavi** says “Cyber Crime is defined as any criminal activity that involves a computer or Networked device, where the computer is either a too or a target of the Crime.”

Source– Alavi, M.A.A. (2015), “Cyber Crime : A New Challenge for law enforcement.”

2. **R.M. Clarke Says** “Cyber Crime refers to any illegal act that involves a computer or a network, including crime such as hacking, online fraud, and identity theft.”⁴⁸

Source- Clarke, R.M. (1999), “The Regulation of Cyber Crime : A Comparative Analysis”

3. **K.A. Stohl Says** “Cyber Crime Encompasses a wide range of illegal activities conducted via the internet, including but not limited to cyber bulling, phishing and the distribution of child pornography.

Source-Stohl, K.A.(2011) ”Cyber Crime: A Multidisciplinary Approach.”

4. **J.J. Wall Says,** “Cyber Crime is a term used to describe criminal activities that are carried out using computers or the Internet, Including offence against individuals property, and society as a whole.”

Source- Wall, J.J. (2007), “Cyber Crime : The transformation of crime in the information age policing and society.”

5. **M.A.S. AI- Khalifa says-** “Cyber Crime is the use of the internet and computer technologies to commit illegal activities, and it poses significant challenges for law enforcement and society.”

Source-AI-Khalifa, M.A.S.(2013),”Cyber Crime, A Global Perspective.”

⁴⁸ European Union Agency for Cybersecurity (ENISA), “Cyber Crime Landscape”, 2021.

These were the foreign authors thought cyber crime while Indian authors says little bit different.

6. **Dr. S.K. Singh Says**, “Cyber Crime refers to any illegal activity that is conducted through the use of computers and the internet, including lacking, online fraud, and identity theft.”

Source- Singh, S.K. (2012), “Cyber Crime ‘An Overview’” International Journal of Computer Application.

7. **Dr. R.K. Gupta Says**, “Cyber Crime is defined as a crime that involves a computer and a network where the computer may be used as a tool, or a target.”⁴⁹

Source- Gupta, R.K. (2013), “Cyber Crime and cyber security : A study” Journal of Information Technology and Software Engineering.

8. **Dr. A.K. Sharma Say**, “Cyber Crime is a growing concern in India, involving various forms of illegal activities conducted through digital platforms, affecting individuals and organization a like.”

Source- Sharma, A.K. (2016), “Cyber Crime in India, A study of trends and challenges” Journal of Cyber Security Technology.

(ii) Need for Cyber law

The need of cyber law are as-

- law is needed for the regulation of cyber crimes.
- Cyber is crucial and it is needed to exercise supervision and control on transactions and behavior on transactions and behavior on and concerning the Internet, the worldwide web and cyber space.
- Cyber law is vehemently needed as it exercises control over all categories of cyber crimes such as child pornography, cyber harassment, cyber stalking, cyber defamation, e-mail spoofing, cracking, SMS spoofing, pornography,

⁴⁹ Challenges in Cyber Policing in India”, International Journal of Cyber Law, Vol. 14, No. 3, 2022.

frauds, on-line libel, on-line slander, cyber smearing, trafficking, financial frauds, identity theft, cyber squatting, cyber trespass, DDOS attacks, worm attacks, hacking, intellectual property theft, cyber terrorism, cyber welfare, pirated software etc.

- Cyber law is needed to help and protect the people and organizations on the internet from malicious people on Internet.

- Cyber law is needed specific issues of intellectual property law, contract law, privacy, freedom of expression and cyber jurisdiction.

(iii) Jurisprudence of Cyber Law

Jurisprudence is a legal philosophy or philosophy of law. Today, the society is facing ethical issues and challenges from social networking sites. Jurisprudence of cyber law is needed to handle and tackle these issues and challenges in proper way. From the view of utilitarian theory, the means for achieving happiness cannot be determined a priori. Determination of a priori is also not possible in a case of social networking sites.⁵⁰

The establishment of the social networking sites brought about a number of legal concerns. The international cooperation and contribution are considered to be the primary cause of the jurisprudence development. The laws pertaining to cyber legislation in most of the countries have been structured based on the foundation of several international instruments or treaties.

The UNCITRAL Model Law has also been taken seriously by cyber laws. The alterations in cyber laws in India and other countries have been highly informed by the court rulings, despite the fact that there are not numerous rulings concerning the same as opposed to other laws. The technological standards are critical in dictating the legislative actions required to bring a fair and practical regulatory framework due to the techno legal cyber law. Many jurists have in their critiques made it clear beyond doubt that international collaboration is required to maintain cyber space under control. International cooperation is

⁵⁰ Data Security Council of India (DSCI), "State of Cyber Security in India", 2022.

hopeless and oblivious as it is. In this regard, cyber legislation harmonization is an immediate need.⁵¹

(iv) Scope of Cyber Law

The coverage of cyber law is growing at an alarming rate in the contemporary world. In the case of internet related crimes, cyber law is the place to be. Throughout this document, cyber crime prevention, prohibition, regulation and control are all discussed. Hacking, virus distributions and cyber terrorism are all popular types of cyber crime.⁵²

When it comes to corporations, cyber law has a lot of potential. Cyber law specialists are in high demand in many industries these days, including the military and corporations. Administration, research and development, lobbying, etc. Cyber law refers to the area of law where the Technology Act of 2000 deals with all cyber crimes. Individuals are safeguarded from cyber crime and ethical lapses by cyber law.

No one region can be the exclusive domain of cyber law. It encompasses both domestic and international legal systems. The area of cyber law offers a great deal of opportunity for solicitors. Jobs in the field of cyber law include cyber consultants for IT firms, cyber lawyers, research assistants for tech firms, web developers, web advisors, corporate entities, and enforcement agencies, among others. Cyber law is a broad area, with many potential employers. The expansion of cyber law is a direct result of the rise of cyber forensics.⁵³

The cyber law covers numerous aspects of cyber world. All these include cyber security, cyber crime prevention and regulation, jurisdiction of cyber space, E Governance, domain name disputes, trademark law, electronic commerce, the role of international organizations and constitutional or human rights issues in the cyber space etc.

⁵¹ National association of software and service companies ,BBC news.com /10 jan 2010/news

⁵² Pawan Dugal, "Cyber Law in India", Universal Law Publishing, 2019.

⁵³ Rachna Gupta, "Cyber Crime Awareness in Rural India: A Case Study", Economic and Political Weekly, Vol. 57, No. 11, 2022.

Frequently used Cyber Crimes

Unauthorized access to computer systems or networks

Hacking refers to this type of behavior. Unauthorized access and hacking are not synonymous in the Indian law since the terms are defined differently in India. Cyber attacks of stolen computer files.

Hacking is the term used to define this kind of behavior. It terms Unauthorized access and hacking are used interchangeably due to the difference in terms as defined by the Indian law. Online theft of digital data.

E-mail bombing

The term “e-mail bombing” describes the practice of flooding a target with so many messages that their inboxes (if they are individuals) or mail servers (if they are businesses or ISPs) go down. An expat who had lived in Shimla, India for about 30 years sought to take advantage of a program the Shimla Housing Board had set up so that people could purchase land for less money. Because the initiative was exclusively open to Indian citizens, his application was denied. He made up his mind to get even. As a result, he inundated the Shimla Housing Board with hundreds of emails, which he continued sending until their servers went down.⁵⁴

Data Diddling

In this type of assault, the attacker changes the raw data right before the computer processes it, and then changes it back once the processing is finished. During the process of privatization, data-tampering programs were introduced into the systems of India's electricity boards.

Salami Attacks

These attacks contribute to the commission of financial crimes. In case a bank employee were to implement a program in the bank servers that will automatically deduct a small amount (say Rs. 5 each month) on the accounts of each customer it will not be reported in one occasion due to the fact that the

⁵⁴ Vakul Sharma, information technology : law and practice 191 (universal law publishing edn. 4th, 2015).

difference will be minimal. The account customer might not know that such an illegal debit is made, but the bank employee is sure to get a good amount on a monthly basis. As an example, an American bank employee has lost his job. Out of frustration because of what he felt were mistreatments by his seniors, the person first had to plant a logic bomb on the systems of the bank.

A logic bomb is a software which when a certain condition is fulfilled, will execute the program. The logic bomb was configured by default to withdraw ten cents per bank account to that bank account which had its name last in the list, or in alphabetical order. Then he went on to open an account under the name of Ziegler. When the money was withdrawn at Nobody at the bank or even the people who held the account did not even realize that there was an error due to the small amount of the accounts. They discovered about it when a customer by the name Ziegler opened an account there. He is surprised by the huge amounts of cash that cropped up in his account each week without explanations.

Denial of Service Attack

A possible method of doing this is to request the help of a computer resource beyond its capabilities. Owing to this, the resource (such as a web server) collapses and ceases its service delivery to the authorized users. The other type of attack that is similar to the normal DOS attack is the distributed denial of service (DDoS) attacks where two or more attackers collaborate to flood a target⁵⁵. These attacks are very difficult to control. The attack starts by bombarding the servers of the victim with requests that lead to crashing of those servers since they become overwhelmed. In the past, links to such sites as Amazon, CNN, Yahoo!, eBay have all been shut down by denial-of-service attacks!

Virus/Worm Attacks

The viruses are software elements that infect computer and files by attaching to one and then transferring to other files and computer in a network. These attacks mostly target computer data that may be deleted or modified.

⁵⁵ Bundelkhand Cyber Crime Cell, "Cyber Crime Report for Selective Area", 2022.

Unlike viruses, worms are able to attach themselves to whatever they find pleasing. They simply reproduce themselves on a functional scale and continue so until all the RAM of a computer is occupied.

Logic Bombs

Programs that are event dependent are available. This implies that such programs are programmed to get activated when a certain occurrence takes place; an example being the Chernobyl virus is a logic bomb as it is not active most of the year but it only activates on a particular date.

Trojan Attacks

It is a Trojan horse since it is the unauthorized program which conceals its real purposes as it is implemented in the functionality of an authorized program.

A Trojan can be installed in the computer of a person in many easy ways. As an example, two friends Rahul and Mukesh (identities withheld) were engaged in a fierce quarrel over a girl, Radha (identities withheld) whom they both were fond of. Rahul had a way of shooting himself in the head when the girl who was asked to make a choice instead of Rahul chose Mukesh. On 14 th February, he spoofed Mukesh with an e-card, which supposedly originated in the mail account of Radha. The Trojan was in fact stored in the e-card.

The Trojan was installed on the computer of Mukesh as soon as he opened the card. As it turned out, Rahul was in full control of the computer of Mukesh and went ahead to harass him in every way possible.⁵⁶

Internet Time Thefts

This is an indication that one is stealing another individual to use his or her paid Internet time without authorization. Before the enactment of Information Technology Act in 2008, a man by the name of Colonel Bajwa of New Delhi approached one of the local internet cafes owners and asked him to install his Internet connection. To achieve this goal, the owner of the cybercafé must be aware of his logins. Once connected, he took away the existing login credentials. He sold this

⁵⁶ Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, 2023.

information to another internet cafe afterwards. After a period of seven days, Colonel Bajwa found out that his Internet time was almost over. In the same week, he had consumed 100 of the hours he had bought. This surprised him and he reported to the Delhi police and shared what happened. The police officers could not imagine that he could have taken so much time.

They completely did not know what time-theft was. Nobody was interested in any findings of Colonel Bajwa. He chose to go up to her. Revised: New Delhi, The Times of India. The report by the New Delhi Police revealed that they had been wanting in handling cyber crimes. The Delhi Police Commissioner then decided to take the law into his hands and made a raid which led to the arrest of the net maker owner of the eatery charged with a felony theft case under the Indian law. During his time in the Tihar prison, the owner of the online cafe received a halal license.

Web Jacking

Once an individual breaks into a site and alters the password, he or she has conquered the site. What is found on a web site is no longer the real owner of the web site. One of the women in the US was recently sent an email by the owner of a children leisure site informing her that a group of hackers had stolen her domain. They demanded one million dollars in order to release her. The fact that the owner was a teacher led her to ignore the threat. She did not pay attention to the email because she believed that it was an intimidating tactic. Until, she did not find out that her website had been hacked after receiving numerous phone calls from throughout the nation. A section of the website named “How to have fun with goldfish” was subsequently upgraded. They had swapped over the word “goldfish” with “piranhas” anywhere it had been referenced. The tiny, deadly fish known as piranhas feed only on flesh. A large number of kids had gone to the well-known website and bought into its claims. Tragically, these kids got themselves severely hurt after following the directions and playing with pet piranhas!⁵⁷

⁵⁷ UP .Police.(2020,august,13)overview of cyber crimes

Theft of Computer System

Theft of a computing device, computer component(s), or computer peripheral(s) is an example of this sort of crime.

2.2 CAUSES OF CYBER-CRIME

The following are three of the most common justifications given by cyber criminals for engaging in cyber crime

- It is possible to commit cyber crimes in order to gain recognition. Most of the time, this is done by kids who are trying to make a statement and feel special of the group of society's large and powerful men. Idealists who simply seek attention, they have no ill intentions and do not intend to cause harm to anyone.
- The desire to earn fast cash is another factor contributing to cyber crime. This gang is comprised of career criminals driven by avarice who manipulate data on the internet, particularly those pertaining to online banking and e-commerce, in order to perpetrate fraud and steal from naive consumers.
- Thirdly, cyber crime can be perpetrated in defense of a cause that the perpetrator believes in, with the goal of causing harm to those who receive it. When it comes to reasons for cyber crime, this is the worst. They don't care who or what fighting for a just cause, so long as they succeed in achieving their objectives. Now we have our cyber terrorists.

The internet based on the general Internet Protocol Suite (TCP/IP) to provide billions of users across the world. The Internet has brought a myriad of potential information resources and services, including the hypertext documents of the World Wide Web (WWW), which are inter-linked, and the infrastructure necessary to facilitate electronic mail. Any one is able to obtain information at any location and any time but the information available on the internet is subject to manipulation by the third party in any way of hacking, phishing, etc. to damage the computer and data stored in computer or accessible on the internet. This kind

of occurrence is referred to as cyber crime.⁵⁸ Cyber crime in any case includes the violation of the privacy of other people or harm to computer-based property including files, web pages or software. This paper is absolutely based on the cyber crime problem, crime patterns and problems that are experienced by Indian users and how the issue of cyber crime can be reduced through the establishment of effective cyber crime legislation in India. Indian cyber crime Statistics, cyber crime cells all over India, and numerous other latest news are also included in the paper. The agencies at the national level can design security guidelines and policy to prevent and protect internet users against cyber crimes.

Present Trends of Cyber Crime in India

India is doing its best to execute the Digital India project, which has a bad track record. When there is maximum connection and minimal cyber security hazards, the Digital India project will be a success. Because of its need to maintain strict control over cyber security, this is an issue for India as well.⁵⁹

The number of recorded cyber scams increased from 22,060 in 2020 to 71,780 in 2021, according to data from the Home Ministry. Up to June 2022, 62,189 cases of cyber fraud have been recorded.

A multitude of international hacker gangs breached 28,481 Indian websites in 2020. After 21,699 in 2021, 27,605 hacking incidents were recorded in 2022.

The National Cyber Records Bureau reports that 1,791, 2,876 and 4,356 cases were registered in the Information Technology Act in 2021, 2022, and 2023, respectively, pertaining to cyber crimes. The number of cases registered under section 422,601 in 2021, 1,337 in 2022, and 1,337 in 2023.

The number of cyber crime incidents reported in the nation has increased by over 40% every year for the last two to three years. During 2018, 2019, 2020, 2021, and 2022, a total of 2,876 cyber crime cases were reported under the IT Act

⁵⁸ Sandeep Yadav, "Cyber Crime Against Women and Children", *Journal of Law and Cyber Security*, Vol. 10, No. 2, 2023.

⁵⁹ Interpol, *Cyber Crime Trends Across Nations*, 2023

2000, according to the National Crime Records Bureau (NCRB). Based on data collected and maintained by the In), a grand total of 308, 371 government websites fell victim to hacking in 2021, 78 in 2022, and 16,035 incidents involving spam, malware, and system break-ins were recorded in 2023.

Cyber Crime Prevention Strategies

The most current forms of cyber crime pose a significant threat to any nation's progress since they affect every facet of that progress. Official agencies, charitable organizations.

The cyber crime gang can hit both the state and non state organizations, and individuals. Cyber criminals like the more traditional criminals are interested in making money in the easiest and quickest way possible. there are a number of critical aspects to the fight against cyber crime, the best of them is the prevention of cybercriminal acts, which could be done quickly and at a low cost. The tenets are awareness and exchange of information. In an attempt to safeguard self against cyber crime, one is expected to assume a security posture. All those who consume technology must be aware that they are all potential victims of cyber criminals, and that there are measures that they can implement to present a lesser target area and defend themselves.⁶⁰

Statutory Provisions

The Indian parliament stated that it needed to consider the resolution carefully and, therefore, passed the same way which saw the adoption of the UN Commission on Trade Law Model Law on Electronic Commerce of the General Assembly. This law is meant to repeal the following laws: 1860, the Indian Evidence Act 1872, the Banker Schedule Evidence Act 1891 or the Reserve Bank of India Act 1934; it is also meant to legalize the electronic commerce and this is mentioned in preamble of the Information technology act 2000 passed and brought to force on 17 th May 2000. These Acts must be amended to adopt them

⁶⁰ Rohit Bansal, "Cyber Crime and Legal Challenges", Journal of Cyber Security Studies, Vol. 8, No. 3, 2021.

in line with the IT Act of 2000 in an effort to establish effective means of regulating and supervising cyber global affairs.

Cyber crimes are covered in detail in chapters IX and XI of the Information Technology Act. Particularly noteworthy are sections 43, 65, 66, and 67. Unauthorized access, illegal downloading, virus assaults, or any contaminant that damages, disrupts, denies access, or interferes with a person's service is specifically addressed in Section 43. As a remedy, this clause allows for a fine of up to one crore Indian rupees. "Tampering with computer source documents" is addressed under Section 65, which carries a maximum penalty of three years in prison and/or a fine of up to two lakhs, or both. Penalties for "hacking with computer system" as outlined in Section 66 include a fine of up to 2 lakhs or three years in prison, or both. In addition, Section 67 addresses the distribution of pornographic content and establishes penalties include fines of up to 2 lakhs rupees and jail terms of up to 10 years.

Analysis of the Statutory Provisions

As far as there has never been legislation covering this niche industry, the enactment of the IT Act of 2000 was, by all means, a good move. on the other hand, the Act has proved to be somewhat ineffective in its application. The Act's numerous gaps are:

1. 'The legislation was approved too quickly, without enough public debate, and it failed to achieve its intended goal. Legislation has been inadequate, according to experts, in part because parliament passed it too quickly and, as a matter of fact, not enough time was allowed for public debate.⁶¹
2. "It is explicitly stated in the preamble and goal of cyber laws that they are intended to assist e-commerce rather than regulate cyber crime. One reason the Information Technology Act of 2000 (IT Act) is inadequate to handle instances of cyber crime, according to Mr. Pavan Duggal, is that its primary purpose was to establish a framework for regulating electronic business.

⁶¹ "Dark Web and Its Influence on Cyber Crime", Centre for Internet and Society Report, 2023.

3. **Cyber torts** : Cyber stalking, cyber harassment, cyber nuisance, and cyber defamation are all new types of cyber crime that the I.T. Act of 2000 has failed to address. Also, new types of cyber crime will supposedly appear in the future and will require attention as well. That is why India ought to become a party to the cyber crime treaty. Nevertheless, these offences can be dealt with by reading the I.T. Act 2000 in conjunction with the Penal Code.
4. **Ambiguity in the definitions** : Section 66 of the Act provides a broad and potentially misused definition of hacking. Misapplication of this provision is certainly possible. The Delhi court has indeed erred in its use of this provision, which is entirely susceptible to misapplication. It is now abundantly evident, thanks to the notorious go2nextjob instance, that might be the end result for someone who is charged under section 66 or the ongoing danger that internet users face. There is 66 as it is right now. To add insult to injury, section 67 is not really clear either. Lascivious or obscene pornographic information is a phrase with a murky definition. The Bal Bharati case further demonstrated our incapacity to handle cyber pornography cases.⁶²
5. **Lack of awareness** : Insufficient public understanding and subsequent failure to put the Act of 2000 into practice are major factors contributing to its incomplete success.
6. **Jurisdiction issues** : Because cyber space is accessible from anywhere in the world, jurisdiction is another contentious issue in instances involving cyber crime. It would appear that the idea of territory is becoming obsolete in the face of the expanding cyber weaponry. Traditional approaches to conflict resolution should give way to more innovative ones. Nothing in the Act of 2000 addresses these concerns.

⁶² Madhurima Sen, "Social Media and Cyber Crimes: A Legal Perspective", Journal of Media and Law, 2022.

7. **Extra territorial application** : The extraterritorial operations of this law, as provided for in Section 75, will only be effective if accompanied by measures to recognize warrants and orders for information issued by those in charge outside of their jurisdiction and enhance cooperation for the exchange of evidence and materials pertaining to computer crimes among law enforcement agencies.
8. **Cyber savvy bench** : We urgently require judges who are up-to-date on technology. It is the responsibility of the judiciary to shape the enactment in accordance with the current order of business. The Kerela High Court acknowledged the P.I.L. via email, which is an important step that deserves praise. The assertion that judges carve law is to 'law ought to be' provides a clue as to the role of judges in today's world. A member secretary of the Law Commission, Mr. T.K. Vishwanathan, has outlined the necessary steps to establish electronic courts in India. He declared in an article for the Hindu that “the Judicial System is one area of Governance where IT may create a huge difference to Indian public.”
9. **Dynamic form of cyber crime** : Admitting that cyber crime is ever evolving “In short, despite our markedly improved capabilities to fight cyber intrusions, the threat is growing even faster and they are falling further behind,” stated FBI Director Louis Freeh. No legal framework can constrain the (de)creativity of the human mind. Therefore, when it comes to applying the laws to situations of cyber crime, the only way out is through liberal construction.⁶³
10. **Hesitation to report offences** : One of the major problems with the Act, as mentioned before, is that cases are often not reported. The police department's lack of cooperation is a prime example of this. Time theft in Delhi provided conclusive evidence of this. When it comes to stopping cyber crime, the police are a formidable force in the modern world. Simultaneously, it has the potential to become overbearing and obstruct

⁶³ UP Police Cyber Crime Department, “Cyber Crime Cases in Selective Areas”, 2023.

innocent people's ability to go about their regular online activities. The events at Meerut and Belgam further reveal the administration's mentality. An integrated police force is necessary to fully implement the provisions of this Act.⁶⁴

Prevention of Cyber Crime

Better to prevent than to treat. When using the internet, it's wise to follow a few safety measures.

A citizen should keep in mind the following things:

1. To stay safe from cyber stalking, it's best to keep your personal information private. This is the same as going public with your identity.
2. There have been cases of people misusing photos shared online, therefore it's best to be cautious when sending photos to strangers or chat buddies.
3. Protect yourself from malware attacks by always using the latest and updated antivirus software.
4. Back up volumes should always be kept to avoid data loss in the event of a virus infection.
5. In order to prevent fraud, you should never provide your credit card information to an unprotected website.
6. You should constantly monitor the websites your children visit to protect them from any form of abuse or inappropriate content.
7. Because leaving cookies unprotected could be disastrous, it is recommended to use a security application that allows control over cookies and sends information back to the site.
8. Website owners should watch traffic and check any irregularity on the site. Putting host based intrusion detection devices on servers may do this.
9. Use of fire walls may be beneficial.

⁶⁴ www.navvi.com

10. It is imperative that web servers hosting public websites are physically isolated and safeguarded from the internal network of the company.

No piece of legislation has ever been able to eradicate crime entirely from the face of the earth, as history attests. Raising public awareness of their rights and responsibilities (including the communal need to report crime) and enforcing stricter legal penalties are the only viable options for reducing crime. The Act is undeniably a watershed moment in cyber history. Moreover, it is undeniable that the Information Technology Act needs updating in order to better tackle cyber crime. Last but not least, I have a word of warning for the pro-legislation camp: make sure the cyber law's requirements aren't so onerous that they stifle industry growth and end up hurting everyone.

2.3 HOW TO ERADICATE CYBER-CRIME

No legislation has been able to successfully banish the plague of cyber crime, according to the research. There have been efforts on a global and national scale, but these laws are not without their flaws. The elements that make a crime Because laws that apply in one nation might not apply in another, it has long been easy for cyber criminals to evade punishment.

Governments should combat idealists through education, not legislation, despite these hurdles. There is evidence that they assist governments and large corporations in identifying security flaws that would make them vulnerable to attacks by cyber criminals or even terrorists. Companies often hire them as consultants to assist in establishing robust security measures for their systems and data. "Idealists frequently contribute to society: by their highly publicized and personally innocuous acts, they assist major organizations in uncovering their technological security vulnerabilities..." Because they would refuse to comply and instead seek ways to disobey the law, imposing it on them is sure to produce problems. "Furthermore, if the objective of cyber crime laws is to eliminate cyber crime, it may as well eliminate an entirely new manner of life..." A far more effective strategy for preventing such behaviors would be to invest in education.

For cyber-terrorists and those driven by greed, harmonising international law and law is another way to eradicate cyber crime. As long as people continue to commit crimes, education will not be able to change their behaviour. To combat them, new laws must be passed, existing laws must be harmonized, and national law enforcement agencies must be encouraged to work together.

2.4 WHO ARE INVOLVED

Those involved in committing cyber crimes are in three categories and they are :

The Idealists (Teenager). They are usually not highly trained or skilful, but youngsters between the ages of 13-26 who seek social recognition. They want to be in the spotlight of the media. Their actions are globally damageable but individually negligible. “Like denying a lot of important e-commerce servers in February, 2000 is said to have caused high damages to these companies. ”Most often they attacks by stems with viruses they created; their actual harm to each individual is relatively negligible.⁶⁵

By the age of 26 when they have matured and understood the weight of their actions, they lose interest and stop.

The Greed– Motivated (Career Criminals).

This type of cyber criminals are dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings money to them. “They started the child pornography often called cyber pornography which encloses legal and illegal pornography on the internet. They are usually very smart and organized and they know how to escape the law enforcement agencies. These cyber criminals are committing grievous crimes and damages and their unscrupulousness, particularly in child- pornography and cyber gambling is a serious threat to the society. Example to show how serious a threat they pose to the society is “the victim of the European bank of Antigua are said to have lost more than \$10 million” “...theft of valuable trade secrets: the hackers could use the code to break all firewalls and penetrated remotely every

⁶⁵ Surabhi Sharma, “Cyber Bullying and Online Harassment: A Study”, Journal of Digital Law, Vol. 12, Issue 1, 2023.

computer equipped with windows were confirmed. Another usage could be the selling of the code to competitors.”

The Cyber– Terrorists

They are the newest and most dangerous group. Their primary motive is a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. The threat of cyber- terrorism can be compared to those of nuclear, bacteriological or chemical weapon threats. This disheartening issue is that they have no state frontiers; can operate from anywhere in the world, and this makes it difficult for them to get caught. The most wanted cyber- terrorist is Osama Bin Laden who is said to “use steganography to hide secret messages within pictures, example, a picture of Aishwarya Rai hosted on the website could contain a hidden message to blow up a building.” A surprising fact is that these hidden messages do not alter the shape, size or look of the original pictures in any way.

2.5 CYBER CRIME

Cyber Crime can be regarded as computer mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by new Information and communication technologies. The Global connectivity of internet, for example, make it much easier for criminals to act beyond National boundaries to conduct their illegal affairs. It also make it possible for existing organized crime to use more sophisticated techniques to support and develop networks for drug trafficking, money laundering, illegal arms trafficking, smuggling and other. For hackers with the requisite computer skills, large a market exists for security and trade secrets which can be accessed and transmitted electronically. Furthermore, the many-to-many communication which is essential feature of internet enables the

production and worldwide dissemination of information and knowledge which could be potentially harmful, threatening or liable to incite violence⁶⁶.

Any person and every computer user should know what 40 Cyber Crime entails. The term cyber or signify. All that pertains to computers, internet, websites, data, emails, networks, software, data storage devices and even electronic device like cell phones. ATM machines etc. In the first case where man reversed the letters computer and in the second case where he reversed the letters technology in the communication between computers, he would never have imagined that the cyber space that he is creating can be submerged with any type of crime that is a cyber crime. However today almost everyone may have heard the term computer crime, cyber crime, e-crime, hi-tech crime or electronic crime which is nothing other than a criminal activity carried out with a criminal motive in the cyber space. Cyber Crime is simply an activity that is criminal in nature and where a computer or a network is the source, tool, target or place of a crime, Cyber Crime is all the activities that are performed in a cyber space with criminal intention.

“Cyber computer and information era. Translated as kybernetes, the Greek term translated as Words such as steersman, governor were first used in the context of cybernetics by Norbert Wiener and others. The regulations governing the online world are referred to as cyber laws and all people using the internet are known as netizens of this space due to the universal jurisdiction that these laws have. The other definition of cyber law is as the law that deals with concerns of lawlessness that may come about due to the utilization of computer systems which form larger computer networks. In short, of law that concerns itself with computer and internet issues.

A robust and efficient regulatory framework is required to further fortify the legal framework, which is essential to the expansion of electronic commerce. Cyber law encompasses all of these systems of regulation and legal

⁶⁶ The Role of Blockchain in Cyber Security, IEEE Research Paper, 2021.

frameworks.⁶⁷ The contemporary world has completely delegated all of its operations to the cyber sphere. Because of how ingrained cyber space has grown in our daily lives, before. The recent Face book data scandal online lives have become. As one delves farther into the online realm, more and more dangers emerge.

“The modern thief is more effective with a laptop and the internet than a of the future will have firearm. It is possible that terrorists greater success using a computer than a bomb.” Cyber crime damage costs to hit \$6 trillion annually by 2022. Every 40 seconds a business falls victim to a ransom ware attack. Cyber security Ventures predicts that will rise to every 14 seconds by 2021.

Crimes that are perpetrated using computers cyber crimes or computer oriented crimes. Either the crime was done on the computer or it was the victim. The victim directly or indirectly, through the use of modern telecommunication networks like the internet (networks including but not limited to Chat rooms, emails, notice boards and groups) is the definition of a cyber crime the victim the victim to have his/her reputation, physical or mental harm. Online crime can pose a threat to the safety or the economic wellbeing of an individual or a country

2.6 DEMAND OF CYBER LAW

Traditional crime is conducted with the help of computers or Internet is used as a means of crime and bear in mind cases of disseminating pornographic content, criminal threats through email or web sites which slander someone or other racial hatred etc. in each of these scenarios, the computer is just a coincidental part of crime. The handing out of pamphlets that advance racial hatred is, in essence, analogous to installing a web site that fosters the ill feelings. When such crimes are conducted through technology, the impact and propagation of the crime goes extremely high. Posting of pamphlets, even in a single locality, is a time consuming and costly process whereas it is very cheap to install a globally accessible site.

⁶⁷ “Cyber Crime Awareness and Prevention Strategies”, Research Paper, Banaras Hindu University, 2023.

In this instance it is arguable that traditional law is capable of dealing with cyber cases. The Government may easily provide a more stringent liability (through imprisonment and fines) in case the crime is executed with the aid of specific 42 technologies. An oversimplified version would be to say that the distribution of pornography through electronic medium should be subject to greater penalties than the distribution of pornography through traditional medium.⁶⁸ conventional law would suffice as long as we are concerned with such issues. The difficulties arise when we consider more complicated questions as the theft of data. In the traditional law, it relates to the movable property that has been removed out of the possession by someone. “Property of every description, bar immovable property” is how the General Clauses Act describes movable property.

“Land, benefits to happen out of land, and things related to the earth, or fixed to anything attached to the earth” are the elements that are defined as immovable property under the same statute. According to these criteria, the computer qualifies as personal property.

Let us examine how such a law would apply to a scenario where data is ‘stolen’. Consider my personal computer on which I have stored some information. Let us presume that some unauthorized person picks up my computer and takes it away without my permission. Has he committed theft? The elements to consider are whether some movable property has been taken out of the possession of someone. The computer is a movable property and I am the legal owner entitled to possess it. The thief has dishonestly taken this movable property out of my possession. It is theft.

Now consider that some unauthorized person simply copies the data from my computer onto his pen drive. Would this be theft? Presuming that the intangible data is movable property, the concept of theft would still not apply as the possession of the data has not been taken from me. I still have the ‘original’ data on the computer under my control. The ‘thief’ simply has a ‘copy’ of that

⁶⁸ Prashant Mali, “Cyber Law and Cyber Crimes in India”, Snow White Publications, 2021.

data. In the digital world, the copy and the original are indistinguishable in almost every case.

Consider another illustration on the issue of ‘possession’ of data. I use the email account rohitjain@gmail.com for personal communication. Naturally a lot of emails, images, documents etc. are sent and received by me using this account. The first question is, who ‘possess’ this e-mail account? Is it me because I have the username and password needed to ‘login’ and view the emails or it is Google, because the emails are stored on their computers.

If some unauthorized person obtains my password. Can it be said that now that person is also in possession of my emails, because he has the password to ‘login’ and view the emails.⁶⁹

With the advent of technology in the society, a lot of problems have been tabled about the integrity, safety of the cyber space, information, privacy, about the rights of intellectual property, electronic transaction etc. As the main source of cyber law, there are a lot of issues that technology Act, 2000 is addressing in its use and abuse. The research and development on the aspect of cyber security is also of utmost significance nowadays and the need of the day. Due to these and other intricacies, the traditional law fails to address the matter of the cyber space. This introduces the requirement of a specific subdivision of law that will address cyber crime and cyber space.⁷⁰

2.7 CYBER CRIMINAL

Cyber criminals, also known as hackers, often use computer systems to gain access to business trade secrets and personal information for malicious and exploitive purposes. Hackers are extremely difficult to identify on both an individual and group level due to their various security measures, such as proxies and anonymity networks, which distort and protect their identity. Cyber security experts assert that cyber criminals are using more ruthless methods to achieve their objectives and the proficiency of attacks is expected to advance as they

⁶⁹ Ministry of Electronics and Information Technology, “National Cyber Security Policy”, 2020.

⁷⁰ “Emerging Threats in Cyber Crime and Digital Safety”, Cyber Peace Foundation Report, 2022.

continue to develop new methods for cyber attacks. The growth of the global cybercriminal network, which is largely credited to the increased opportunity for financial incentives, has created a number of different types of cyber criminals, many of which pose a major threat to governments and corporations. A person who commits a cyber crime or helps other in committing cyber crime is a cybercriminal.

There are three basic categories in which we can categories cyber criminals-

1. Hackers and phreaks.
2. Information merchants and mercenaries.
3. Identity thieves and internet talkers.
4. Phishing scammers.
5. Terrorists, extremists and deviants.

The information age touches not only our businesses and our private lives, but also the national infrastructure and economics. If hackers can penetrate computer systems within universities and businesses, then why not banking system, air traffic control, railway switching system, television and radio and this need not be performed merely for fun or in an extortion attempt—it can instead from a key part of a coordinated and well integrated offensive, it can form an element of cyber war.

More than this instead of seeking to damage it, the computer infrastructure and capabilities of the information age can be used by the criminals or terrorists directly to assists in the laundering of money, to hide illegally imported software or digitized pornography or even to disseminate carefully framed propaganda and disinformation. From the perspective of the hacker, thief or terrorist, digital crimes therefore involve using computers to assist in illegal activities, subverting security within computer system, or using the global internet or banking networks in an illicit or misleading manner.

And finally, although much of the value of a computer system comes from the information it holds, the physical components themselves can also command criminal attention. In particular, the theft of memory and processor chips from

computers, or even from the manufacturing plants themselves, has become widespread. This might not be seen as a ‘high– tech’ crime to stand alongside hacking and money laundering but it is none the less an important and distinctive feature of the information age– a crime resulting from the cybernation dependence upon digital technology.⁷¹

2.8 STAGES OF CYBER CRIME

Deliberation, planning, effort and action. Just like this, there are also phases of commission of a cyber crime. These stages are as under-

1. Planning : Most of cyber crimes are not spontaneously done but carefully planned often for extensive periods. For this purpose, the criminal acquires certain information such as data entry practices, program listings, systems

2. Documentation : locations of the system data and other systems details in addition to the controls on system access and system security procedures. Execution: Execution of computer crimes differs from execution of other crimes. The presence of the perpetrators is not necessary for the computer crime to be committed, There are different methods for commission of computer crimes such as using terminals or communication channels to gain access, modifying transaction to an input file, physical removal of programs or data, accessing controlled information and copying the same, physical action such as arson or theft and manipulating the actions of programs or people.

3. Concealment : Once the crime has been committed, the tendency of the criminal is to remove traces of crimes. There are several ways to hide the crime including representing the crime as an error or omission in an otherwise normal run, representing a fraudulent transaction as a normal transaction being executed, modifying an individual account but manipulating the system totals to reflect normal result, misrepresenting a criminal activity as an error of flow within a system and performing the illegal act in conjunction with an authorized activity⁷².

⁷¹ “Impact of Cyber Crime on Digital Economy”, NITI Aayog Report, 2021.

⁷² Indian Evidence Act, 1872 – Amendments related to Digital Evidence.

4. Conversion: Once the crime has been committed, the immediate problem for the criminal is take forms such as sale of data unauthorized cases of revenge, or in most of the cases financial gain.

2.9 CYBER & E- COMMERCE

The word commerce refers to buying, selling, trading, advertising and transactions of all kinds that lead to an exchange of value between two parties like banking and other financial service, sales of software, consumers goods and services. E commerce is a new way of conducting, managing and executing business transactions using computer and telecommunication networks. It is the international character of E commerce with borderless medium and not targeted to a specific geographic market. Commercial websites can provide even a small business with access to markets and internet user worldwide. E-commerce is changing linear view of supply chain. Instead of goods flowing from one participant to the next, this new online marketplace can connect each participant with the customer.

The Electronic Commerce Act would support the establishment of sound regulatory framework in electronic commerce by offering a regulatory framework in the legal context that governs electronic contracting, security and integrity of electronic transactions, the application of digital signature and other matters concerning electronic commerce. Contractual issues, computer crime and data protection are covered in the information technology act. It has also a section covering digital signatures. The E commerce will have an influence on intellectual property rights, patents on business methods and virtual distribution of film, music and other pictures. Electronic Commerce Support Act is aimed at modifying several examples of Central Acts.

1860, 1872, the Contract Act, the Indian Penal Code, 1860. 1872, the Indian Telegraph Act, 1885. The Banker books India act, 1891, the general clauses act, 1897, the act of reserve bank of India, 1934 so as to facilitate electronic commerce.

2.10 CONCEPTUAL ANALYSIS OF CYBER CRIME

Numerous forms of cyber crime exist, as previously stated. While cyber criminals may seek payment in a variety of ways, the majority of cyber crimes have a financial motive. The following are examples of particular forms of cyber crime:

Cyber extortion: A crime where the perpetrator demands money to halt an attack or threats of an attack. The use of ransom ware is an example of cyber extortion. In this scenario, a hacker breaches a company's defenses and encrypts all of the company's documents and files (or anything else that could be valuable) until the owner pays a ransom. Most of the time, this takes the form of crypto currency like Bit coin.

Crypto jacking: A kind of malicious scripting that secretly mines crypto currency in users' browsers. Installing bit coin mining software on the victim's system is one method of crypto jacking assaults. Yet numerous assaults rely on in-browser mining JavaScript code when the user's browser is open with the malicious site in a tab or window. Because the in-browser mine code is executed at page load, no virus installation is necessary.

Identity theft: An assault that happens when someone gains access to a computer and steals personal information from users. This information can be used to commit identity theft or get access to valuable accounts like banking and credit cards. On dark net marketplaces, cyber criminals provide a variety of accounts, including bank ones, streaming video services, webmail, audio streaming, online auctions, and more. Another common type of personal information that identity thieves target is health records.

Credit card fraud: An intrusion attack happens when cyber criminals gain access to a retailer's computer systems with the intent of stealing consumers' financial information. Hacking groups that have obtained a large number of credit cards can make a profit by selling them on dark net markets. Lower-level cyber criminals can then use these stolen cards to commit credit card fraud versus individual accounts.

Cyber espionage: Cyber crime occurs when an intruder gains access to protected data stored by a government agency or other legitimate business through a computer network. Attacks might be driven by ideological or financial motives. Cyber espionage encompasses a wide range of tactics, including hacking into computer systems to steal, alter, or destroy data, eavesdropping on communications via email, text, or instant messaging, and the use of network-connected devices to spy on specific individuals or groups.

Software piracy: An assault that targets software programs through their illegal copying, distribution, and use, whether for personal or commercial gain. This sort of cyber crime is frequently linked to trademark, copyright, and patent infringements.

Exit scam: As expected, the dark web has given birth to the digital incarnation of a long standing crime called the exit scam. What we see now as administrators of the dark web effectively engage in the theft of virtual currency from other criminals by transferring it from marketplace escrow funds to their own identities.

Examples of Cyber crime

Distributed denial of service (DDoS) assaults are among the most prevalent forms of cyber crime; they aim to disable systems and networks. By flooding a network with connection requests, this attack type turns its own communications protocol against it. While distributed denial of service (DDoS) assaults can be orchestrated for nefarious purposes or as a cyber extortion scheme, they can also be employed to divert the victim organization's attention from other concurrent attacks or exploits. An example of an attack that damages the system or harms people is infecting networks and systems with malware. One way to achieve this is to corrupt the system, its software, or the data it stores. Similar assaults can occur with ransom ware, which encrypts or disables victim systems until a ransom is paid. Cyber criminals target business networks with phishing attacks. One method is to send phishing emails to business users in the

hopes that they'll open attachments or click on links, which will infect their computers and eventually the networks of their employers.

When hackers try to get access to a victim's system or personal accounts by stealing or guessing their user IDs and passwords, they are committing a credential attack. Installing key logger software or taking advantage of software or hardware flaws that reveal the victim's credentials are two ways brute-force assaults can be carried out. In addition, hackers may try to take over a website in order to alter or remove content or gain unauthorized access to databases. Attackers can gain unauthorized access to sensitive information and data, including customer passwords, credit card numbers, personally identifiable information (PII), trade secrets, and intellectual property (IP), for instance, by inserting malicious code into a website through a Structured Query Language (SQL) injection exploit. This code can then be utilized to exploit vulnerabilities in the website's database. Cyber crime also frequently includes illicit gambling; illegally procuring, manufacturing, owning, or disseminating child pornography; and selling illicit products such as firearms, narcotics, or counterfeit goods.

2.11 CYBER SPACE AND CYBER WORLD

Cyber space or cyber world is a world dominated by electronic appliances with only optical fibers, digital signals, data, and bytes among others possibly being considered. It is a place of virtuosity in which you cannot see so much; and so much you can see but not feel. It is a fantasy world unlike the one that we live in. It is an imaginary world that has highly charged the real world. It possesses great potential and limitless possibilities to man to an extent that man is now obsessed with living in this electronic world. He attempts to seek, and entertains a belief that he is certain to possess what he could not have even imagined in the real world. Therefore his interest and attraction towards this is increasing with every moment his life encounters.

It has been described in many ways as a sphere in which electronics and the electromagnetic spectrum are used to store, modify and exchange data using networked systems and related physical infrastructures; or the electronic medium

of computer networks, in which online communication occurs or the data stored in a large computer or network expressed as a three dimensional model in which a user of virtual-reality can navigate; or the national landscape in which digitized information is communicated on computer networks; or a computer network comprising of a global system of computer networks that utilize the TCP/IP network protocols to facilitate the transmission and exchange.

The world cyber space is believed to have been coined by author William Gibson in his sci-fi novel 'Necromancer', written in 1984. Gibson visualized the cyber space in these words.

“A consensual hallucination experienced daily by billions of legitimate operations, in every nation, by children being taught mathematical concepts....A graphical re presentation of data abstracted from the banks of every computer in the human system. Unthinkable complexity, lines of light ranged in the non-space of the mind, clusters and constellations of data.”

Cyber world is a word that is closely related and almost similar to Cyber space, and it refers to the world of computer savvy people, net surfers and so on. So is another word Cyberia. Cyber world has been broadly defined as

- (i) transact any business or personal activity as naturally and freely as they can transact them in the real world; or
- (ii) an online sophisticated computing environment; or the futuristic online world of computing.

CHAPTER–III

CYBER LAWS IN INDIANS CENARIO

3.1 COMPUTER AND INTERNET

The Computer is coined after a Latin word, Computer, which means to calculate or to count, to add up or to think together. Computer is therefore strictly speaking defined as a computing device. It is an electronic machine that holds the memory of the information with the input devices and manipulates the information to create output as per the instructions given. Internet refers to an interconnected formation that constitute the computer network in the world, and which offers diverse data and communication services. The internet as a whole can be referred to as the Net. An enormous web of interlinked computer systems. A computer is a machine that may be programmed to execute series of arithmetic or logical actions automatically through computer programming. The contemporary computers can execute generalized sets of operations known as computer programs. These programs allow the computers to do and will so many tasks, which were extremely wide⁷³.

Net is a global system of interconnected computer networks. It is based on TCP/IP to connect devices across the globe. Internet Protocol suite is TCP/IP. It is a network of networks. There are private, public, academic business and government networks, which comprise Internet. One of these networks is of local to global scope. These are connected through a wide range of electronic, wireless and optical networking technologies. It is the Internet that carries with it an enormous amount of information resources and services including the inter linked hypertext documents and applications of the world wide web (www), electronic mail, telephony, file sharing etc.⁷⁴

Computer is an electronic machine that adheres to a program to execute sequentially information and mathematical and logical operations. Internet refers

⁷³ Information Technology Act, 2000 (As Amended In 2008), Government of India. (section 43, 65, 66, 66a, 66c, 66d, 66e, 66f, 67, 69 Etc.)

⁷⁴ Indian Penal Code, 1860 – Sections Related To Cyber Crime (Sections 66a, 66c, 66d, Etc.).

to a global network of computers or computerized gadget and servers. The company that offers Internet facility to the users is known as Internet service provider.⁷⁵

Computers and the internet represent one of the biggest technological advances of 21st century which is beneficial to the users and provides the opportunities to them in the fields of education, employment, business, career advancement, personality development, knowledge sharing, effective communication and like that. We use the computers and Internet in our daily life frequently⁷⁶.

There are certain advantages and disadvantages of computer and Internet. These advantages and disadvantages can be summarized in brief as discussed below.⁷⁷

Advantages

Computer and the Internet enable us to store huge amounts of data safely and securely. The hard devices on computers and the virtual storage facilities on the internet provide data storage facilities. Such stored data can be accessed at any time as per our need and convenience. Computers and the Internet facilitate us to stay in touch with the people all over the world. Staying in touch with the people all over the world of e- mail, social media, video conference, video chatting etc.

Computers and the Internet facilitate us to update all of the world's knowledge and to stay informed. Computers and the internet are helpful and useful to obtain information and knowledge for research purpose also:

- Use of computers and the internet is beneficial and essential for study purpose from school level.

⁷⁵ Pavan Duggal, *Cyber Law In India*, Universal Law Publishing, 2019.

⁷⁶ Ministry Of Electronics And Information Technology (Meity), "National Cyber Security Policy, 2013".

⁷⁷ Justice K.S. Puttaswamy (Retd.) V. Union Of India AIR 2017 10 Scc 1 – Right To Privacy And Its Cyber Law Implications.

- Use of computers and the Internet serve a purpose of enhancement of our creativity and personally development e.g. painting programs, music editing software etc.
- Computers and the Internet provides an opportunity of sharing our ideas with the people all over the world through a writing of blogs, writing of articles, research papers, essays etc. and uploading the same.
- The Internet news is updated more quickly than printed newspapers are. Thus, the use of the computers and the Internet serves a purpose of staying informed about the current events.
- The use of the computers and the Internet serves the purpose of speeding up calculations.
- They are useful for staying organized through the maintenance of files organized.
- Use of computers and Internets facilitates us to get the means of relaxation and winding down. e.g. watching of DVD, favorite radio show etc

Disadvantage

- It skills are tricky to learn. It results into a waste of time for some people as it becomes too hard and difficult for them to become computer literature.
- A simple power cut or lack of internet supply can spell disaster for your day if you rely on computers and internet without cultivating traditional skills like the maintenance of handwritten accounts or use of library rather than on- line etc.
- The Internet is considered to keep us in touch with other people. But to remain busy with computers and the Internet may result in isolation.⁷⁸
- Excessive use of computers and the internet results in eye strain.
- Use of computers for a long period can lead to painful condition and can damage our posture.
- It may hamper our routine work.

⁷⁸ Shreya Singhal V. Union Of India (AIR2015 SC1523) – Striking Down of Section 66a of It Act.

- Excessive use of computers and the Internet results into the loss of traditional skills and arts. e.g. when we spend all our time typing e-mails, we may loss a skill to write a beautiful handwritten letter.⁷⁹
- It is very difficult to judge and verify the quality on the Internet

Use of the Internet

Some of the important uses of the Internet are-

1. On-line Communication

The use of e-mail service on the Internet is extensively applied by computer users worldwide in a bid to communicate with one another. Chat is also a facility that is used by many users of the platform to communicate with one another in real-time. As an illustration, webmessengeryahoo.com and facebook.com Internet sites offer chat possibility. The e-mail facilities and chat, tool for millions of users.⁸⁰

2. Software Sharing

The Internet provides access to a large number of shareware software, development tools, and utilities. For example, Free Software Foundation provides a wealth of GNU software tools on the Internet, which a user can download free of charge. For more details on software tools offered by Free Software Foundation, you can anonymous to the Internet siteprep.at.mit.edu, and look in the directory /pub/GNU. The Internet sites filehippo.com andisohunt.com also offer free downloadable software.⁸¹

3. Exchange of views on topics of common interest

The Internet has a number of news groups. Each news group enables a group of users to exchange their views on some topic of common interest. For

⁷⁹ Rohit Bansal, "Cyber Laws And Their Implementation In India", *Journal Of Cyber Security Studies*, Vol. 9, No. 2, 2022.

⁸⁰ Indian Evidence Act, 1872 – Amendments Related To Electronic Evidence (Sections 65a & 65b).

⁸¹ "The Role Of Data Protection Laws In India", Niti Aayog Report, 2023

example, the news group Search Win/T.com contains views of Microsoft Windows administrators and computing managers.⁸²

4. Posting of information of general interest

The Internet is like a huge electronic bulletin board and many users post on the Internet general information they are interested in to attract the attention of the interested users worldwide. Part of such information involves career opportunities conference and event announcements and conference and journals calls. E.g., such web site as erodov.com is a technology news site and technology review.⁸³

5. Organization Promotion

The modern world has seen a majority of organizations producing their own web sites to spread timely information about related corporate events, products announcement, new strategic alliance, press reports and other information that may be of interest to all those involved.⁸⁴

6. Product promotion and feedback about products

The commercial organizations also utilize the Internet to market their products/service and in this case to receive information on how their existing products are satisfying the user and the market potential of the new products and also some ideas on how a new product can be created. An organization achieves this through posting information on its web site regarding its products/services provided and an interactive survey application on its web site.⁸⁵

7. Customer support service

Many organizations also use the internet to provide timely customer support. The combined e-mail, ftp, and other services on the Internet provide necessary enabling tools for such first-rate customer support. For example, users of a software product can report bugs in the software to the organization that

⁸² Justice B.N. Srikrishna Committee Report On Data Protection, 2018.

⁸³ Personal Data Protection Bill, 2019 (Now Replaced By The Digital Personal Data Protection Act, 2023).

⁸⁴ Digital Personal Data Protection Act, 2023, Government of India.

⁸⁵ Reserve Bank Of India, "Guidelines On Digital Payment Security, 2022".

owns the software by e-mail, and the organization can make available to its customers bug fixes, minor releases, workarounds, known problems and limitations, and general advice about the product via an ftp server.⁸⁶

8. On-line Journals, Magazines, Encyclopedia and Dictionary

Electronic subscriptions on the Internet are currently available in literally thousands, both free and low-priced. The Internet has a great number of WWW sources devoted to electronic copies of numerous journals and magazines. Also available are sites, where one has access to electronic encyclopedia and/or dictionary. The Internet version of Times of India newspaper can be found at the Internet site, coined timesofindia.com. On line encyclopedia are available in the site Wikipedia.org and a non-line dictionary in the sitewikitionary.org.⁸⁷

Researchers have extended this idea to support full-fledged electronic libraries (called digital library) on the Internet.

9. On-line Shopping

The Internet has made it easy to introduce a new market concept which entails virtual shops. These outlets are 24 hours all year round and are 18 reachable by buyers across the globe. sale of products or services via WWW servers. 6 services, customers make certain product requests and demand certain sales quotes. With a clearly defined authorization and authentication application, the virtual shops will, via the Internet services, receive orders made by the customers, process order payment and order tracking to completion. Indicatively, the Internet store amazon.com is one such virtual bookstore on the Internet, which has details about all kinds of International books and CDs and takes orders of the same on-line.⁸⁸

⁸⁶ Supreme Court Of India, "Anvar P.V. V. P.K. Basheer", Air 2014 Sc 2686 – Admissibility of Electronic Records.

⁸⁷ Cert-In (Indian Computer Emergency Response Team) "Cyber Security Guidelines, 2022".

⁸⁸ Google India V. State Of Uttarakhand" AIR 2020 U H Intermediary Liability in IT Act.

10. Worldwide video conferencing

Internet-based video-conferencing enables a team of users to communicate and interact with one another in a part of the world, as though they were sitting in the same room and arguing. The communicating parties can view each other speaking on the computer screen and understand the voice of the other party using a special audio- device installed in their computers.

11. Worldwide webcasting

In the contemporary world, there are numerous organizations which distribute a single through the Internet. video information to a large number of simultaneous listeners or viewers across the globe. The process of broadcasting of such content via the use of the Internet/ is called- web casting. A web casting software transmits to a large number of simultaneous listeners or viewers a media file which contains audio or video information over the Internet. It does it using streaming media technology. A web casting software can be used to distribute a media file on-demand or live. Web casting E-learning program involves lecturing or seminars to a group of interested people with global participation.. Webinar is a new terminology, which refers to webcasting of a seminar Politicians use web casting to deliver talks to a wider audience. Commercial organizations use web casting to make corporate presentations or announcements of their new products and services to their existing and prospective customers located worldwide. Virtually all major broadcasters have web cast of their output including BBC, CNN, and UNTV.ezwebpresentation.com offers web casting services.

12. Internet Search Engines–

An Internet search engine is an application, which helps users locate websites containing useful information and reference to such information on the WWW. To search information on the WWW, a use types the description of the information using the user interface of the search engine. The search engine then searches the requested; information on the WWW and returns the results to the

user. The results enable the user to locate the requested information quickly from the vast ocean of information available on the internet.⁸⁹

Major Elements of Internet Search Engines—

Three major elements of an Internet search engine are as follows:

1. Search request interface— Enables users to provide description of desired information to the search engine. Depending on the complexity of this element, the search engine may allow specifications of simple keywords and phrases, combination of keywords and phrases using Boolean operators and exclusion/inclusion operators, and the title and URL limiters.⁹⁰

2. Information discoverer— discovers information from the WWW and creates a database for the search engine. The search engine uses the database to locate useful information during the search process. Information discoverer accrues this information in two ways : (a) in manual method, provide information about their websites to the search engine; (b) in automatic method, information discoverer collects the information using programs, such as web crawlers, spiders, robots. These programs, periodically roam on the Internet, and store links of information about each page they-visit along with their associated hyperlinks. Information discoverer then creates an index from the results of automated search. If a web page owner updates his/her/its web page, the spider finds these changes and updates its index.

3. Presenter of search— Results returns search results, ranking them in an order it believes, is most relevant to the search. Search engines often list search results in accordance to a relevance score.⁹¹ Relevance scores reflect the number of times a search term appears in a web page.

Some Popular Internet Search Engines— Today, there are more than two dozen major search engines available on the WWW. Some popular ones are:

⁸⁹ Meghna Bal, "Intermediary Guidelines And Cyber Censorship In India", *Economic & Political Weekly*, 2022.

⁹⁰ "Dark Web And Cyber Law Challenges In India", Centre For Internet And Society Report, 2023.

⁹¹ Cyber Appellate Tribunal – Functioning And Role In Cyber Disputes In India.

1. Users HotBot (www.hotbot.com)
2. Yahoo(www.yahoo.com)
3. Lycos(www.lycos.com)
4. Infoseek (www.infoseek.com)
5. Google(www.google.com)
6. Inference Find (www.infind.com)
7. Ixquick (www.ixquick.com)

4. The Internet and On-line Resources–

In general, web pages and documents on the Internet provide useful information. While on on-line resource is typically data and educational in nature, any support software available on-line can also be considered a resource.

The World Wide Web (WWW)–

The World Wide Web (called WWW or W3 in short) is the most popular and promising method of organizing and accessing information on the Internet. Main reason for its popularity is use of a concept called hypertext. Hypertext is a new way of information storage and retrieval that enables authors to structure information in novel ways. A properly designed hypertext document can help users locate desired type of information rapidly from vast amount of information on the Internet. Hypertext documents enable this by using a series of links. Different systems show a link on screen in different ways such as a labeled button, highlighted text than different color text than normal text, or author-defined graphic symbols. A link is a special type of item in a hypertext document connecting the document to another document that provides more linked item. The latter document can be anywhere on the Internet (in the same document in which the linked item is, on the same computer in which the former document is, or on another computer at the other end of the world). By ‘connect’ we mean that

a user simply selects the linked item (using a mouse or key command) and sees the other document on his/her computer terminal almost immediately.⁹²

WWW Browsers–

To use a computer as a web client, a user needs to load on it a special software tool known as WWW browser (or browser in short). Normally, browsers provide following navigation facilities to help users save time while. Internet surfing (process of navigating the Internet to search for useful information):

1. Unlike FTP and Telnet, browsers do not require a user to log into a server computer remotely, and then to log out again when the user finishes accessing information on server computer.
2. Browsers enable a user to visit a server computer's site directly and access information on it by specifying its URL (Uniform Resource Locator) address. URL is an addressing scheme, which WWW browsers use to locate sites on the Internet.
3. Browsers enable a user to create and maintain a personal hotlist of favorite URL addresses of server computers that the user is likely to visit in future frequently. A user's hotlist commands to enable a user to add, delete, update URL addresses in hotlist, and to select an URL address of a server computer from hotlist, when the user wants to visit the server computer⁹³.
4. Many browsers have a 'history' feature. These browsers maintain a history of server computers visited by a user in a surfing session. That is, they save (cache) in the user's local computer's memory, the URL addresses of Server computers visited by him/her during a surfing session, so that if the user wants to go back to an already visited server later on (in the same surfing session), the link is still available in local computer's memory.⁹⁴

⁹² "Impact Of Artificial Intelligence On Cyber Laws", Research Paper, 2022.

⁹³ Rachna Gupta, "Cyber Law Enforcement In India: Issues And Challenges", *International Journal Of Law & Technology*, 2022.

⁹⁴ "Nazir Ahmad V. King Emperor" AIR 1936 – Importance Of Best Evidence Rule In Cyber Cases.

5. Browsers enable a user to download (copy from a server computer to local computer's hard disk) information in various formats (i.e., as a text file, as an HTML file, or as a PostScript file). The user can use the downloaded information later (not necessarily in the same surfing session). For example, the user can later print downloaded information saved as PostScript file on a PostScript-compatible printer, which can reproduce even graphics properly.

Computer Industry Development.

Be ginned with the history of First Generation Computers which was developed in the 1940s. The transistors and integrated circuit of 1950s contain some resistors, transistors and diodes among other things packed on a silicon chip. It was in the year 1970s that the conversion of integrated circuit to the VLSI technology became possible. Even smaller silicon chips were incorporated using VLSI technology making them more powerful. Accordingly, evolution of second, third and fourth generation of the computers has occurred between 1950 to 1970.

We are currently at the fifth generation of computing technology. The fifth generation computers can perform the work of the human beings. It has been made possible through occurrence of artificial intelligence methods. The use of computers as well as the use of robots has become very common nowadays and it is found everywhere. Between 1940 and 1960, computers were limited to research departments of the limited number of Universities and military bases. These computers were extremely cumbersome to manage and Operate because they were hand made, hand wired and made of valves. These computers could only perform mathematical calculations. The new advancement of the computer technology in 1960 was in the development of the integrated circuits. The new development went on with the development of VLSI in 1970s and artificial intelligence technique. Industries began spending increasing amount of money to conduct more research and development on the field of computer programming

and development of facilities within the field. appropriate in their application in industries. Computer Industry further developed minicomputers.⁹⁵

The mode in seventies was to buy as large as possible. machines possible and to make as much work on it as possible. The current trend however is to acquire smaller computer of higher efficiency and flexibility in its operation. These consumer tastes witnessed the introduction of microcomputer industry which began to provide personal computers (PCs) in 1980. The much needed small size computers, occupying desk top, and having higher efficiency, to be useful in the business world. It completely transformed the computer industry and the new technology was easy and attractive to everyone. The machines did not require any special knowledge operating and with a little training, a layman would be able to operate the machine.

The other breakthrough in the history of computer technology occurred in the year 1950 when computers which were programmable and general purpose were introduced. The industry was not a booming one as initially, it was commercially not viable to invest in this industry. A single all-inclusive price would also be provided on the software by the hardware industry. This bundling encouraged the non-hardware firms not to venture into the software market because the company that may want to buy a hardware product had to pay the price required to acquire its software whether it was good or not effective. Many customers could easily find out more efficient software. As they had already paid the hardware retailer full bundle price.

It was not commercially advisable for them to purchase software to perform the same functions. The practice of bundling greatly stifled the growth of software industry. The few soft ware houses that had come into existence pressed hard against the bundling practice as it amounted to tying arrangement prohibited by the Anti Trust laws. IBM, being well established and large in size, was made a target. This tirade started during the late 1950, and early 1960s. In view of the rising opposition to bundling practice, IBM decided in mid 1960 to

⁹⁵(Data Security Council of India (Dsci), "Cyber Security Frameworks In India, 2023".

unbundle the hardware, software and service and announced that henceforth it was going to charge price on these items separately. This proved a starting point for the growth of today's software industry.⁹⁶

Evolution of internet- today world is depend on net ,all things are electronic ,it all depend on the information. Computers, scanners identify birth defect or identify sex and are linked some time even after death till insurance matters are resolved. The computer has infiltrated all spheres of life and the effect has been so fast that it has taken the law and justice institutions by surprise. The new developments are challenging the old principles of law which had been very effective prior to the advent of this technology. The issues have introduction of Internet. It is already debatable whether there is a need to frame entirely new laws or whether the old laws can be applied in adopting new issues.⁹⁷

3.2 CYBER CRIME IN INDIAN SCENARIO

To conduct an offence against an individual or group of individuals with the goal to damage their reputation or inflict them physical or mental harm is the definition of a cyber crime, according to Wikipedia in some way, through the use of contemporary communication networks like the Internet as an instrument, a target, or a tool to commit additional crimes falls under the umbrella of crime. . There is no limit to the number of countries and states that cyber crime can traverse; it knows no bounds. Because cyber crime encompasses such a wide variety of actions, the scope and complexity of the problem mean that what constitutes criminal behavior in one country may not in another. Mainly these cyber crime: (1) those that directly attack There are two main types of computers and (2) those that use computers, networks, or gadgets to commit other crimes

Like-

1. Spam is the unsolicited sending of bulk e-mails for commercial purposes.
2. In order to hide unauthorized transactions, change or delete stored data, or manipulate, suppress, or steal output, fraud can be perpetrated. changing

⁹⁶ "Social Media And It Laws In India", Ministry Of Home Affairs, 2023.

⁹⁷ United Nations Office On Drugs And Crime (Unodc), "Global Perspectives On Cyber Laws", 2022.

or abusing preexisting software or system tools, or by modifying or creating code for deceitful ends. Bank fraud, identity theft, extortion, and classified information theft are some of the other types of fraud that computer systems enable.

3. **Controversial or insulting content:** (Section 67) Some prohibit racist, blasphemous, slanderous, or provocative content that might lead to hate crimes. nations have laws.
4. **Harassment** can take many forms, including cyber bullying, stalking, hate crimes, or the targeting of specific individuals based on their gender, race, religion, nationality, or sexual orientation with the use of obscenities. The use of a cell phone to encourage, entice, coerce, or enable the travel of a juvenile to engage in forbidden sexual activity resulted in an enhanced sentence for Kramer in the case of *United States v. Neal Scott Kramer*⁹⁸.
5. **Threats :** (Section 503 IPC) spoken or written “criminalized because of intent to harm or intimidate that also applies for online or any type of network related threats in written text or speech⁹⁹”.
6. **Drug trafficking :** (NDPS Act) drug traffickers are increasingly taking advantage of the Internet to sell their illegal substances through encrypted e mail. The virtual exchanges allow the more inhibited individuals to comfortably purchase illegal drugs.
7. **Cyber terrorism :** focuses upon the use of the Internet by non state actors to cause damage to a nation's economic and technological infrastructure. Since the September 11 attacks of 2001, public awareness of the threat of cyber terrorism has grown dramatically. Someone who intimidates or coerces a Government or organization to advance his political or social objectives by launching computer based attack against computers, network, and the information stored on them is a cyber terrorist Hacking

⁹⁸United state vs. neal scott ,437 u.s 82(1987)

⁹⁹ “E-Commerce And Cyber Law Regulations In India”, Confederation Of Indian Industry (Cii) Report, 2022.

activities directed towards individuals, families, tending to cause fear among people, demonstrating power, collecting information relevant for ruining people's lives, robberies, blackmailing etc are all cyber terrorism.

8. Cyber extortion is a form of crime in which a website, e-mail server, or computer system is subjected to repeated denial of service or other attacks by malicious hackers, who demand money in return for promising to stop the attacks¹⁰⁰.
9. Cyber warfare is Internet-based conflict involving politically motivated attacks on information and information systems. It can disable official websites and networks, disrupt or disable essential services, steal or alter classified data, and cripple financial systems among many other possibilities In August 2008, Russia allegedly conducted cyber attacks, in a co-ordinate and synchronized campaign against the State of Georgia.
10. **Pornography:** may be stated as the description or the demonstration of sexual actions in order to stated as the description or the demonstration of sexual actions in order to. A use sexual excitement through books, films, etc. This would include pornographic websites, pornographic material produced using computers and use of Internet to download and transmit pornographic videos, pictures, writings photos etc.
11. **Forgery (Section 463 IPC):** Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners.
12. IPR violations trademarks violations, theft of computer source code, patent violations etc .
13. **Banking/Credit Card related crimes:** In the corporate world, Internet hackers are continually looking for opportunities to compromise a company's security in order to gain access to confidential banking and financial information in order to commit frauds and thefts.

¹⁰⁰ Uttar Pradesh Cyber Crime Department, "Annual Cyber Law Enforcement Report, 2023".

14. E-commerce/Investment Frauds Merchandise or services that are purchased or contracted by individuals online are never delivered¹⁰¹.
15. Sale of illegal articles, Online gambling.
16. Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with etc.
17. Pedophiles are persons who intentionally prey upon children After earning 3 their trust, they gradually seduce them into sexual or indecent acts.
18. **Data diddling** : (Section 65) when entering a computer The NDMC Electricity Billing Fraud Case which occurred in 1996 is a typical example The NDMC relied on computers to receive and account the electricity bills and to maintain records and remit to the bank was solely entrusted to a private contractor who was a computer professional He misappropriated the massive funds by using computers to show less receipt and bank remittance¹⁰².
19. Trojan Attack The program that acts like something useful but does things that are quiet harmful The programs of this kind are called as Trojan as.
20. Virus and worm attacks A program that has capability to infect other programs and make copies of itself and spread into other programs is called virus Programs that multiply like viruses but spread from computer to computer are called as worms.
21. Defamation Section 499 (PC) is the intentional infringement of another person's right to his good name Cyber Defamation occurs when someone's name is maligned with the help of computers and/or the Internet. someone publishes defamatory matter about someone on a website or

¹⁰¹ Rajiv Kumar, "Intellectual Property Rights And Cyber Law In India", *Journal Of Law & Innovation*, 2022

¹⁰² National Digital Communications Policy, 2018 – Cyber Law Implications On Digital Infrastructure.

sends e-mails containing defamatory information to all of that person's friends.

Some Cases Related to Cyber Crime are :

- Bazee.com case the CEO of Bazee.com was arrested in December 2004 because a CD with objectionable material was being sold on the website This opened a Pandora's Box as to how much is the service provider responsible for what is being sold through his website
- In 1983, a nineteen-year-old UCLA student used his PC to break into a Defense Department international communications system
- On 26 March, 1999, the Melissa worm infected a document on a victim's computer, then automatically sent that document and copy of the virus via email to other people
- The News SKY TV service was hacked a few times as part of a continuing technological arms race between a pan European hacking organization and News corp. The first of complete law in the whole world. India was previously unaware of cyber law only that a torrent of cyber crimes has compelled the law makers to take their seats and take the situation into account. Information Technology Act. 2000 had been passed, but with numerous shortcomings. The amendment of information technology Act in 2008 introduced a lot of changes in this respect but the amendment has introduced a fresh start to problems with cyber crimes by extending it a horizon continue to persist.¹⁰³

The problem of jurisdiction has been quite controversial since cyber crimes are not limited to manual lines. In such a manner, the notion of territorial jurisdiction as perceived by Section 16 of Cr. P.C and Section 2 of the 1PC approach of settling of disputes.

The routinely destroyed. The system of crime investigation is also paralyzed in case of further gathering of information beyond the territorial scope.

¹⁰³ Indian Cyber Crime Coordination Centre (I4c), Ministry Of Home Affairs, Government Of India, 2023 Report.

Newer modes must be developed to be a head of the criminal minds and be capable of countering them. They are the most affected by cyber attacks as they form the largest segment of the recipients of the attacks in homes.

The any electronic trail of information in their computers, use of anti-virus, firewalls, use of intrusion detection system etc. More strict application of cyber laws should also be enforced to curb crime.

CHAPTER–IV

CYBER CRIME COMPARATIVE STUDIES IN OTHER COUNTRIES

4.1 INTRODUCTION

Jurisprudence covers the study of the concepts of law and the effect of social norms and regulations on the development of law. Jurisprudence refers the philosophy of law or legal theory and case law. Legal theory does not study the characteristics, development, functioning, and implementation etc. of law in a particular country but studies law in general i.e. those attributes common to the legal systems in a globe. Case law is the law that is established through the decisions of the courts and other officials. Case law assumes even greater significance when the wordings of a particular law are ambiguous. The interpretation of the courts helps to clarify the real objectives and meaning of such laws¹⁰⁴.

The concept of cyber crimes is largely incorporated in jurisprudence of cyber law. Justifications in the cyber jurisdiction, cyber criminals, modes of Use of technology in such a misuse as cyber crimes, cyber crimes of various kinds, general and legal difficulties of drafting and enacting cyber laws etc.¹⁰⁵

The causes of cyber crime under cyber jurisdictions have to do with the causes of the vulnerability of computers like ability to store information in relatively small areas, easy accessible, complicity and negligence. The types and forms of cyber crimes committed via cyber space include: children and adolescents, organized hacker, professional hacker/cracker, disconnected employees etc. models and methods to computer systems or networks/hacking, e-mail bombing, data diddling, salami attacks, denial of service attack, virus/worm attacks, logic bombs, Trojan attacks, Internet time theft, web jacking etc.

¹⁰⁴United Nations Office on Drugs and Crime (UNODC), "Global Cyber crime Report", 2022.

¹⁰⁵Interpol, "Cyber Crime Trends Across Nations", 2023.

The cyber space jurisprudence of cyber crime classification includes cyber crimes against individuals, cyber crimes against organization and cyber crimes against the society at large. Other relevant cyber crimes compared to IT Act, 2000 are mostly cyber stalking, cyber squatting, cyber defamation, Trojan attack, forgery, financial crimes, virus/worm attack, e-mail spoofing, e-mail bombing, salami attack, web jacking etc¹⁰⁶.

Through International Legal Regime, one can explore cyber jurisprudence at International Law. It encompasses cyber laws of key nations, laws on cryptography, international legal regime on cyber crimes and international legal regime on intellectual property rights. There are numerous conventions included in the International Legal Regime regarding cyber crimes which include- EU. crime, Convention on cyber crime, Budapest. European Cyber Crime Convention. Hague Convention on Jurisdiction etc.

International Legal regime relating to intellectual property rights includes various conventions and treaties such as- Berne Convention, Rome Convention, WWIPO Copyright Treaty, WIPO Performance and Phonograms Treaty, UDRP, OECD Convention on Database Protection etc. The international views of the cyber law have many areas and concerns like- UN and (ITU) efforts. EDI concept and law issues, Asia Pacific Economic Cooperation and Development (OECD), organization and operation of World Bank, Common Wealth of Nations and reasonable security practices.¹⁰⁷

In India, till 2000, cyber space was un-regulated. The overall law is the act, 2000 which entails the prevention, regulation and control. The Provisions of Indian Penal Code govern 2000.

4.2 COMPARATIVE ANALYSIS OF CYBER LAWS

A comparative analysis of cyber laws across different countries reveals variations in legal frameworks, approaches to regulation, and priorities in

¹⁰⁶ Council of Europe, "Convention on Cyber crime (Budapest Convention)", 2001

¹⁰⁷ FBI Internet Crime Report, Federal Bureau of Investigation, USA, 2023.

addressing cyber-related challenges. Here are some key aspects to consider in such an analysis.

A- Scope and Coverage:

Different countries may have varying scopes of cyber laws, covering areas such as cyber security, data protection, electronic commerce, intellectual property rights, and cyber crime. Some countries may have comprehensive legislation addressing multiple aspects of cyber space, while others may have fragmented laws focusing on specific issues.¹⁰⁸

B- Legal Principles and Concepts:

While the fundamental legal principles underlying cyber laws, such as jurisdiction, sovereignty, security, privacy, and accountability, are universal, their interpretation and application may vary across countries. Cultural, political, and social factors influence how these principles are reflected in national legal frameworks.

C- Regulatory Frameworks:

Countries adopt different regulatory approaches to govern activities in cyber space. Some countries may rely on prescriptive regulations with detailed requirements and obligations for stakeholders, while others may adopt principles-based approaches that provide flexibility for adaptation to evolving technologies and practices.¹⁰⁹

D- Data Protection and Privacy:

Laws and regulations governing data protection and privacy vary significantly across countries. Some countries have comprehensive data protection laws with strict requirements for data processing, consent, and data subject rights, while others may have minimal or fragmented legislation in this area.

¹⁰⁸ Europol, "The Internet Organised Crime Threat Assessment (IOCTA)", 2022.

¹⁰⁹ UK Home Office, "Cyber Crime Annual Report", 2023.

E- Cyber security Measures:

Cyber security laws and regulations may differ in terms of the requirements imposed on organizations to safeguard their networks, systems, and data. Countries may have different approaches to cyber security standards, incident reporting, information sharing, and government intervention in cyber defense.

F- Intellectual Property Rights:

Laws protecting intellectual property rights in cyber space, such as copyright, trademarks, patents, and trade secrets, may vary in terms of scope, enforcement mechanisms, and penalties for infringement. Countries may have different thresholds for copyright protection, approaches to digital rights management, and liability regimes for online intermediaries.¹¹⁰

G- Cyber crime Legislation:

Cyber crime laws and regulations address offenses such as hacking, identity theft, fraud, and online harassment. Countries may have different definitions of cyber crimes, penalties for offenders, and procedures for investigation, prosecution, and international cooperation in combating cyber threats.

H- Internet Governance:

Legal Internet law Internet law regulating internet governance, domain name registration, and internet infrastructure might be different in different countries. Whereas others can pursue multi stake holder attitudes to internet governance.¹¹¹

I- Enforcement and Compliance:

The effectiveness of cyber laws depends on their enforcement mechanisms, resources allocated for implementation, and compliance by stakeholders. Countries may face challenges in enforcing cyber laws due to

¹¹⁰ Australia Cyber Security Centre (ACSC), "Annual Cyber Threat Report", 2022

¹¹¹ China's Cybersecurity Law (2017) and Recent Amendments, Government of China.

limited resources, technical capabilities, legal capacity, and cross- border jurisdictional issues.

J- International Cooperation:

Countries engage in international cooperation and collaboration to address transnational cyber threats, harmonize legal frameworks, and exchange best practices. Bilateral and multilateral agreements, treaties, and initiatives facilitate information sharing, capacity building, and joint efforts to combat cyber crime and promote cyber security.

Overall, a comparative analysis of cyber laws across different countries highlights the diversity of legal frameworks, regulatory approaches, and challenges in addressing cyber-related issues at the national and international levels. By understanding these variations, policymakers, legal experts, and cooperation, learn from best practices, and enhance the effectiveness of cyber laws in promoting a secure, trustworthy, and inclusive digital environment.¹¹²

4.3 CYBER LAWS IN CHINA

The National People's Congress approved the Cyber Law of the peoples Republic of China (Chinese), otherwise referred to as the Chinese Cyber security Law, in an attempt to enhance cyber security, data localization, and sensitive information protection, allegedly in the name of national security. This act is an attempt by the Chinese government to strengthen its national security legislation; it is not the only legislation. Since 2014, there are several laws, most of which were approved in close succession, including laws related to data security, national intelligence, national security, counter-terrorism, and foreign NGO administration.¹¹³

A- Brief History

Chinese policymakers became increasingly concerned about the risk of cyber attacks following the 2010s global surveillance disclosures by Edward

¹¹² European Union Agency for Cybersecurity (ENISA), "Cyber Threat Landscape", 2023.

¹¹³ Kaspersky Lab, "Global Ransomware Report", 2022

Snowden, which demonstrated extensive United States intelligence activities in China. The Cyber security Law was part of China's response following policymakers' heightened concerns of foreign surveillance and data collection after these disclosures.¹¹⁴

This law was passed by a Standing Committee of the National People Congress on November 7, 2016, and it became effective on June 1, 2017. It permits the spot checks of networks belonging to a company by the Chinese authorities and makes network providers store part of their data in China.

It is the common agreement that cyber security is an essential principle. Based on this, the statute falls at the top in the cyber security legislative pyramid. The legislation is a macro-level framework that is the development of previous levels and area cyber security rules and regulations. The legislation also includes bare minimum standards on certain issues that are not much critical at this time but will be relevant in future. These norms will be used as a source of legal reference when new issues arise.

B- Legal Provisions

The law is a significant pillar of the Chinese data regulatory environment. It

- Created the principle of cyber space sovereignty
- Defined the security obligations of internet products and services providers
- Detailed the security obligations of internet service providers
- . Further refined rules surrounding personal information protection
- Established a security system for key information infrastructure
- Instituted rules for the transnational transmission of data from critical information infrastructures.¹¹⁵

¹¹⁴ The United States Department of Justice, "Cyber crime Prosecutions in the USA", 2023.

¹¹⁵ Canada's "Cyber Security Strategy", Public Safety Canada, 2022.

The cyber security law applies to network operators and firms within vital sectors. The Chinese telecommunications, information, energy, transport, water, financial, public, and electronic government service industries are the most significant critical sector firms in the country in terms of networking. Of special concern are the articles 28, 35 and 37 of the statute.¹¹⁶

Article 28: compels vaguely defined “network operators”, (interpreted to include: social media platforms, application creators and other companies, to cooperate with public security organs such as the Ministry of Public Security and hand over information when requested.

Article 28: Operators of networks are obligated to offer technical support and cooperation to national and public security agencies that are conducting lawful investigations into criminal activity and protecting the nation's security.

Section 1: 'Ordinary Provisions'

Article 35 is targeted at purchases of foreign software or hardware by government agencies or other “critical information infrastructure operators”, requiring any hardware or software purchased to undergo review by agencies such as China's SCA or State Cryptography Administration, potentially involving the provision source codes and other sensitive proprietary information to government agencies paving the way state theft of intellectual property or transmission to domestic competitors. Above all, the article creates further regulatory burdens for foreign technology companies operating in China, indirectly creating a more favorable playing field for domestic competitors which would naturally be more prepared to comply with the regulations.¹¹⁷

Article 35a : Before making any purchases of network items or services that could compromise national security, operators of critical information infrastructure are required to complete a national security review that is coordinated by the State cyber space and information departments and the appropriate State Council departments.

¹¹⁶ “Cyber Crime in the Asia-Pacific Region”, Asia-Pacific Economic Cooperation (APEC) Report, 2022.

¹¹⁷ “Cyber security in Latin America”, Organization of American States (OAS), 2023.

Section 2: 'Operations Security for Critical Information Infrastructure'

The law establishes stringent data localization requirements

All Chinese companies who operate their own data networks or servers are subject to the law. Among other things, network operators should make sure everyone knows who is responsible for what when it comes to cyber security, implement practical safeguards to keep network operations secure, stop data leaks and theft, and notify users and the appropriate sector implementing department of any cyber security incidents.

It comprises subsidiaries of regulations which clarify on the intent of the law. As an illustration, the CII Security Protection Regulations and Measures of the security assessment of the transfer of personal information and important data across the borders are worthy and pertinent examples. However, the act is not in full swing yet as the Chinese government is still preparing some more rules that should be available to ensure that it aligns better with the cyber security law. The inclusion of the existing VPN and data security legislations into the cyber security law would enable the Chinese government to further control the internet and emphasize on the international corporations operating under the Chinese regulations.¹¹⁸

Regulations and definitions of legal liability are also provided under the cyber security law. A wide range of penalties, including fines, suspension for correction, and the revocation of licenses and permits, are established by law for many forms of unlawful behavior. As a result, the bill gives cyber security and administration agencies the power and the rules they need to crack down on criminal activity.

Related regulations

In July 2021, the Cyber space Administration of China issued “Regulations on the Management of Security Vulnerabilities in Network Products” requiring that all vulnerabilities be reported to government agency

¹¹⁸ German Federal Office for Information Security (BSI), “Cyber Security Report”, 2022.

responsible for overseeing business and IT (MIIT) and prohibits the public disclosure of vulnerabilities, including to overseas organizations.¹¹⁹

Reactions

Legal constraints, such as the Great Firewall, have been a source of concern for international technology companies doing business in China. Concerning the certification and spot-check requirements, international law firms have expressed concern that companies may be asked to provide encryption keys, source code, or other sensitive information for government review. This could lead to intellectual property theft, data loss, sharing with local competitors, or even exploitation by government officials. The FBI expressed concern that the regulation may subject businesses that send data via Chinese computers to espionage and data surveillance.¹²⁰

Some analysts from Western backgrounds consider this law to be comparable to the EU's GDPR. They have suggested that the law could improve the Chinese government's ability to monitor the public, as well as giving Chinese companies an advantage over foreign companies. The wording and particular requirements of the bill caused alarm on a global and national scale. Since this rule mandates that foreign corporations and businesses in China "store their data on Chinese-law governed local servers and cooperate with Chinese national security agencies," its proponents worry that it may discourage foreign investment in China in the future.

Since its inception many foreign technology companies have already complied with the law. Apple for example, announced in 2017 that it would invest \$1 billion in partnership with local cloud computing company Guizhou Cloud Big Data or GCBD to construct a new data center located in China's Guizhou province for the purposes of compliance. Simultaneously, the company also said that it will move i Cloud operations and storage to mainland China.

¹¹⁹ South Korea's Cyber Terror Response Centre, "Annual Cyber Threat Review", 2023

¹²⁰ Japan's National Police Agency, "Cyber Crime White Paper", 2022.

Microsoft has also stated that it will be investing in additional servers to expand its Azure services in conjunction with cloud computing provider 21Vianet. Chat apps like Skype and Whatsapp, which did not want their data stored locally, were either removed from domestic app stores or restricted from further expansion.¹²¹

Foreign technology and other companies operating in China are compelled by law to either join forces with service providers like Tencent, Alibaba, or Huawei, who already have server infrastructure in place, or invest in new server infrastructure to comply with the law, resulting in capital expenditure costs for companies. Most people believe the regulation is in keeping with the 12th Five-Year Plan (2011–2015), which seeks to establish homegrown leaders in fields like big data processing and cloud computing. Proponents of the bill point to its benefits for domestic businesses, while opponents say it unfairly disadvantages foreign IT giants like Google and Microsoft.¹²²

The bill supporters have made it clear that the bill is not intended to deter or even ban foreign firms to conduct business in China and enhance domestic competitiveness. A 2015 study by Matthias Bauer and Hosuk Lee- Makiyama found that data localization leads to small losses in the economic growth of a few countries thanks to the delays in the data transfer protocols and duplication of the data across numerous countries. The feeling is that the government of China is attempting to have firms localize their data in an effort to be prosecuted easier due to violation of rules of the Chinese internet.

The bill supporters have made it clear that the bill is not intended to deter or even ban foreign firms to conduct business in China and enhance domestic competitiveness. A 2015 study by Matthias Bauer and Hosuk Lee- Makiyama found that data localization leads to small losses in the economic growth of a few countries thanks to the delays in the data transfer protocols and duplication of the data across numerous countries. The feeling is that the government of China is

¹²¹ "Cyber security and Data Protection in Africa", African Union Commission Report, 2023.

¹²² Indian Computer Emergency Response Team (CERT-In), "International Cyber Threat Analysis", 2022.

attempting to have firms localize their data in an effort to be prosecuted easier due to violation of rules of the Chinese internet.

Critics said the rule curtailed people's ability to freely express themselves. For instance, in order to comply with the law, the majority of Chinese internet services must gather user identification information, confirm their identities, and, if asked, hand over this data to the authorities without a warrant. Protesters claim this regulation makes it easier to spy on dissidents and discourages individuals from expressing themselves freely online, thereby limiting dissent.¹²³

4.4 CYBER LAWS IN PAKISTAN

The Pakistan government's amendment to its cyber crimes act is the latest in a concerted campaign to restrict freedom of expression and stifle dissent, Amnesty International and Human Rights Watch said today. On February 18, 2022, the government passed an ordinance amending the Pakistan Electronic Crimes Act, 2016 (PECA) to make online "defamation" of authorities, including the military and judiciary, a criminal offense with harsh penalties. "PECA has been used to silence freedom of expression on the pretext of combating 'fake news,' cyber crime, and misinformation," said Nadia Rahman, Acting Deputy Regional Director for South Asia at Amnesty International. "This amendment not only violates the Pakistan Constitution, but also puts anyone who questions the government or other state institutions at further risk. It particularly targets journalists, human rights defenders, and political opponents who run the risk of prosecution for merely doing their jobs."¹²⁴

While PECA already contained broad provisions criminalizing defamation of "natural persons," the Pakistan Amendment Ordinance (2022) expands those provisions to include criticism of government bodies and the military by inserting a new definition of "person" that includes "any company, association or body of persons,... institution, organization, authority or any other body established by the Government under any law or otherwise." The amendment makes defamation

¹²³ "Dark Web and Cyber Crime", Research Paper by Harvard University, 2021.

¹²⁴ Russian Cyber Crime Laws and Regulations, Ministry of Internal Affairs of Russia, 2023.

a non-bailable offense, and increases the prison term, if convicted, from three to five years. It also expands the definition of those who can initiate criminal proceedings for defamation, allowing any person or institution to register the complaint.¹²⁵

Pakistan has ratified the International Covenant on Civil and Political Rights (ICCPR). Article 19 of the ICCPR permits limitations on the freedom of expression in order to safeguard the reputation of others, but any limitation should be limited and only in rare cases. Amnesty International and Human Rights Watch are against criminal defamation laws in their entirety because they are an excessive and unjustified reaction to the reality of reputation protection which paralyzes freedom of expression. Extending PECA criminal defamation provisions which are already far-reaching to online statements regarding government institutions are in contravention with the international requirements of Pakistan. The government did not include the consultation of the civil society groups and the private sector in amendments, thus depriving the real scrutiny of the amendments by the people before it was enacted¹²⁶.

The amendment to PECA also makes it incumbent upon courts to conclude trials within six months and furnish monthly progress reports of pending trials, and orders federal and provincial officials to remove any obstacles that may hinder the progress of the proceedings. It is not evident how an already overburdened court system will safeguard people from unfair trials and poor evidence gathering, the groups said. “The Prevention of Electronic Crimes Act neither protects the public from legitimate cyber crime concerns nor respects fundamental human rights,” said Patricia Gossman, Asia associate director at Human Rights Watch. “The new amendments will further embed violations of basic rights with a thin veneer of legality.”

¹²⁵ United Arab Emirates (UAE) Cyber Crime Law, 2012 (Revised 2022).

¹²⁶ “Comparative Study of Cyber Laws: India, USA, and Europe”, International Journal of Cyber Law, Vol. 15, Issue 2, 2022.

On February 23, the Islamabad High Court restrained the Federal Investigative Agency, the main investigative body for PECA, from making any arrests under the ordinance. While this offers temporary relief, it is not enough to mitigate the grave impact that the amendment will have on Pakistan's already imperiled freedom of expression by potentially putting anyone at risk of criminal charges for expressing their views online, Human Rights Watch and Amnesty said.

The act of Pakistan Electronic Crime, 2016 is a draconian act which includes vague and too broad offences. The human rights defenders and civil society groups in Pakistan have criticized this move to criminalize legitimate modes of expression on the issue of the so called national security grounds and to defend majoritarian readings of Islam. Censorship of online and offline speech is one of the continuing oppressions of dissent.¹²⁷

In 2021, the Pakistan Media Development Authority Ordinance was proposed which effectively enables press censorship by bringing all media under one regulator, granting the government unchecked powers to punish journalists through steep fines, instituting special “media tribunals” and appointing government officials to key positions. The draconian Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules—legislation that would censor online content—was enacted in October 2021¹²⁸.

“The amendment, in effect, permits authorities to digitally police what people are saying online and levy heavy punishments if they do not like what they are saying,” said Patricia Gossman. “Laws should be centered around protecting human rights, not insulating the government from legitimate criticism.

The authorities should either swiftly repeal PECA and this amendment entirely, or substantially amend them to align them with international human rights standards,” Nadia Rahman said.

¹²⁷ “Cyber Fraud Trends in Developed and Developing Nations”, World Economic Forum Report, 2023.

¹²⁸ Singapore's Personal Data Protection Act (PDPA) and Cybersecurity Regulations, 2023.

New Cyber security Legislation

The bills, signed into law on June 21, aim to strengthen the federal cyber work force and foster collaboration across all levels of government. The two cyber security bills were signed into law by the U.S. President Joe Biden on June 21, 2022. The most recent of a succession of attempts. security, the new law is supposed to ensure competencies and experience amongst the federal cyber work force and foster security coordination at every government level. The State and Local Government Cyber security Act of 2021 is aimed at enhancing coordination between the Cyber Security Agency (CISA) and the states, local, tribal, and territorial governments. Such bodies will find it easier to share security tools, procedures and information under the new law.

“For hackers, state and local governments are an attractive target,” Rep. Joe Neguse (D-Colo.), who introduced the bill, said in a statement. “We must increase support to these entities so that they can strengthen their systems and better defend themselves from harmful cyber attacks.”

In the month of last month alone there were several ransom ware attacks made to state and local governments including New Mexico and Ohio school systems, the city of Quincy in Massachusetts and the Somerset County in New Jersey. The Federal Rotational Cyber Work force Program Act of 2021, a second new piece of cyber security legislation, will permit the U.S. government worker in the IT and cyber security sector, as well as other related areas, to rotate among different positions across the agencies, thereby allowing them to acquire new knowledge and experience in numerous job operations. In January, a CISA-funded report by the National Academy of Public Administration discovered that the federal government lacks a comprehensive, integrated approach to the government-wide strategy. The developing a work force” The rotation program aims to expand cyber professionals’ career horizons while improving interagency knowledge transfer and cooperation.¹²⁹

¹²⁹ Brazil’s General Data Protection Law (LGPD) and Cyber Crime Regulations, 2022.

Justin Fier, Darktrace’s vice president of tactical risk and response, told Security that the act “will grant federal cyber professionals valuable transferable skills and diversify their career paths,” but cautioned that “it also adds to an industry already suffering peak burnout.” In a recent survey by Threat Connect, nearly a third of cyber security professionals reported feeling highly stressed at work. The new laws continue a trend of increased efforts to shore up cyber security at the federal, state, and local levels. This March saw the passage of the Cyber Incident Reporting Act, which requires organizations in critical infrastructure sectors (as defined by CISA) to report a cyber attack within 72 hours and a ransomware payment within 24.

That act, which VMware’s head of cyber security strategy Tom Kellerman called a “game changer,” was passed unanimously by the Senate, indicating increasing recognition of the importance of cyber defense. “I’ve been in cyber security for 23 years,” Kellerman said. “To have true bipartisanship action in this regard is historic.”

Lev Craig is an editor at EC-Council covering cyber security, block chain, and Dev Ops. Before joining EC-Council, Lev worked as a freelance writer and editor in a range of areas in tech, including AI and machine learning, software development, and data privacy. Lev graduated from Harvard University in 2016 with a B.A. in English and lives in New York’s Hudson River Valley.

The Biden-Harris Administration released the National Cyber security Strategy on March 2, 2023, to secure the full benefits of a safe and secure digital ecosystem for all Americans. The Strategy recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyber space. It outlines two fundamental shifts in how the United States allocates roles, responsibilities, and resources in cyber space¹³⁰.

1. We must rebalance the responsibility to defend cyber space by shifting the burden for Cyber security away from individuals, small businesses, local

¹³⁰ New Zealand Cyber Security Strategy, Government of New Zealand, 2023.

governments, and infrastructure operators, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.

2. We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.

“Cyber security is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense.”

Improving the Nation’s Cyber security

The following is commanded by me, the President, by virtue of the power bestowed upon me by the Constitution or the law s of the USA:

Section 1. Policy.

The private and governmental sectors, as well as the safety and privacy of the American people, are under constant attack from malevolent cyber attacks that are getting more and smarter. It is imperative that government enhances its measures to recognize, discourage, safeguard, detect, and react to such activities and individuals. The federal government also has a responsibility to thoroughly investigate and learn from any significant cyber event. However, cyber security cannot be addressed alone by the government.

The government of the United States needs to collaborate with the private corporations to protect the nation against the cyber criminals. The private sector must be malleable when it comes to constructing and running products, as it tries to keep pace with the constantly evolving threat environment. It can also assist in protecting cyber space by acting together with the federal government. Finally, our level of trust toward our digital infrastructure should be based on how reliable and transparent it is and the possible consequences of losing the trust.

To safeguard the basic institutions on which the American way of building life involves, the federal government will have to go through drastic reforms and huge expenses, small steps will not be enough. Every single federal government computer system, be it cloud; be it on-premise; or it be a hybrid set-up should have the full power of the law behind to make certain that it is safe and secure. IT systems which process data and OT systems which power the potentially critical machinery to ensure our safety need to be part of the protection and security.

The national and economic security is based on our capacity to detect, investigate, and fix cyber problems upon their occurrence. This will be in accordance to my administrative policies. The federal government should provide a good example. There is an urgent need of ensuring that all the Federal Information Systems comply, even exceed the requirements of the Cyber security requirements, identified and developed as a result of this directive.¹³¹

Section 2. Removing Barriers to Sharing Threat Information.

(a) Outside information technology and operations technology companies are hired to the federal government to operate the numerous routine activities running on the federal information systems. The service providers, cloud providers and others, are provided with unique knowledge regarding the cyber incidents and threats to federal information systems. The investigation and remediation of cyber incidents fall under the mandate of executive branches and agencies (including the Cyber security and Infrastructure Safety Agency (CISA), the Federal Bureau of Investigations (FBI), and other members of the Intelligence Community). The dissemination of such threat or incident information to such agencies can also however be restricted by the existing contract terms or limitation.

Member ship (MC). To enhance the safety of the systems of the federal agencies and the information that is collected, processed, or stored on behalf of

¹³¹ "Comparative Analysis of Cyber Laws: GDPR vs. US Data Protection", International Data Privacy Journal, 2022.

them and accelerate the process of deterring, preventing and responding to any incidents, it is necessary to eliminate these contractual barriers and enhance information sharing concerning such threats, incidents and risks.¹³²

The next step would be taken within sixty days of date of this order the head of the OMB, in consultation with the defenses secretary, the attorney general, the secretary of homeland security, and the director of national intelligence would study the language and requirements of contracts with information technology and operational technology services providers as stipulated in the Federal Acquisition Regulation (FAR) and the Defense Federal Acquisition Regulation Supplement and recommend modifications to those provisions to the FAR Council and other appropriate agencies. Some of the proposed modifications in the text of the contract include the description of the category of contractors that would be included.

- (a) The suggested contract language and requirements as detailed in subsection of this section shall be designed to provide that:
- (b) service providers gather and maintain data, information, and reporting that applies to the prevention, detection, response, and investigation of cyberspace events on all information systems under their control, including systems on behalf of agencies, in accordance with the needs of the agencies;
- (c) such data, information, and reporting are shared with such agencies by the service providers, as they relate to cyber incidents or potential incidents where any agency may have contracted them and any other agency which the Director of OMB in consultation with the Secretary of Defense, the Attorney General, the Secretary of Homeland Security and the Director of National Intelligence considers it appropriate, in accordance with the current rules on privacy; service providers cooperate with Federal Cyber security or investigative.

¹³² "International Efforts to Combat Cyber Crime", NATO Cyber Defense Centre Report, 2023.

Agencies in their investigations and response to incidents or potential incidents on Federal Information Systems, including by implementing technical capabilities, such as monitoring networks for threats in collaboration with agencies they support, as needed; and

- i) The information provided by service providers to agencies regarding cyber threats and incidents, whether in industry-standardized format or not, is used in response and remediation of incidents.¹³³
- (ii) The FAR Council will within 90 days of the receipt of the recommendations outlined in subsection (a) of this section consider the proposed contract language and conditions and may, in accordance with he suitable circumstances, publish to public, proposed updates to the FAR.
- (iii) The Secretary of Homeland Security and the Director of OMB will work within 120 days of this order date to take reasonable actions to ensure to the best of their ability that data that is shared by service providers with agencies, CISA, and the FBI is necessary to enable the Federal Government to respond to cyber threats, cyber incidents, and cyber risk.
- (iv) The providers of ICT services should also have direct reporting to CISA whenever they report under subsection (f)(i) under Federal Civilian Executive Branch (FCEB) Agencies, and CISA will centralize and control such information.¹³⁴
- (v) reports made under National Security Systems, within the meaning of section 10(h) of this order, shall be received and processed by an appropriate agency as may be decided under subsection of this section

In order to enact the policy contained in subsection (f) of this section: The Secretary of Homeland Security, after consultation with the Secretary of Defense through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB shall propose to the FAR Council contract

¹³³ World Bank Report on “Cyber Crime and Economic Impact in Emerging Markets”, 2022.

¹³⁴¹³⁴ OECD (Organisation for Economic Co-operation and Development), “Cybersecurity Policy Framework”, 2023.

language that identifies: Within 45 days of date of this order, the Secretary of Homeland Security, in consultation with the Secretary of Defense through the Director of the National Security Agency (NSA), the Attorney General, and the Director of OMB shall propose to the FAR Council contract language that

- A- The nature of cyber incidents that require reporting;
 - B- The types of information regarding cyber incidents that require reporting to facilitate effective cyber incident response and remediation;
 - C- Appropriate and effective protections for privacy and civil liberties;
 - D- The time periods within which contractors must report cyber incidents based on a graduated scale of severity, with reporting on the most severe cyber incidents not to exceed 3 days after initial detection;
 - E- National Security Systems reporting requirements; and
 - F- The type of contractors and associated service providers to be covered by the proposed contract language.
1. Within 90 days of receipt of there commendations described in subsection(g)(i) of this section, tHe FAR Council shall review there commendations and publish for public comment proposed updates to the FAR
 2. Within 90 days of the date of this order ,the Secretary of Defense acting through the Director of the NSA, the Attorney General ,the Secretary of Homeland Security, and the Director of National Intelligence shall jointly develop procedures for ensuring that cyber incident reports are promptly and appropriately shared among agencies.
 3. Current Cyber security requirements for unclassified system contracts are largely implemented through agency-specific policies and regulations, including cloud service Cyber security requirements. Standardizing common cyber security contractual requirements across agencies will stream line and improve compliance for vendors and the Federal

Government.¹³⁵

4. Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA, in consultation with the Secretary of Defense acting through the Director of the NSA ,the Director of OMB ,and the AdministratorofGeneralServices,shallreviewagency-specificcybersecurity requirements that currently exist as a matter of law, policy, or contract and recommend to standardized contract language for appropriate cyber security requirements. Such recommendations shall include consideration of the scope of contractors. and associated service providers to be covered by the proposed contract language.¹³⁶
5. Within 60 days of receiving the recommended contract language developed pursuant to subsection(i) of this section ,the FAR Council shall review the recommended contract language and publish for public comment proposed updates to the FAR.
6. The Director of OMB shall incorporate Into the annual budget process cost analysis of all recommendations developed under this section.¹³⁷

Section 3. Modernizing Federal Government Cyber Security.

- (a) To keep pace with today’s dynamic and increasingly so phisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cyber security, including by increasing the Federal Government’s visibility into threats, while protecting privacy and civil liberties. The Federal Government must adopt security best practices ;advance toward Zero Trust Architecture ;accelerate movement to secure cloud services, including Software as a Service(SaaS),Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and stream line access to cyber security data to drive analytics for identifying and managing cyber security risks; and investing both technology and personal

¹³⁵ International Telecommunication Union (ITU), “Global Cyber security Index (GCI)”, 2022.

¹³⁶ World Economic Forum, “Global Risks Report: Cyber security Threats”, 2023.

¹³⁷ “Cyber Crime in the Middle East: Challenges and Countermeasures”, Gulf Cooperation Council (GCC) Report, 2023.

to match these modernization goals.

- (b)** Within 60 days of the date of this order, the head of each agency shall:
- (c)** Update existing agency plans to prioritize resources for the adoption and use of cloud technology as outline din relevant OMB guidance;
- (d)** Develop a plan to implement Zero Trust Architecture, which shall incorporate,as appropriate,themigrationstepsthattheNationalInstitute of Standards and Technology(NIST) within the Department of Commerce as outline standards and guidance ,describe any such steps that have already been completed, identify activities that will have the most immediate security impact ,and include as schedule to implement them
- (e)** ProvideareporttotheDirectorofOMBandtheAssistanttothePresidentand National Security Advisor (APNSA) discussing the plans required pursuant to subsection(b)(i)and(ii)of this section.¹³⁸
- (f)** As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture ,as practicable.
- (g)** The CISA shall modernize its current cyber security programs, services, and capabilities to be fully functional with cloud-computing environments with Zero Trust Architecture.
- (h)** The Secretary of Home land Security acting through the Director of CISA,in consultation with the Administrator of General Services acting through the Federal Risk and Authorization Management Program(Fed RAMP) within the General Services Administration, shall develop security principles governing Cloud Service Providers(CSPs) for in corporation into agency modernization efforts. To facilitate this work:
- (i)** Within 90 days of the date of this order, the Director of OMB, in

¹³⁸ Malaysia's Cyber Security Strategy, National Cyber Security Agency (NACSA), 2022.

consultation with the Secretary of Home land Security acting through the Director of CISA, and the Administrator of General Services acting through Fed RAMP, shall develop a Federal cloud-security strategy and provide guidance to agencies accordingly. Such guidance shall seek to ensure that risks to the FCEB from using cloud-based services are broadly understood and effectively addressed, and that FCEB Agencies move closer to Zero Trust Architecture.¹³⁹

- (j) Within 90 days of the date of this order, the Secretary of Home land Security acting through the Director of CISA, in consultation with the Director of OMB and the Administrator of General Services acting through Fed RAMP, shall develop and issue, for the FCEB, cloud-security technical reference architecture documentation that illustrates recommended approaches to cloud migration and data protection for agency data collection and reporting.¹⁴⁰
- (k) Within 60 days of the date of this order, the Secretary of Homeland Security acting through the Director of CISA shall develop and issue, for FCEB Agencies, a cloud-service governance framework. That frame work shall identify a range of services and protections available to agencies based on incident severity. That frame work shall also identify data and processing activities associated with those services and protections.
- (l) Within 90 days of the date of this order, the heads of FCEB Agencies, in consultation with the Secretary of Homeland Security acting through the Director of CISA, shall evaluate the types and sensitivity of their respective agency's unclassified data, and shall provide to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB a report based on such evaluation. The evaluation shall prioritize identification of the unclassified data considered by the agency to be the

¹³⁹ France's National Cyber security Strategy, Agency National de la Securities des Systems d'Information (ANSSI), 2023.

¹⁴⁰ Switzerland's Federal Cyber security Law and Response Mechanisms, Swiss National Cyber Security Centre, 2022.

most sensitive and under the greatest threat, and appropriate processing and storage solutions for those data.

Conclusion

The cyber security laws is not proper in Pakistan. Cyber crime increase day-to day in Pakistan. The Cyber law did not specific related to same thing. This law is govern under criminal law. The specific law in mention Pakistan electronic crimes act. 2016 and the U.S. passes new cyber security legislation in June 2022. According to present time this law in not sufficient. The removing various related to the disclosure of information about potential dangers as stated in the aforementioned statutes. Act does make reference to federal cyber security legislation.¹⁴¹

4.5 CYBER LAWS IN JAPAN

Cyber crime Would any of the following activities constitute a criminal or administrative offence in your jurisdiction: hacking; denial-of-service attacks sale of hardware, software or other tools used to commit cyber crime; possession or use of hardware, software or other tool used to commit cyber crime; identity theft or identity fraud; electronic theft; unsolicited penetration testing; or any other type of activity that has a detrimental or threatening impact on, or threat to, the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data? And, so, please tell me about the crime, penalty up to hand that would be imposed in the most severe case, and the cases of prosecution in your jurisdiction: As background, attacks, namely (A) the that criminalize cyber Defiance of Unauthorized Computer Access (the UCAL), and (B) the Penal Code.¹⁴²

A. UCAL Imposes Criminal Sanctions

The UCAL imposes criminal sanctions on any person who makes an “Unauthorized Access” to a computer (an “Access Controlled Computer”), the

¹⁴¹ “A Comparative Review of Cyber crime Laws in Nordic Countries”, Scandinavian Journal of Law and Digital Security, 2022.

¹⁴² “Cyber Warfare and Digital Threats”, NATO Cyber Defense Centre Annual Report, 2023.

access to and operation of which are under the control of an administrator (the “Access Administrator”).

Unauthorized Access means any action that operates an Access Controlled Computer by either (i) inputting an identification code (shikibetsu-fugou) (e.g., password and ID) allocated to a user who is authorized to access the Access Controlled Computer, without the permission of the Access Administrator or the Authorized User, or (ii) inputting any information (other than an identification code) or command that enables that person to evade control (e.g., cyber attack of a security flaw), without the permission of the Access Administrator (UCAL, Article 2, Paragraph 4)

The UCAL prohibits the following actions:

- i. Unauthorized Access (Article 3);
- ii. Obtaining the identification code of an Authorized User to make Unauthorized Access (Article 4);
- iii. Providing the identification code of an Authorized User to a third party other than the Access Administrator or the Authorized User (Article 5);
- iv. . Keeping the identification code of an Authorized User that was obtained illegally to make Unauthorized Access (Article 6); and
- v. Impersonating the Access Administrator or causing a false impression of being the Access Administrator by: (a) setting up a website where a fake Access Administrator requests an Authorized User to input his/her identification code; or (b) sending an email where a fake Access Administrator requests an Authorized User to input his/her identification code (Article 7).¹⁴³

The maximum sentence in case of breaching the requirements of the article (i) of Article 3 is three years in jail or fine in one million Japanese yen (JPY) (Article 11). The fines applicable to the breach of items (ii) to (v) above (Articles 4 to 7) may be a fine of up to JPY 500,000 or a one-year prison term (Article 12).

¹⁴³ Turkey’s Law No. 5651 on Internet Crimes and Cyber security Measures, 2023.

Article 13 makes the offender pay a fine of up to JPY 300,000 in case they are not aware that the recipient will utilize the Unauthorized Access identifying number (iii) (Article 5)

B. Penal Code Provides for Criminal Sanctions

The Penal Code provides for criminal sanctions on the creation and provision of “Improper Command Records”, which give improper commands, such as a computer virus, to a computer. Improper Command Records mean (i) electromagnetic records that give a computer an improper command that causes the computer to be operated against the operator’s intentions or to fail to be operated in accordance with the operator’s intentions, and (ii) electromagnetic or other records that describe such improper commands.

A person can face up to three years in prison or a fine of up to JPY 500,000 if they are found guilty of creating or providing Improper Command Records without a valid reason, or if they intentionally infect or try to infect a computer with these records (Article 168- 2). A fine of up to JPY 300,000 or imprisonment of up to two years may be imposed on anyone found guilty of obtaining or maintaining improper command records with the intent to carry out the aforementioned activities (Article 168-3). In addition, the Penal Code provides for the following additional penalties:

- i. Any person who obstructs the business of another by causing a computer used in that business to be operated against the operator’s intentions, or to fail to be operated in accordance with the operator’s intentions, by (a) damaging that computer or any electromagnetic record used by that computer, or (b) giving false information or an improper command to the computer, is subject to imprisonment of up to five years or a fine of up to JPY 1 million (Article 234-2);
- ii. Any person who gains or attempts to gain, or causes or attempts to cause a third party to gain, illegal financial benefits by: (a) creating false electromagnetic records by giving false information or an improper command to a computer; or (b) providing false electromagnetic records

for processing by a third party, in either case, in connection with a gain, a loss or a change regarding financial benefits, is subject to imprisonment of up to 10 years (Article 246-2); and

- iii. Any person who creates, provides or attempts to provide electromagnetic records for the purpose of causing a third party to mistakenly administer matters that relate to rights, obligations or proofs of facts is subject to imprisonment of up to five years or a fine of up to JPY 500,000. However, if the act relates to records to be made by public authorities or public servants, the penalty is imprisonment of up to 10 years or a fine of up to JPY 1 million (Article 161-2).¹⁴⁴

Hacking-

Hacking is Unauthorized Access under the UCAL, punishable by imprisonment of up to three years or a fine of up to JPY 1 million. If the hacking is made through Improper Command Records, it is also punishable under the Penal Code (please see question 1.1, point 1, (B)). In addition, if a business is obstructed by such hacking, the crime is punishable by imprisonment of up to five years or a fine of up to JPY 1 million (Penal Code, Article 234-2)

Denial-of-service attacks- These carry the same penalties as hacking

Phishing- Article 7 of the UCAL prohibits phishing, while Article 4 of the UCAL prohibits obtaining any identification code through phishing. These actions are punishable by imprisonment of up to one year or a fine of up to JPY 500,000 (Article 12). In addition, any person who gains illegal benefits by using identification codes obtained by phishing is subject to imprisonment of up to 10 years under Article 246-2 of the Penal Code.

Infection of IT systems with malware- This is an equivalent punishment to hacking. In a major criminal case, the Supreme Court on 20 January 2022 acquitted a website administrator who installed a program to mine cryptocurrency on his site without notifying the visitors to the site. The code enabled

¹⁴⁴ “Digital Financial Frauds: A Comparative Study in the EU and USA”, International Finance and Cybersecurity Journal, 2023

the administrator to mine crypto currency into the computers of the visitors without their awareness. The lower court found him guilty and subject to Article 168-3 of the Penal Code, he was accused of maintaining electronic records containing unauthorized commands and to wit that such a program was unlawful he had to act against the will of the users and that he must have a socially objectionable program. The application of the program was not within the intention of the users in this case and misused the computer resources of the users, nevertheless, it was not socially permissible and compared it to the Supreme. to pop-up advertisements, which are displayed on the websites without consent of the users.¹⁴⁵

Distribution, sale or offering for sale of hardware, software or other tools used to commit cyber crime

It is a crime or fine of up to JPY 500,000 (Penal Code, Article 168-2) to give Improper Command Records (see above) to any third party without a valid reason, although there is no general prohibition on the distribution, sale or provision of tools that might be used to commit cyber crime..

Generally, if a person provides hardware, software or other tools knowing that those tools will be used for Unauthorized Access (see above) or to infect a computer with Improper Command Records, that person will be an accessory to these crimes. However, the Supreme Court has taken a relatively modest approach in punishing providers of software that can be used for either legitimate or illegal purposes. The Supreme Court on 19 December 2011 acquitted a developer of a P2P software that could be and actually was used for copyright violation, saying that a software provider may be punished as an accessory only if he knew that the software will be used for a specific criminal act or mostly for criminal acts. In this case, the court found that since the developer constantly warned users not to use the software in violation of any copy right, it wa

¹⁴⁵ Mexico's Federal Law on Cyber Crime and Data Protection, Government of Mexico, 2022.

difficult to attribute knowledge to the developer.¹⁴⁶

Possession or use of hardware, software or other tools used to commit cyber

One can face a fine of up to JPY 300,000 or two years in prison for obtaining or retaining improper command records with the intent to use them. 300,000 (Penal Code, Article 168-3). As an example, nine people were prosecuted for uploading software that contained a computer virus to an online storage system and infected the computers of people who accessed the storage and downloaded the software from September to December 2016.

Electronic theft- Besides the criminal sanctions that may be imposed on phishing, electronic theft is punished in the Unfair Competition Prevention Act, which includes Unauthorized Access. (a) employee: (a) obtains a trade secret of an employer through theft, fraud, threat or other illegal acts (the “Illegal Actions”) or (b) uses or discloses a trade secret of the employer through the use of the Illegitimate actions, to obtain wrongful benefits or to harm the owner of the trade secret, imprisonment of up to 10 years, or a fine of up to Also, in case that employee has committed any of the above outside Japan, the fine will be raised to a value up to JPY 30 million (Article 21, Paragraph 3). If you want to let someone else download films or music electronically.

Without the owner's consent, you might face up to 10 years in prison or a fine of up to JPY 10 million, or both, according to the Copyright Act (Article 119, Paragraph 1). In addition, it is stated in Article 119, Paragraph 3 that anyone who is aware of copyright protection and downloads electronic data that is protected by another person might face a fine of up to JPY 2 million, two years in prison, or both. Article 120-2 also states that a fine of up to JPY 3 million or three years in prison may be imposed on anyone caught selling, lending, manufacturing, importing, holding, or uploading any program or device that can remove, disable, or alter copyright protection technology (e.g., copy protection code).

¹⁴⁶ “Cyber Espionage and National Security: Case Studies from China and the USA”, Harvard Cyber Law Review, 2022.

Unsolicited Penetration Testing

Since there is no exemption for this type of testing, unsolicited penetration testing is punishable as Unauthorized Access. Vulnerability testing without permission is generally not allowed. However, the National Institute of Information and Communications Technology (the “NICT”) (and only the NICT) is allowed to conduct vulnerability testing without permission under the Law on the National Institute of Information and Communication Technology, which exempts the NICT from the prohibition against Unauthorized Access

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data This carries the same penalties as electronic theft.

The above-mentioned offences have extraterritorial application -The UCAL provides for the extraterritorial application of Articles 3, 4, 5 (except where the offender did not know the recipient’s purpose) and 6 of the UCAL (Article 14). The Penal Code also has extraterritorial application (Article 4-2). There are any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences(Eg. where the offence involves “ethical hacking”, with no intent to cause damage or make a financial gain)?

The above-mentioned offences are not subject to exceptions such as “ethical hacking” or lack of intention to cause damage or make financial gains. As discussed above , vulnerability testing without permission may be conducted only by the NICT based on a special law, and there are no general exceptions to similar activities for other persons.

Cyber security Laws

Applicable Laws: Please cite any Applicable Laws in your jurisdiction relevant to cyber security, such as the law relevant in the monitoring, detection, prevention, mitigation and management of Incidents. It can be such as, among

others, the law of data breach notification, the law of confidentiality, and the law of information security among others. In addition to the UCAL, the Penal Code and the Unfair Competition Prevention Act described above, the following laws are also applicable to cyber security.

A. Basic Act on Cyber security (the “BAC”)

This provides the basic framework for the responsibilities and policies of the national and local governments to enhance cyber security. In September 2021, pursuant to the BAC, the Japanese government issued the Cyber security Strategy (drafted by the Cyber security Strategy Headquarters (the “CSHQ”) and established under Article 25 of the BAC to promote Japan’s cyber security measures, and its secretariat, the National Center of Incident Readiness and Strategy for Cyber security (the “NISC”).

Furthermore, the BAC obligates operators of critical infrastructure to make efforts to voluntarily and proactively enhance cyber security, and to cooperate with the national and local governments to promote measures to enhance cyber security. In December 2018, the BAC was amended to establish the cyber security council (the “Cyber security Council”). The Cyber security Council is intended to be the avenue to allow national and local governmental authorities and business operators to share information that may facilitate the proposal and implementation of cyber security measures.

B. Tele communication Business Act(the “TBA”)

One provision of the TBA states that a telecommunications carrier must not violate the confidentiality of any communications in transit. Another provision states that an individual involved in the telecommunications industry must not reveal any trade secrets acquired during their employment, with regard to any communications in transit, even after leaving their position.

The confidentiality of communications safeguards not just the messages themselves but also any information that might lead someone to deduce their meaning. Thus, the confidentiality of communications safeguards information

contained in access logs and IP addresses. If a telecom provider knowingly acquires information that is protected by the secrecy of interaction, shares this information with unauthorized individuals, or uses it for their own benefit, they are in violation of this law exchanged messages, the telecom company is in violation of Article 4 (1).

It would be beneficial for telecommunications companies to gather data on cyber attacks, such as access records of compromised devices, and share it with other telecommunications companies or government agencies in order to combat cyber attacks. But the TBA doesn't say anything about how a telecom company can handle intrusions legally (1). In 2014, 2015, 2018, and 2021, the Ministry of Internal Affairs and Communications (the “MIC”)—the main government body in charge of carrying out the TBA—released reports discussing the possibility of cyber attacks on telecom carriers and problems related to communication secrecy.

The Council for the Secure Use of the Internet published recommendations on cyber attacks and communication secrecy (the “Guidelines”), which incorporate the results and details of the MIC's four studies. This Council is made up of five associations: the Japan Cable and Telecommunications Association, the Japan Internet Providers Association, the Japan Telecom Services Association, the Telecommunications Carriers Association, and the ICT Information Sharing and Analysis Centre Japan (the “ICT-ISAC Japan”). Although the Guidelines do not have the force of law, they are highly respected due to the fact that the MIC validated them prior to their release.¹⁴⁷

Furthermore, in 2013, the MIC started a project called ACTIVE (Advanced Cyber Threats response Initiative) that aims to protect internet users from cyber attacks by collaborating with ISPs and IT systems vendors. To prevent computer virus infections, ISPs that are members of ACTIVE may warn users or block communications in accordance with the Guidelines. In addition, in

¹⁴⁷ South Africa's Cyber crime Act, 2021, and Implementation Report, 2023.

May 2018, the TBA was amended to introduce a new mechanism that enables a telecommunications carrier to share with other carriers information on transmission sources of cyber attacks through an association confirmed by the MIC as being eligible to assist telecommunications carriers. After the amendments became effective in November 2018, the MIC confirmed the ICT-ISAC Japan to be that association in January 2019.

C. Act on the Protection of Personal Information (the “APPI”)

The APPI is the principal data protection legislation in Japan. It is the APPI’s basic principle that the cautious handling of “Personal Information” under the principle of respect for individuals will promote the proper handling of Personal Information. Personal Information means information about specific living individuals that can identify them by name, date of birth or other descriptions contained in the information (including information that will allow easy reference to other information, which may enable individual identification) (Article 2, Paragraph 1). A business operator handling Personal Information may not disclose or provide Personal Information without obtaining the subject’s consent, unless certain conditions are met.¹⁴⁸

In order to reduce the likelihood of cyber attacks, it would be beneficial for business owners to gather data about these assaults (such as access records from compromised equipment) and share it with other business owners or government agencies. If the data contains personally identifiable information (PII), however, it must adhere to the APPI’s regulations on the collection, use, and sharing of such data. Any incident involving the leakage, loss, or loss of personal data must be reported to the Data Protection Commission (“PPC”) and the data subjects must be notified under the APPI. (defined in the APPI) that it handles, if certain conditions are met (Article 26)

¹⁴⁸ “Block chain and Cyber Security: Comparative Trends in the USA, EU, and Asia”, MIT Technology Review, 2022.

D. The Japanese Foreign Exchange and Foreign Trade Act (the “FEFTA”)

The FEFTA regulates the export of sensitive goods and technologies, including encryption software and hardware , as well as inward direct investments such as acquisition of shares in Japanese companies by non-Japanese investors. From the viewpoint of national security, prior notification to the Ministry of Finance and other competent authorities will be required for an acquisition of 1% or more of shares in a Japanese company that engages in information technologies, software, and telecommunications businesses, unless an exemption is applicable, and the foregoing authorities may order the cessation of the acquisition.

E. New Security Clearance Legislation

A new security clearance legislation that will apply not only to the public sector but also to private companies and employees having access to sensitive information is under discussion, since the current Specified Secrets Protection Act only applies to the public sector. In June 2023, the Expert Committee on Security Clearance System for Economic Security published an interim report that discusses the breadth of the sensitive data that needs to be safeguarded, any necessary security clearance screening, and any other relevant issues. In 2024, the new law is anticipated to be passed.¹⁴⁹

Critical or essential infrastructure and services: there is legislation that mandates certain measures for cyber security (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in jurisdiction.

The UCAL requires Access Administrators to make efforts to manage the identification codes of Authorized Users, examine the validity of functions to control access to the Access Controlled Computer and implement necessary measures, including enhancing functions (e.g., encryption of codes, definite deletion of codes that have not been used for a long time, implementing a batch

¹⁴⁹ Argentina’s Cyber security Framework and Digital Crime Analysis, Ministry of Justice, 2023.

program to address a security flaw, program updates, and appointing an officer for network security) (Article 8).

The so-called “Critical Information Infrastructure Operators” are required to make efforts to deepen their interest and understanding of the importance of cyber security, and to voluntarily and proactively ensure cyber security purpose of providing services in a stable and appropriate manner (BAC, Article 6). Article 3(1) of the BAC defines Critical Information Infrastructure Operators as operators of businesses that provide an infrastructure that is a foundation of people’s lives and economic activities that could be enormously impacted by the functional failure or deterioration of that infrastructure. The CSHQ formulated the Cyber security Policy for Critical Infrastructure Protection as a non-mandatory guideline that designated critical infrastructure areas under its coverage. These areas are information and communication, financial services, aviation, airports, railways, electric power, gas supply, government and administrative supply, medical, water, logistics, chemical, credit card, and petroleum.

The Further, the Act on the Promotion of National Security through Integrated Economic Measures, which was promulgated on 18 May 2022, will introduce new requirements applicable to essential infrastructure services. In order to prevent essential facilities from external interference, including cyber attacks, specified essential infrastructure providers will be required to submit a certain plan to the competent government ministry for review before they install certain essential facilities or outsource the maintenance or management of certain essential facilities. Depending on the results of the review, the ministry may recommend that the specified essential infrastructure providers change or discontinue the plan or take risk-reduction measures. If the specified essential infrastructure providers do not follow the recommendation, the ministry may issue an order to them to take necessary measures. These new requirements will be applied to essential infrastructure areas, namely electric power, gas supply, petroleum, water, railways, motor freight, ocean freight, aviation, airports, telecommunications, broadcasting, postal services, financial services, and credit

cards, which mostly overlap with the sectors subject to the BAC but do not include the medical sector.¹⁵⁰

4.6 CYBER LAWS IN BANGLADESH

Changes in the Nature of Cyber Crimes

Please provide a detailed account of the chronological development and progression of cyber crimes. It is imperative to comprehend the manner in which technological advancements have engendered the emergence of novel manifestations of digital threats, thereby mandating the creation of resilient legal frameworks to effectively confront and redress such perils.

Cyber Crimes Laws in Bangladesh :A Legal Frame work

To expound upon the various legal measures available to combat cyber crimes. Kindly allow me to elucidate the legal provisions pertaining to cyber laws in the jurisdiction of Bangladesh, with a focus on comprehending the intricate structure of the legislative framework designed to effectively counteract an array of digital offenses.¹⁵¹

Cyber Crimes Types

Through the intricate terrain of various cyber offenses. In light of the myriad digital offenses that individuals and businesses may encounter, it is imperative to delve into the diverse manifestations of such transgressions, ranging from hacking and identity theft to online fraud and cyber bullying

Prevention and Cyber security

It is imperative to emphasize that the proactive implementation of preventive measures is of utmost importance. Please allow me to elucidate the various precautionary measures and cyber security strategies that both individuals and organizations can implement in order to bolster their digital fortifications against the perils of cyber threats.

¹⁵⁰ "AI in Cyber Crime Prevention: A Global Perspective", Journal of Artificial Intelligence and Cyber security, 2022

¹⁵¹ "Big Tech and Cyber security Regulations: Comparing EU, USA, and China", Stanford Law Review, 2023.

Cyber Crimes Investigation

In the process of investigating cyber crimes, that it is crucial to comprehend the formidable obstacles encountered by law enforcement agencies when endeavoring to trace digital footprints and amass evidentiary material for the purpose of prosecuting individuals involved in cyber criminal activities.

Reporting Cyber Crimes

The act of reporting is of utmost importance in facilitating expeditious and decisive measures. Please be advised that we shall now proceed to elucidate the mechanisms pertaining to the reporting of cyber crimes within the jurisdiction of Bangladesh. Our objective is to provide comprehensive knowledge on this matter, thereby enabling both individuals and businesses to assume an active and participatory role in the relentless fight against digital threats.

E-Commerce and Cyber laws

In the realm of the digital marketplace, it is imperative to acknowledge that the practice of electronic commerce, commonly referred to as e-commerce, is susceptible to various forms of unlawful activities commonly known as cyber crimes. Please allow me to elucidate the manner in which the cyber laws in Bangladesh have been meticulously crafted with the specific intention of safeguarding the interests of online enterprises and individuals partaking in electronic transactions International.

Cyber Law Collaboration

The issue at hand pertains to the transcendence of cyber threats across international borders. Please allow me to delve into the intricate dynamics of the collaborative endeavors undertaken by Bangladesh and the esteemed international community in order to effectively combat the pernicious menace of cyber crimes. These efforts are primarily centered around the exchange of vital intelligence, the pooling of expertise, and the establishment of a robust

framework for legal cooperation.¹⁵²

Cyber law Enforcement Issues

Not with standing the existence of legal frameworks, the enforcement there of encounters various challenges. Upon careful examination, it is imperative to acknowledge the various hurdles that arise in the enforcement of cyber laws. These hurdles encompass jurisdictional issues, the ever-evolving nature of technologies, and the remarkable adaptability demonstrated by cyber criminals.

Recent changes and developments

It is imperative that you remain informed and up-to-date with the latest developments in the legal field. Please be advised that we shall now proceed to examine the recent amendments and developments in cyber laws within the jurisdiction of Bangladesh, with a specific focus on elucidating the steadfast dedication of the government in proactively addressing and mitigating emerging digital threats.

Cyber Education and Awareness

Education, being a formidable shield, holds considerable efficacy in safeguarding one's interests. Please acquaint yourself with the various endeavors aimed at fostering cyber awareness and education, which serve to equip both individuals and enterprises with the requisite understanding to navigate the digital realm in a secure manner.

Case Studies : Cyber crime Prevention Success

An analysis of case studies that exemplify efficacious cyber crime prevention initiatives in Bangladesh. Please be advised that it is imperative to comprehend the manner in which collaborative endeavors have yielded concrete outcomes in the realm of mitigating digital threats.

¹⁵² "Big Tech and Cyber security Regulations: Comparing EU, USA, and China", Stanford Law Review, 2023.

Future Cyber Law Trends

In consideration of the subject matter at hand, namely the future of cyber laws, it is imperative to engage in a comprehensive analysis of the prevailing legal landscape in order to ascertain potential developments and trends that may arise in the foreseeable future. By virtue of this exercise, one may endeavor to anticipate the trajectory of Please be advised that we shall now delve into the examination of nascent patterns and advancements that are poised to influence the realm of cyber legislation within the jurisdiction of Bangladesh. Our objective is to guarantee a forward-thinking methodology towards the safeguarding of digital assets and the preservation of online security.

Conclusion

In summation, as the nation of Bangladesh wholeheartedly embraces the advent of the digital age, the imperative nature of combating cyber crimes is amplified to an unprecedented degree. The synergistic endeavors undertaken by the government, law enforcement agencies, commercial enterprises, and private citizens are of paramount importance in the establishment and maintenance of a robust digital milieu. Through the act of remaining duly informed, diligently implementing preventive measures, and providing steadfast support to ongoing initiatives, Bangladesh possesses the ability to persistently strengthen its defenses against the ever-evolving cyber threats, thereby ensuring the preservation and protection of the digital future of the nation.¹⁵³

4.7 CYBER CRIME LAWS IN NEPAL

Crimes perpetrated via or in connection with computer systems or networks are collectively known as cyber crimes. This includes crimes like unlawful data possession or distribution. An online crime is a crime perpetrated using the internet. Incidents of Cyber crime and Online Crime: Gaining comprehension: Another type of cyber crime is gaining unauthorized access to someone else's computer and then either deleting or endangering the data on that computer, or even destroying it physically. In particular, the internet is a

¹⁵³ "Children and Cyber Crime: Legal Protection in Different Nations", UNICEF Cyber Safety Report, 2022.

necessary component of online crime (e.g., hacking, phishing, spamming, E-mail bombing, etc.). *cyber crime also refers to crimes committed on the internet.

1. This is cyber crime

When there is the presence of the following:

- Illegal act
- Using computer With or without internet
- Must have mala fide intention
- The harm caused to the property or life of the person.

2 The elements of cyber crime

To prove one act as cyber crime: it requires the following elements:

- Actus Reus (physical element)
- Mens Rea(mental element)
- Modus Operandi(computer,internet)

The emerging trending cyber crime

- Phishing Bot net attacks(robot)
- Voice over IP communication
- Cloud computing Not only methods but impacts also changed.

The major cyber crimes in Nepal

- IP theft and privacy
- Photo mutilation
- Imposter Email
- fraud for ransom
- Pornography
- Cyber bullying
- Forgery
- Online gambling

- Child trafficking
- Sex texting, sex tortion, etc.

The legal provisions of cyber crime in Nepal

In Nepal, the Nepal Police have been using the Electronic Transactions Act 2063 (Hereafter referred ETA) in order to control cyber crimes. The most common provision of the Act used to combat cyber crime in Nepal is Section 47. According to this part, whomever uses a computer, the internet, or any other form of electronic media to publish or exhibit content that is offensive, immoral, hateful, or malicious is guilty may face up to five years in prison, a fine of one million rupees, or both Section 48 Commonly used as well, this section of the Act states that whoever, while exercising the authority granted by this Act or the Rules framed hereunder, discloses or causes to disclose the confidentiality of any record, book, register, mail, it information, document, or material to an unauthorized person faces a punishment of up to two years in prison, a fine of up to ten thousand rupees, or both, depending on the seriousness of the offence

The punishment provisioned by the law of Nepal relating to pirating, destroying, or altering computer source data

As per the ETA, 2063 (section 44), Someone can face up to three years in prison or a fine of up to two hundred thousand Rupees, or both, if they intentionally or negligently steal, damage, or alter computer source code that is meant for use by any computer, machines programmer, computer system, or computer network.

The Unauthorized access to computer materials, as a cyber crime

Not Authorized The law makes it clear that access is a crime. A person may be punished with a fine of up to 200,000 rupees or jail time of up to three years, or both, depending on the gravity of the crime, if they gain access to any program, information, or data on a computer without the owner's or responsible party's permission, or if they act contrary to the original authorization.[Section 45, ETA 2063]

The provisions regarding damage to any computer and information system

Someone can be punished with a fine of up to 2,000 Rupees and/or three years in prison, or both, if they intentionally damage, delete, alter, disrupt, or knowingly cause any institution to suffer wrongful loss or damage by destroying, damaging, or diluting the value or utility of any information stored in a computer system[Section 46, ETA 2063]

The publication of illegal materials in electronic form allowed as Cyber Crime

No, that's wrong. The punishment for publishing or displaying illegal, immoral, or otherwise objectionable material on electronic media, such as computers or the internet, can include a fine of up to 100,000 Rupees or up to five years in prison, or both. The material in question must not incite hatred or jealousy towards any individual or group, or threaten the peace and harmony that exists among India's many diverse ethnic groups and communities [Section 47, ETA 2063]

The provisions of the law of Nepal regarding computer fraud

In the event that someone makes, posts, or otherwise gives out a digital signature certificate with the intent to commit fraud or any other illegal act, or gains financial gain from the payment of any bill, balance amount of any account, inventory, or ATM card through fraud, the victim will receive the money back from the offender. The offender faces a punishment of up to two years in prison, a fine of up to 100,000 Rupees, or both [Section 52, ETA2063]

The punishment for a person who abets others to commit a computer related offense

Anyone who conspires with another to commit a computer-related offence under the ETA Act or who attempts to commit such an offence faces a punishment of up to six months in prison or a fine of up to 50,000 Rupees, or both, depending on the seriousness of the offence [Section 53, ETA 2063]

The punishment for an offence committed outside Nepal

Even though the offender is physically located outside of Nepal, they may still be subject to prosecution and punishment under the ETA Act if they conduct an offence involving a computer, machine, or machines network system in Nepal [Section 55, ETA 2063]

4.8 CYBER CRIME LAWS IN VIETNAM

We came across this great opinion piece that sheds light on the insider sentiments on the A.I. race and hype. The alarm bells are sounding from the inside and for good reason. The author, Ezra Klein, acknowledges the complexity of the regulatory landscape and emphasizes the need for ongoing discussions and collaborations among policymakers, researchers, and industry experts. Read this condensed version to be in the know.



In order the international community to further align its policies with standards and personal data protection best practices, the Vietnamese authorities have recently released a significant Decree covering key elements on data security. The contents of the Decree may apply to a vast number of businesses active in or doing business with Vietnam, thus we advise international investors to peruse it carefully and take necessary actions to comply with its requirements.¹⁵⁴

¹⁵⁴ “Emerging Trends in Ransomware Attacks Across Continents”, Cybersecurity Ventures Annual Report, 2023

From the release of the 2018 Law on Cyber security, the guiding Decree of this law, Decree was finally promulgated on 15th of August 2022, and is dated effective as of 1st of October 2022. In the following article, we seek to delineate specific components of the Decree which relate to investors and enterprises doing business in Vietnam, offering practical insights and interpretations.

The National Socialist Republic of Vietnam assembly passes the cyber security law in 2018. The pursuant to the constitution of socialist republic of Vietnam. The National Assembly promulgates the Cyber Security Law. This law is divided to chapter 1 to 7 and the chapter 1 specific general provisions like article 1 the scope– 6 This law provides for protection of national security and public order in cyber space; responsibility of relevant organizations and individuals.

Article 2 definitions for the purpose of this document, the terms below are construed as follows like cyber security– means assurance that activities in cyber space do not harm national security, public order, the lawful rights and interests of any organization or individual. “cyber security protection” includes prevention, discovery, and actions against violations of cyber security. “cyber space” means a network of information technology (IT) infrastructure which includes telecommunications network, the Internet, computer network, communication systems, information processing and control systems, databases; cyber space is where people’s activities are not limited by space and time and other word also define according to law.

The article 3 state policies on cyber security.

Give priority to assurance of cyber security in national defense and security, socio-economic development, science and technology development and diplomacy. Develop health cyber space without jeopardizing national security, public order or the lawful rights and interests of any organization or individual. Prioritize resources for development of a professional cyber security force; improve capacity of the cyber security force and any organization or individual that participate in cyber security protection; prioritize investment in research and

development of cyber security technology. Encourage and enable other organizations and individuals to participate in cyber security protection, handle cyber security threats; research and develop cyber security protection technologies, products, services and applications; cooperate with competent authorities in cyber security protection. Increase international cooperation in cyber security.

Article 4. Cyber security protection principles,

Article 5. Cyber security protection measures

Article 6. Protection of national cyber space,

Article 7. International cooperation in cyber security,

Article 8. Prohibited acts,

Article 9. Actions against violations against regulations of law on cyber security,

Chapter II Cyber security of National Security Information Systems

Article 10. National security information systems,

Article 11. Appraisal of cyber security of national security information systems,

Article 12. Assessment of cyber security of national security information systems,

Article 13. Inspection of cyber security of national security information systems,

Article 14. Supervision of cyber security of national security information systems,

Article 15. Response and remediation of cyber security incidents occurring to National security information systems, Chapter III Prevention and Actions Against Cyber security Violations,

Article 16. Prevention and handling of cyber information that is meant to oppose the government of Socialist Republic of Vietnam, cause riots, disturb the peace, humiliate or slander, or violate economic management laws,

Article 17. Prevention and response to cyber espionage; protection of state secret

information, business secrets, family secrets and privacy in cyber space,

Article 18. Prevention and response to use of cyber space, information technology or electronic devices for violations of regulations of law on national security and public order,

Article 19. Prevention and response to cyber attacks,

Article 20. Prevention and response to cyber terrorism,

Article 21. Prevention and response to cyber security emergencies,

Article 22. Cyber security protection activities,

Chapter IV Cyber Security Protection Activities,

Article 23. Cyber security protection in central and local authorities and political organizations,

Article 24. Inspection of cyber security of information systems other than national security information systems,

Article 25. Protection of cyber security of national cyber space infrastructure and international internet gateways,

Article 26. Assurance of information security in cyber space,

Article 27. Cyber security research and development,

Article 28. Improvement of cyber security independence,

Article 29. Protection of children in cyber space,

Chapter V Assurance of Cyber security Protection,

Article 30. Cyber security forces,

Article 31. Assurance of human resources for cyber security protection,

Article 32. Recruitment, training and development of cyber security forces,

Article 33. Cyber security training,

Article 34. Dissemination of cyber security knowledge

Article 35. Cyber security protection funding,

This Law is passed by the 14th National Assembly of Socialist Republic of Vietnam on June 12, 2018 during its fifth session. Recently Central Government of India Hon'ble Prime Minister Shri Narendra Modi & Vietnam's P.M. contact to short out the very important issue tourism and cyber security. his is a very important point out by Central Government. The Crime Ratio day-to-day increase at present time so this step taken by Government. The Indian System may be strong after this contact. Being a researcher I hope some problem short out after some time.¹⁵⁵

¹⁵⁵ Interpol, "Cyber Crime Trends Across Nations", 2023.

CHAPTER–V

JUDICIAL INTERPRETATION IN CYBER CRIME

“Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire; it wafts across the electrified borders.”-Ronald Reagan.

The cyber crimes of the new age and provide insights into the latest trends and techniques used by cyber criminals. Through a series of case studies and real- world examples, deliberation will be on various types of cyber crime, including questions around privacy, admissibility of digital evidence, method of investigation, surveillance, and the balance between security and civil liberties. Ultimately, our goal is to provide readers with a comprehensive understanding of the complex and ever-evolving landscape of cyber crime in the new age.¹⁵⁶

The thesis begins with some earlier judgments on cyber crimes after the inception of Information Technology Act, 2000. It further exploring the various types of cyber crimes and admissibility of digital evidence in court. The cases presented in this thesis cover a wide range of cyber crimes, including financial fraud, ransom ware attacks, cyber stalking, and even state-sponsored cyber espionage. Each case is analyzed in detail, providing insights into the act used by cyber criminals and the measures that were taken to prevent or mitigate the damage caused by these crimes. Through the analysis of these cases, this book aims to provide readers with cyber crime, interpretation of court on various issues.

A greater understanding of the By examining these real- world incidents, 8 nature and scope of readers will gain valuable insights into the tactics used by cyber criminal, and will be better equipped to protect themselves and their organizations from these growing threats. By compiling these real world cases, we want to contribute our beat to our law fraternity include advocates, judges, law teachers, law students & law enforcement agency. We believe that by sharing

¹⁵⁶ National crime records bureau –ministry of home affairs ,crime in india -2023 compendium

these case compilation work, with all major stake holder to deliver more clarity and understanding on importance or cyber crime investigation, Importance of collection, preservation and production of digital evidence in court for admissibility and to increase convictions rate of cyber crimes case in India.

5.1 JUDGMENT IN BRIEF

High Court Judgment

R.M. Malkani v. State of Maharastra¹⁵⁷

In its analysis of the case, the High Court held that the police officers intercepted the phone call made by the appellant, Dr. Morwani, which was against section 25 of the Indian Telegraph Act. Although the telegraph act was violated, the high court had to rule that the audio recording could be used as evidence. The tape recorder in this case was linked to the telephone by the police officer under the direction of Dr. Morwani. One cannot say that the police officer overheard a message that fell under section 25 since they did not listen to a conversation that Dr. Morwani was having but recorded it through a device. The Indian Telegraph Act 25 makes it specific that the crime in question is damaging, removing, tampering with or touching a battery line or post to intercept signals or being aware that one has damaged, removed, or touched any equipment. In the process of phone conversation, someone can record or eavesdrop into the conversation. One can not say that the other party who has the right to so do is damaging, removing, tampering, touching or intercepting or getting acquainted with the contents of any machinery battery line or post.

Supreme Court Judgment

The appellant was represented in court by a lawyer who alleged that the recording of the conversation was done in an illegal manner. The law suit states that the illegal action was against Indian Telegraph Act section 25. Considering the prevailing situation, it has not violated the section 25.case of the Telegraph Act. Evidence may still be relevant even whereby it was gathered unlawfully. An

¹⁵⁷ AIR1973SC157CriLJ228

English case over a hundred years old said that, had it been held, the evidence found on an unlawful search of the pockets of the appellant could not be used against him in a criminal prosecution. This was because the search was undertaken by a constable.

A tape recording of a conversation that goes unobserved by the people having it can become significant and admissible⁸ in the same way that a photograph taken of someone without their knowledge does. The admission of such evidence will be subject to twofold scrutiny by the court. It must be authentic and undamaged before the Court may accept it. Second, the Court has the authority to ensure that the Police act with the utmost integrity. The fact that a judge is more inclined to consider the officer with caution and care if he acts appropriately while obtaining evidence, and vice versa. Consideration of the relevant facts and circumstances is essential when making any determination on the accused's status, the investigation's focus, and the seriousness of crime.

Where a Court is authorizing a tape recording to be recited to it is acting on real evidence provided it is acting on the intonation of the words that are intoned to be real and genuine. The Court also has in mind the fact that tape recorded conversation can be altered when receiving it as evidence. The tape-recording of the conversation between Dr. Morwani and the Appellant can not be described as illegal in the current case since Dr. Morwani did not object to the placement of the tape-recording device to his instrument. On the contrary, Dr. Morwani allowed the Police Officers to listen to the conversation. In case the dialogue was transmitted via a microphone or an amplifier over the telephone, and the police officers overheard the identical conversation, it would enable them to provide first-hand testimony of what they had heard. This was direct evidence by the police officers of what they viewed and what they did what they documented due to voluntary permission granted by Dr. Morwani. The recorded discussion is a relevant contemporaneous evidence which is thus admissible. It is not contaminated by pressure and injustice. This evidence should not be left out.

There was also an argument that the evidence that was recorded contravened the Indian Constitution which do not imply the admission. the argument that was raised was that the appellant was involved because there was the legal process. for obtaining followed. The speech of the appellant was not coerced. It was not at all pressurized. The appellant was not aware that the recording machine was attached to tape the conversation. It does not make a difference whether the conversational evidence is admissible or not. The statement of the appellant was neither coerced nor forced. Some sort of a mechanical machine was employed to play a deaf man in the bushes in case the conversation was recorded on tape.

It would be admissible in evidence no matter the way it was acquired, as it was in the case of **R. v Lathan**¹⁵⁸. Any evidence obtained illegally does not nullify it provided it lacks a reasonable confession of guilt. The evidence does not support the possibility of the appellant being pressured into confessing his guilt. In their conversation, both parties had no evidence on the appellant. Nobody coerced him into speaking and confeding anything. Article 21 was referred to by submitting that, the privacy of the conversation of the appellant was considered to deprivation of life or liberty. Courts will ensure the telephonic conversation of an innocent citizen will not be interfered with wrongfully or in high handed manner by tapping the conversation. It does not protect the guilty citizen against the attempts of the police to purify the law and avoid the corruption of public servants. This should not be interpreted to mean that the Courts will allow the protection of the citizen to be jeopardized by allowing the police to act by unlawful or irregular means. The current case does not have an illegal or improper means of getting the tape recording of the conversation.

Ziyouddin Burhanuddin Bukbari v. Brij Moban Ramdas Mehra & Ors.¹⁵⁹—

The audio recordings of talks categorized under Article 3 of the Indian Evidence Act are described as documents, that is, the Supreme Court concurs with the decision made by the High Court that the audio recording of the talks could be

¹⁵⁸ AIR 1976 1All ER

¹⁵⁹ AIR 1975 SC 1778: (1976) 2 SCC 17: SCR 453

used as evidence as long as it met some requirements. following conditions. speaking has to be identified by the person making the audio recording by others who know it. The maker of the record had to prove accuracy of what was actually recorded and also satisfactory evidence, direct or circumstantial evidence must exist to rule out chances of any tampering with the record. The subject-matter that was recorded had to be demonstrated as being relevant under rules of relevancy under the evidence act.

State of Maharashtra v. Dr. Praful B. Desai¹⁶⁰ – Video conferencing according to section 273 of the Criminal Procedure Code can never be employed to take evidence, and therefore, the Supreme Court has determined that evidence cannot be taken by video conferencing. The High Court, after referring to several dictionaries, made a conclusion that the presence of section 273 of the act means any real physical presence in court. The High Court made a decision in favour of this argument. The presence of evidence during the accused or otherwise does not matter, as ruled by the High Court, which has referred to numerous cases of previous High Courts on section 273 of the Criminal Procedure Code. In this regard, the ruling of the High Court is impeccable. Subsequently, the High Court reviewed the activity of foreign courts, primarily American courts. In Section 273, dispensation of personal attendance is made available. In this case, recording evidence may be attended by the pleader. On this basis, the pleader is said to have the Accused in his presence. Constructive presence is thus taken into account in section 273. This proves that it is not necessary to be physically present. This is to show that the appropriate word is presence. In this respect, does not imply presence physically. The literal meaning of section 273 does not give the narrow meaning in which the Respondent is trying to give the word presence.

The result of this is the rejection of the contested decision. Thereupon the Magistrate will proceed to video conference Dr. Greenberg to obtain his testimony. The case is pending we are asking determine it as early as you can,

¹⁶⁰ AIR 2003 SC 2053; (2003) 8 SCC 180; 2003 Cri LJ 2033

and preferably in a year. According to these guidelines, appeals are dismissed and further that the Respondent will compensate the State and the complainant the costs of these Appeals.

State of Tamil Nadu v. Subas Katti¹⁶¹ – Due to this fact, the evidence was still presented to the court despite all these objections. This was the same IP address occupied by the accused and the harasser. The defendant was testified against by an eyewitness, who was the owner of Cyber Café. Based on the evidence provided in court by experts and other pieces of evidence, the Additional Chief Metropolitan Magistrate convicted the defendants of the contravention of the provisions of section 469 and 509 of the Indian Penal Code and section 67 of the IT Act 2000 and. (Forgery intending to defame- 469 of the Indian Penal Code.) Words, gestures or acts that shall be offensive to the modesty of a woman are punishable by Section 509 of the Indian Penal Code. 67 of The Information Technology Act of 2000 (Sanctioning the dissemination of electronic content including sexually explicit acts etc.) The culprit is also convicted and a penalty is given to the crime committed. The section 509 amendments will impose a fine of Rs. 500 and 1-year S.I. (Simple Imprisonment) on him. As per the provision under sections 469 of the Indian Penal Code, he should also undergo two years of rigorous imprisonment. The violation of section 67 of the Information Technology Act, 2000 is punished by a fine of Rs, 4,000 reclusion in prison. The lag time between any of the phrases will be non-existent.

State (NCT of Delhi) v. Navjot Sandhu @ Afsan Guru¹⁶² – The Supreme Court has that Judgment of Special Court– Mohd. was charged on the Indian Penal Code and Evidence and Sentencing Act charges. Afzal, Shaukar Hussain and S.A.R. Gilani were convicted. Mohd Afzal and Shaukar Hussain were also charged with the POTa. The death sentences were against Mohd with a conviction under section 123. Afsal, Shukar, and Gelani were grounded on the section of the Indian penal Code 302, 120B of the same code, and section 3(2) of Pakistan Offenses Theft Act.

¹⁶¹ AIR 2004CC No 4680

¹⁶² 11 SCC 600: AIR 2005 SC 3820: (6) Scale 177: 2005 Cri LJ 3950

Decision of Division Bench of High Court– Mohd had death penalty served. Afzal Guru and Shaukar Hussain rejected their appeals against the decision of the special court by the High Court. The High Court granted the appeals of the other two defendants, namely, S.A.R. Gelani and Afsan Guru

Decision of Supreme Court– The Supreme Court, in the given case ruled that the acquittal of the competent witness on charges associated with the use of the computer when and how to take printouts was sufficient to prove the validity of the call records. Section 65B of the Evidence Act discusses the admissibility of electronic records but section 63 and section 65 of the Evidence Act does not outlaw the introduction of secondary evidence. Though the certificate containing the details stated in sub-section (4) of the section 65B may have not been filed in the case, that does not rule out the use of secondary evidence as it is within the legal parameters of the section 63 and 65. Mohd was rejected by judges R.M. Lodha, Kurian Joseph and R.F. Nariman of Supreme Court. Afzal was appealing and maintained his death penalty. On a partial appeal Shaukar was convicted of the Indian Penal Code and fined Rs. 25,000 and sentenced to 10 years in prison. The state denied its appeals against S.A.R. Gelani and Afsan Guru acquittal and the court ruled on as secondary evidence. Mohd. Afsal Guru was sentenced to death by the hanging gallows on February 9, 2013, when the president turned down his petition requesting mercy. The execution of Mohd was given the name Operation Three Scar. Afsal Guru.

P.R. Transport Agency v. Union of India¹⁶³– The Supreme Court would conclude that the petitioner would have received the acceptance of the respondents on the tender at his place of business, Varanasi or Chandauli, the sole places where he is physically present. The court proceeded to assert that the petitioner argument on the issue of the territorial jurisdiction was that since the petitioner obtained the acceptance of the tender through the e-mail service at Chandauli (U.P.) then the contract on which the dispute arose was fulfilled at Chandauli. The completion of the contract “cause of action in a case in which

¹⁶³ AIR 2006 All 23: (1) AWC 504

performance of the contract is sought, or in which there are assertions that the respondents have breached the contract. In this case, the location at which the contract was fulfilled through the acceptance communication being received is referred to as the place where the part of the cause of action appears. A contract is said to be final when the acceptance has been received, the court has cited Halsbury Laws of England, 4th edition and whether the parties negotiated the agreement either through phone or on a paper (through telex or fax).

There must be a fixed point between the sending and receiving terminals for those concepts to work. There is no specific location for the transmission or reception of data in the case of electronic mail; rather, the sender (in this example, an acceptance) can send the message from any location to a “server” that could be located anywhere in the globe, and the recipient (also an addressee) can access the message from any location. In circumstances where a contract is entered into over the phone, the High Court ruled that the law is rather clear: the contract is considered complete upon communication of acceptance and receipt of the same. However, this rule does not apply to electronic correspondence because the recipient of an email can be located anywhere in the globe. An electronic record is considered received at the place where the addressee has his place of business, according to section 13(3) of the IT Act, 2000, which addresses the lack of a fixed location for transmission or reception. Based on this categorical provision, the High Court determined that it possessed the necessary territorial jurisdiction to decide the issue since the email acceptance is considered to have been received at UP. Section 28 of the Indian Contract Act, 1872 states.

That parties cannot, by their agreement, completely circumvent the statutory authority of civil courts. A number of civil courts, however, subject to the jurisdiction of any civil court or courts so designated, and the Indian Contract Act, section 28, would not prohibit such an arrangement. When an action takes place entirely or partially within the High Court's territorial jurisdiction, the court may exercise its territorial jurisdiction. Thus, there is some similarity between the terms employed in the two clauses.

K. K. Velusamy v. N. Palanisamy¹⁶⁴ – According to the highest court in the land, Section 151 does not establish or grant courts any new authority or jurisdiction. It just acknowledges that every court has discretionary power as an intrinsic part of doing justice according to the law, doing what is “right” and undoing what is “wrong,” or doing whatever is needed to achieve justice's goals and prevent its abuse. By ostensibly using its inherent powers, a court cannot do something that is forbidden by law or the Code. Nobody can use their inherent power to go against the powers granted by the Code or in a way that contradicts those provisions if the Code covers a certain subject or feature and those provisions either explicitly or by necessary implication cover all the court or jurisdiction can do about that. Put another way, if the remedy or procedure is already laid out in the Code, the court cannot rely on the unique provisions of Section 151.

A.R. Priyasamy v. G. Karunakaran,¹⁶⁵ - which held that the evidence made on record is admissible, ought have directed the trial court to allow the applications. The court had requested the petitioner to present an interlocutory application to the trial court so that an expert could be brought to look at the recorded contents and ascertain their relevance and accuracy. The name of the person who made the record should be established through direct or circumstantial evidence to eliminate chances of tampering since the court held that the tape itself is primary and direct evidence could only act as a corroborating evidence. with the record. The trial court must also offer a chance to the two parties.

The trial court and the High Court have not considered whether the evidence sought to be admitted will assist in clarifying the issue before the court. They dismissed the application mechanically on the ground that the case was at its final stage and the arguments have been concluded. This was a fit case for the trial court to exercise discretionary powers under section 151, CPC to accept the application presented for the admission of the said compact disc upon satisfaction

¹⁶⁴ AIR 2011 SCW 2296

¹⁶⁵ AIR 1973 SCC 399

that the said disc could not have been presented earlier. The court may also listen to the recordings before accepting or rejecting the application for admission. The trial court was ordered to hear the matter judgment of this case.

SMC Pneumatics (India) Pvt. Ltd. v. Shri Jogesh Kwatra Original Suit¹⁶⁶— Supreme Court has that the court in afore-mentioned case has ruled against the plaintiff because electronic evidence furnished before the court did not certify as evidence under the section 65B of the Indian Evidence Act. position to receive the most compelling argument on behalf of the plaintiff in the circumstance in the view of the absence of any direct evidence to conclude that it was the defendant in particular, that person who was sending those emails. Court by keeping in view the facts and circumstances of the case, dismissed the suit of the plaintiff.

Rajesh Hariprasad Tripathi v. State of Gujarat Crl. Misc¹⁶⁷.— The Given the applicant's lengthy incarceration period (more than ten months) following his arrest, the Supreme Court has reached the conclusion that he is entitled to an extension of his bail under § 439 of the Code.

Hence, the application is allowed and the applicant is ordered to be released on bail in connection with FIR being C.R.No. I-226 of 2013 registered with Varachha Police Station, on his executing a personal bond of Rs. 5000 (Rupees Five Thousand Only) with one surety of the like amount to the satisfaction of the learned Trial Court and subject to the conditions.

Sanjaysinh Ramrao Chavan v. Dattatray Gulabrao Phalke¹⁶⁸— The Supreme Court has upheld a ruling by the Hon'ble High Court of Delhi in a corruption case. The court noted that the audio and video CDs in issue cannot be used as evidence, so the trial court made a mistake in relying on them. As a result, the court believed that the petitioners and co-accused conspired to commit the offence in question. Thus, there is no evidence to suggest that the petitioners were involved in committing the crime in question. An audio recording made during a sting operation served as the basis for this case's evidence. According to

¹⁶⁶ Suit No. 1279 of 2001 Delhi District court

¹⁶⁷ Appl. No. 10858 of 2014 (Guj HC)

¹⁶⁸ Criminal appeal no .97 of 2015 SC

the director of the state forensic science laboratory, the audio was too faint to be evaluated for spectrographic analysis. As the prosecution's legal team pointed out, the panch witnesses had confirmed the translation of the exchange. Since the voice recorder was not examined, the Supreme Court declined to use the translated versions of the conversation. Source and legitimacy are the two most important considerations when evaluating electronic evidence, according to the court”.

Tomaso Bruno and anr. V. State of Uttar Pradesh¹⁶⁹ – Because the prosecution failed to provide sufficient evidence to establish motive, the Supreme Court has decided to acquit two Italians serving life terms for the 2010 murder of a friend. The life sentences handed down to Tomato Bruno and Alyssa Betta Bon Compagni, two Italian nationals, by the Allahabad High Court were overturned by a bench. Here, the plaintiff's testimony is based on post-hearing corrections, which, in our view, does not give the court reason to believe it. For this particular instance, the courts do not properly appreciate the evidence and distance in the chain of circumstances sought by the plaintiff.

“We conclude that the plaintiff has failed to provide sufficient evidence to establish beyond a reasonable doubt that the accused is guilty, given the available facts and circumstances of the case. It is possible to find the appellant and the accused guilty. The judges, he continued, had disregarded the “best evidence”—the significance of CCTV cameras—and had not even considered the fact that the patients' medical records had shown no signs of sore throat.

In light of all the evidence and circumstances, the Supreme Court has laid forth the following scenario: the plaintiff's case proof of the accused's guilt, and the accused should be granted the benefit of the doubt. The appellant's conviction under section 302/34 of the Indian Penal Code was, therefore, overturned. Candidates ought to be discharged without delay.

¹⁶⁹AIR 2015 7 SCC 178: 3 SCC (Cri) 54

Shajeeb Khan v. State of Kerala¹⁷⁰ – The Supreme Court has that the application in the present was allowed and a bail with conditions was granted to the petitioner. Following conditions were imposed:

- Executing bond for Rs.1,00,000 with two solvent sureties.
- Sureties shall produce document to establish their identity and solvency.
- Petitioner shall appear before the investigating officer.
- Shall not indulge in any offence while on bail.
- Shall not intimidate witness.
- Not to leave Kerala without permission.
- Surrender passport.
- Lower court free to cancel bail if any above condition breach.

Kalandi Charan Lenke v. State of Odisha¹⁷¹ – The Supreme Court has that after going through all the materials, it appears that through the electronic form there is stalking, online transmission of sexually explicit or obscene morphed naked picture of the victim. So, the offences under the Information Technology Act Prime facie cannot be ruled out. Here court referred **Shanat Babu Digwmani v. Govt. of NCT Delhi case**¹⁷² and stated in the case above under 292, 294 of IPC, 1860 and section 67, 67A and 67B of IT Act, 2000 remunerate. was permitted to opine but the Apex Court was satisfied that there was no section 292 of IPC to go hand in hand with the reason that the IT Act is special provision which would apply in the sphere of offence committed through electronic form. Applying the ratio of the case, in the instant case the entire obscene message and fake Facebook account showing stalking and obscene representation or morphed naked photograph of the victim are all prima facie committed by the petitioner through electronic form as per the Police papers.

Moreover, the material about the pamphlets or any other form of

¹⁷⁰ B.A. 8074 of 2015 (Ker HC)

¹⁷¹ AIR2017(I) OLR 543

¹⁷² AIR 2015 11 SC (573)

defamation to the character of the victim pasted on the wall of the College or hosted as alleged being not investigated to have been made by the present petitioner except a suspicion is raised about his involvement with such crime. But offence under the IT Act is prima facie made out against the petitioner. On the other hand, the offences under the IPC against the petitioner are yet to be made out. Be that as it may, offence under section 67A of the IT Act is prima facie in this case against the petitioner is non-bailable.

Statement of the victim again it appears that through the electronic form the petitioner had made it clear that he has got a one side love and being not successful in materializing the design of love, he took shelter of cyber law to commit crime. The dignity of woman is always required to be protected and under Article 51A of the Constitution every citizen has got fundamental duty to protect the dignity of the woman. Even if the offence prima facie committed through electronic form but the punishment under section 67A of the IT Act is up to five years if committed at first.

Considering the punishment prescribed for the offence prima facie found out, most of the offences as alleged by prosecution are bailable, character of evidence as discussed above including absence of criminal antecedent of petitioner and period of his custody, lenient view is taken to release him on bail. But the dignity of the woman as discussed above has to be kept in view as stalking or opening of fake Facebook account or obscene representation including morphed naked photographs are menace to the society and the right of the woman. Here petitioner allowed to bail with strict conditions.

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal¹⁷³ -The case presented to the court in An election appeal contesting the legitimacy of Mr. Arjun Pandit Rao Khotkar held an appeal of 97 whereby the nomination papers were presented by him after the deadline. The video recording evidence could not be supported using the Evidence Act since there were no relevant certifications. The recording was admitted as evidence in the High Court after it was testified to

¹⁷³ AIR 2007 SCC 1

by one of the EC officials. The same was requested to be submitted by the petitioner. The party interested in the use of the electronic record may apply to the court to provide the required certificates in case the competent party or body is not willing to provide them. That being the case, the Court held that the condition of section 65B(4) was mandatory as opposed to discretionary, it should have been met to allow secondary electronic records to be admissible. The electronic evidence should be provided before the commencement of the trial and the Court has the mandate to order the production of the evidence at any time before the trial terminates in accordance with section 65B. (4).

The Court upheld the decision of the High Court after outlining the scope of section 65B, had been used. that was not certified evidence (4). Having said that, this happened alongside the electric as well as the admissible evidence already produced, the High Court determined that nomination documents were not filed on time. The Court ruling does not imply that the provision in section 65B(4) is available, but it depends on the specific circumstances of the fact that other pieces of evidence were also present. Wherever a secondary reproduction of an electronic record is undertaken as has been described by Justice Nariman, a certificate 126 in section 65B(4) has to be secured..

Cross-examination by an Election Commission officer proved the originality of the video footage. The High Court admitted the video recordings as evidence on the basis of this testimony even though the certificate which is expected in section 65B(4) was not produced. Since a competent authority had confirmed the authenticity of the video recordings, the High Court had concluded that there was a substantial prosecution of section 65B.

According to Section 65B(1), which is highlighted by Justice Nariman, a difference is made between the original electronic record created by the original computer and the secondary copy produced out of the primary record. In this case scenario, the initial storage place of the video footage i.e. on the computer of Election Commission would be the original electronic record. The secondary copies of the records will be the CDs with the material of the video recording.

According to the court, the certificate needed in section 65B(4) could only be obtained when the secondary copies of the electronic record are provided to the court.

There is no need to create a certificate at the time of the first creation of an electronic record. In case the individual who first saved the information on the computer, tablet, or mobile phone being directly presented in the court and testifying to this fact himself, the original electronic record may be presented personally in the court. According to the Information Technology Act of 2000, where the original storage of the electronic record is a computer which is also part of a Computer Network or Computer System and it is not physically possible to bring such a network/system to the Court, the production of secondary copies can be accompanied by certificate as has been specified by section 65B(4).

Justice Nariman was another judge who shared this opinion expressed in the *Anwar v. Basheer*- that section 65B is a complete code on its own regarding the admissibility of electronic evidence and will not be subject to any other piece of evidence act. **Anwar v. Basheer**¹⁷⁴ too believed that- If such an electronic record is utilized as the primary evidence under section 62 of Evidence Act the same is admissible in evidence without satisfying the requirements of section 65B of 127 Evidence Act. Justice Nariman made it clear in the dictum that we should read it without including the words under section 62 of the Evidence Act. The reason is that 65B is a full code of electronic evidence and it will override other regulations like section 62. By this Justice Nariman suggests that there is no need to make reference to section 62, since section 65B(1) on its own draws the distinction between the original electronic record and the secondary copies of the electronic record.

AZZ Infraservice Ltd v. Quippo Infrastructure Ltd. SLP (C) No. 8636¹⁷⁵— The Court said that the Supreme Court cannot deny that prima facie there is an admission on the part of the respondent that the due balance of 8.18 crores against the appellant is fulfilled. Even though the counsel of the respondent

¹⁷⁴ AIR 2014 10SCC473

¹⁷⁵ Appeal (c) no(s)8636/2021 HC (Calcutta)

argued that the WhatsApp messages used are forged but did not have sufficient techniques to support his argument. According to On appeal Supreme Court, it is stated that; Messages sent in social media site WhatsApp are inadmissible in evidence and that the person who sends such WhatsApp messages is also not associated with those messages, particularly where such messages relate to business arrangements, which are bound by an agreement. The court also further provided that E-mails confirmation of quotes when compared by WhatsApp messages will be admissible in the Indian Evidence Act, 1872 and in the section 65B of the Information Technology Act, 2000. To this end, however, emails must be accompanied by an approval mail that has an evidential value.

Sattai Durai Murgan v. The Inspector of Police Crl OP (MD) No. 9381 ¹⁷⁶The seen that the petitioner has been languishing in jail since June 16, 2021 Supreme Court has that It is almost fifty days and he has filed an affidavit, pledging in future he would not engage in such activities and is willing to follow any such terms that would be set by the Court. As also observed, the wife of the petitioner has given an affidavit dated August 4, 2021 before this Court that the petitioner has been infected with urinal tract a number of days ago and despite being given treatment, he has failed to heal completely. Considering the facts and the circumstances of the case, the nature of allegations leveled against the petitioner, the duration of his imprisonment, affidavit that was undertaken by the petitioner, that he would not indulge in such activities in future and his infirmities, this Court is tempted to grant bail to the petitioner. Sentenced to hear cancel bail granted, January 20, 2022.

Asked if the government had any mechanism through which such misuse could be prevented and appointed Advocate K.K. Ramakrishnan as amicuscuriae to assist the court on the issue. The judge orally asked Duraimurugan's counsel whether the you Tuber was making money out of such videos. Duraimurugan had earlier given an undertaking to the court that he would not repeat the offence if granted bail. The judge pointed out that in several other cases, too, accused have

¹⁷⁶ Crl appeal No. 9381 of 2021

confessed that they learn about making guns, committing robbery and such other offences from YouTube videos, holding that social media is being misused, the judge sought reply from authorities regarding steps taken to curb such activities. The court adjourned the case by a week.

M/s DRS Logistic Ltd. & Another v. Google India Private Limited & Anr.¹⁷⁷ –

–The Supreme Court has that So, here court for reaching on to the conclusion referred judgment V. LMG of **Amway India Enterprises Pvt. Ltd. and Ors. Technologies Pvt. Ltd. and Ors., 260 (2019) DLT 690**¹⁷⁸, where a Coordinate Bench of this court in the context of considering the usage of the Mark Amway by third party e commerce platforms, to advertise their own sales, has found the use of a mark in meta-tag or in advertisement without the proprietors rights to the mark, as a violation of trademark rights of the owner. Actually, the Court also believed that the section 29(8) further gave it clear that when there is any advertising of a mark that has unfair advantage on the mark or it is otherwise detrimental to the distinctive character of the mark even without sale, then there is infringement.

Similarly, is the decision of the Bombay High Court in **People Interactive (I) Pvt. Ltd.**¹⁷⁹ (*supra*) in which the Court noted that the Defendant No. The plaintiff was a third party marking shaadi.com and the name of the domain, which no.I was using. shadi.com as a meta-tag in the first defendant site which the Court held was an endeavor to embezzle the mark of the plaintiff and usurp the internet traffic of the plaintiff by a fully dishonest and mala fide use of plaintiffs mark and name in the meta-tags of his own competitor of the plaintiff site.

Court further adds that it is in the policy of Google that it will not research the keywords but the Ad content, which consists of the ad text and ad title but not of the keywords. To determine the quality score, Google also looks at the quality

¹⁷⁷ CS (Comm.) 1 of 2017, I.A 2646/2020 at HC (Delhi)

¹⁷⁸ AIR 2019 DLT 609

¹⁷⁹ AIR 2015 comm ipNO. suit no 118

of the landing page which mostly is the web-site of the advertiser that might or might not have/ display the infringed trade mark. Differently put, the situation is not about Google, that adoption of same shall not constitute an infringement of trademark because the keywords are not visible to a consumer. Yet, with the Ad words Program they also view the landing page i.e. web site of the advertiser, the infringing trademark, which is also a keyword, being involved, in such a situation, Google cannot off-load the responsibility of ensuring that the keyword is not an infringement of trademark.

Finally, Court mention that plaintiff may enjoy protection of its trademarks which are registered in pursuit of section 28 of the TM Act, but may not have any right on surnames/generic words such as Packers or Movers separately. Order Accordingly, court based on the discussion above in consideration that the applications are subject to be permitted, pending a final decision of the suit in the subsequent manner:

1. The defendant Nos. 1 and 3 shall investigate any complaint to be made by the plaintiff to them alleging use of its trademark and its variations as keywords resulting in the diversion of traffic from the website of the plaintiff to that of the advertiser.
2. The defendant Nos. 1 and 3 shall also investigate and review the overall effect of an Ad to ascertain that the same is not infringing/passing off the trademark of the plaintiff.
3. If it is found that the usage of trademark(s) and its variations as keywords and/or overall effect of the Ad has the effect of infringing/passing off the trademark of the plaintiff then the Defendant Nos. 1 and 3 shall restrain the advertiser from using the same and remove/block such advertisements.

Harsh Kadam @ Hitendra Kumar v. State of U.P. ¹⁸⁰Case under Section- The Supreme Court has that when the above stipulation of the law has been invalidated by the Apex. Contact court vide judgment and order dated March 24, 2015, how any FIR could have been filed in the year 2019. Court also offer

¹⁸⁰ appeal No. 5244 of 2021 (Allahabad HC)

guidance on how the charge sheet could have been filed in on the same section when the FIR could not have been lodged under this section. Moreover, no FIR or charge sheet could have been made in this case and the learned Magistrate ought not to have made summoning order. Court held that the said argument of Sri Singh is entirely valid as far as the allegation in the 7 FIR could not have been lodged under the aforesaid provision of law under section 66A of the IT (Amendment) Act, 2008, as to how the charge sheet has been instituted and the summoning order has been given.

This case is a clear-cut example of non-application of mind by the Investigating Officer who has filed charge-sheet on September 2, 2019 in a particular section i.e., section 66A of the IT (Amendment) Act, 2008 which has se already been struck down by the Apex court in re; **Shreya Singhal**¹⁸¹ (supra) on March 24, 2015 and by the learned court below who has taken cognizance of that charge sheet without verifying the legal aspect which was incumbent upon him. Therefore, charge-sheet was quashed, which has been filed against the petitioner under section 66A of the Information Technology (Amendment) Act, 2008 as well as the summoning order dated January 25, 2020 passed in the aforesaid criminal case.

State v. Salman Ansari Cyber, Jamtara Dist. Court¹⁸²– The Supreme Court has that In this Case Investigation Officer is important witness. He has supported that the Mobile No has fitted with IMEI number Obtained from possession of Salman Ansari was used in creation of several e-wallets. From the produce evidence it is clearly reveal that the said mobile is linked with the Union Bank of India Account and IDFC First Bank Account which are on the name of Salman Ansari. It is also revealing that the several transactions of cheated money by using the said mobile no. recovered from possession of Salman Ansari. CDR of mobile number showing the tower location of village Bhithra which were issued in the name of Kuidip Ali, Pallav Jana and Shankar Rai of West Bengal Which clearly reveals that these SIM Nos. have been used by Salman Ansari.

¹⁸¹ AIR2015 SC 1523

¹⁸² Appeal No. 5244 of 2021 (Allahabad HC)

E-wallets have been created by which several transactions of money have been made by using the several cards, but it appears that although several persons have been alleged to have been cheated but no one has come before the court to depose that he has been cheated or his amount has been fraudulently withdrawn. Thus, the essential ingredients for constituting the offence under section 420 of IPC is not made out.

The accused had not submitted Customer Acquisition Form to the retailer and distributor. No comparison of signature of accused has been made with alleged Customer Acquisition form or on any document which is alleged to be forged one. On prosecution evidence, proven that accused has retailers. Therefore, it seems that there is no compelling and credible evidence that accused himself had forged any particular document. Hence, the essential ingredient for constituting the offence under section 468 of IPC is also not being fulfilled but in view of entire evidences, it is apparent that accused Ansari was found with possession of aforesaid fake SIMs, which were issued in the name of aforesaid Layla Bibi, Pallav Jana, Shankar Rai and Kuidip Ali on the basis of false CAFs and by using their unique identification features like Identity Card and thumb impression. It has been established that accused Salman Ansari had used the said SIMs in creation of e-wallets and several transactions, thus, it is apparent that the accused namely Salman Ansari had obtained forged SIMs and used the same and he had full knowledge and reason to believe that the said SIMs are forged and have been obtained on the basis of false documents.

During examination of accused under section 313, Cr.P.C he has denied questions put before him in the simple way that it is wrong and highly unsatisfactory on this point, argument advanced by the defence counsel is totally ruled out. court to be cautious on this point that there was any It is the duty of the possibility of deliberation to falsely implicate any person in crime which is lacking in this case. Therefore, the essential ingredients for constituting the offence under section 471 of IPC and section 66(c) of IT Act 2000 stands proved against accused Salman Ansari.

So far as the allegation under sections 414, 419, 420, 467 and 468 of IPC and under section 66B and 66D of IT Act are concerned it appears that none of the witnesses has stated that accused Salman Ansari had used stolen mobiles and SIMs. None of the witnesses has stated that accused had cheated him by impersonation and further none of the alleged victims has been examined to support the fact of cheating by way of impersonation. Similarly, no cogent and reliable evidence has been brought on record to prove the fact that accused Salman Ansari had made any document that appeared to be a valuable security as provided by the section 467, Cr.P.C. Correspondingly, it can be prosecuted that charges against aforesaid accused Salman Ansari can not be substantiated under sections 414, 419, 420 and 468 of IPC and under section 66(B) and 66(D) of IT Act 2000.

Thus, none of the charges has been proved against accused Salman Ansari beyond all reasonable shadow of doubts and he is acquitted under the charges under sections 414, 419, 420, 467 and 468 of IPC and under section 66(B) and 66(D) of IT Act. However, Court found and hold that accused Salman Ansari is found guilty for the offences under section 471, IPC and under section 66(C) of Information Technology Act. He is in judicial custody.

Payel Bishwas v. Commissioner of Police WP–¹⁸³ The Supreme Court has held that the Judgment in CP Girija instructs the installation of CCTV cameras not on public places but in intimate, privative places. The judgment by the Supreme Court is very clear in that any invasion should fulfill the three-fold requirement of (i) legality, which presupposes the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them. In the first place, unless a legislature mandates by law that CCTV cameras ought to be installed in a certain space, if anyone doing so it would violate Article 21.

The message, which the Government sent in this instance, considers installing CCTV cameras, which are only at the points of entry and exit. It

¹⁸³(MD)No. 22667 of 2021 (Madras HC)

expressly waives that this would not prejudice the privacy of the person. Therefore, when passing subordinate legislation, the executive has been aware of the privacy issues of the citizens. When it comes to a decision to install a CCTV camera that is said to have some kind of bearing on the privacy of a person, the most considerations should be given-the government should put to good use its head and see what form of regulations should be implemented on its proper usage. The mere suspicion of evil deeds being undertaken in massage centres is not enough to invade into the right of an individual to relax because it is inherent in his basic right to privacy.

Ashlesh Biradar v. State of West Bengal WPA¹⁸⁴—The Supreme Court has that therefore, in view of the above mentioned reasons and prima facie conclusion that the impugned order under section 144 of the Cr.P.C has been passed without the aid of law and not taking any of the requirement of section 5(2) of the Indian Telegraph Act, 1885, the Rules of 2017, consideration of the case of **Anuradha Bhasin and PUCL**¹⁸⁵ (supra) and also the fact that the reason now advanced in support of passing the impugned order are not contained Nevertheless, the Court was additionally informed that the State Government so suspended internet services on the basis of the Temporary suspension of Telecom Services (Public Emergency or Public Service) Rules, 2017.

Shiv Kumar v. State of Bihar¹⁸⁶— The Supreme Court has it that Cyber crimes commence with sale of SIMs to cyber criminals with false documents. After this forgery is perpetrated, it is impossible to track the cyber criminals who use the SIM by obtaining Patna High Court CR, MISC, No. 38807 of 2020 (15) dated February 1, 2022 on the premises of the existence of forged documents, but the common people have to pay. The rule especially of registration of the F.I.R./ complaint by the Telecom Companies not just a mere procedure is to be adhered to by the Telecom Companies but when the F.I.R./ complaint is registered by the individual in relation to a specific crime, then the Police will be set into action

¹⁸⁴ WPA (P) 104 of 2022 (Calcutta HC)

¹⁸⁵ AIR 2020 SC1308

¹⁸⁶ Criminal Misc. No. 3807 of 2020 (Patana HC)

and those people who are using the SIMs relying on the false and fake documents can be tracked and arrested. Failure to have the FIR registered on complaints filed by the Telecom Companies means that the cyber criminals working within the State will never be tracked and arrested. The Telecom Companies should not be permitted to act in utter contravention of the guidelines of the Department of Telecommunications (DoT). Apparently, the D.G.P not the DoT had not intervened at the time when the DoT guidelines were being disobeyed with impunity. The act of the officer-in-charge of the Kadamkuan police station is contemptuous and is unable to deny in such kind of thing as also failure to register the FIR is also violation of the directions of **Lalita Kumari case**¹⁸⁷(supra) So here court ordered that Kadamkaun police station was directed to file a show cause as to why a contempt proceeding could not be initiated against him for not registering the FIR.

Justice K.S. Puttasamy (Retd.) v. Union of India—¹⁸⁸ The Supreme Court has that Supreme Court in this case approved the Aadhaar Scheme as valid scheme after striking down the unconstitutional section 57 of the Aadhar Act. Court pointed out that government has taken sufficient security measures to protect the data of citizen which have been asked to reveal for Aadhaar. Nine Judges bench further stated that information which has been obtained through Aadhaar should not be released to commercial banks, payment bank/ gateways, e-wallet companies and telecom companies for buying SIM card. They also added that school shall not ask students their Aadhaar details for appearing in board examination or for admission. Constitutional bench made Aadhaar details mandatory to avail social welfare schemes, filling income tax return and for acquiring PAN ID. Supreme Court explained difference between other identity cards and Aadhaar Cards. Court said that Aadhaar cards have a unique identification number which cannot be duplicated like any other website. The principal objective of Aadhaar card compulsion is to enable to receive schemes of social welfare. Aadhaar scheme was pronounced to be valid by Supreme

¹⁸⁷ Lalita Kumari vs Govt. of U.P. AIR 2014 SC 187

¹⁸⁸ AIR 2017 SC 4161: (2017) 10 Scale 1: (2017) 10 SCC 1

Court. Nonetheless, section 33(2), 47 and 57 of the Aadhaar Act was struck down by Apex court on the ground that they found. unconstitutional. the pronged test needed to establish the encroachment of Article 21 Right to Privacy-

- State action must have a legislative man date
- It must be pursuing a legitimate state purpose
- It must be proportionate

Commentary given by Bench

Justice Chelameswar's three Comment– Justice J. Chelameswar said that fundamental rights are the only constitutional firewall to prevent State's interference with those core freedoms constituting liberty of a human being. The right to privacy is certainly one of the core freedoms which is to be defended. It is part of liberty within the meaning of that expression in Article 21.

Justice Bobde's Comment– Justice S.A. Bobde said that the first and natural home for a Right of Privacy is in Article 21 at the very heart of 'personal liberty' and life itself. There are innumerable activities which are virtually incapable of performed in any case, or even with dignity, unless one be the one alone, or one be otherwise authorized to secure his or her privacy. Birth and death are occasions in which the privacy is demanded in obtaining dignity among all the civilized people.

Justice Nariman's Comment– Justice Rohinton F. Nariman on privacy in an elitist construct: The bulk of poor people that the Centre (Attorney- General K.K. Venugopal speaks about are people who in the totally different and changed world today have cell phones, and would stand forward to demand the basic right of privacy, not only against the Government, but also against individuals privately. We do not find the slightest hostility between the rich and the poor, in this respect. The point of On Centre that privacy does not have to be enshrined in the constitution as a right and can be secured by parliamentary act: Statutory law can be created and also repealed by an ordinary majority of Parliament. Put simply, the ruling party has the power at its own will to abolish either or all of the

safeguards in the statutes referred to hereinabove. Basic rights on the other hand are included in the Constitution such that there would be rights that the citizens of this country would enjoy regardless of the governments that they may be electing.

Justice Sapre's Comment– Justice A.M. Spare: essential right of a citizen assured by part III of the Constitution. But this is not an absolute right but subject to certain reasonable restrictions.

Justice Kaul's Comment– Justice Sanjay Kishan Kaul opined that Privacy is merely a sort of dignity, which is a subdivision of liberty. So, out of the one great tree there are branches which in turn give rise to sub- branches and leaves.

Nishant Ray vs. State of U.P.¹⁸⁹- This case deals with a bail application filed by Nishant Roy, a BBA student, accused in a large-scale cyber fraud involving over ₹1.48 crore, under various provisions of the IPC and Information Technology Act, 2008. The Allahabad High Court assessed the seriousness of cyber crime and its impact on society while deciding the bail. The case arises from a large-scale cyber fraud executed between 23rd and 25th April 2024 targeting Smt. Kakoli Das Gupta, a senior citizen.

The fraudsters posed as FedEx courier officials and police officers, falsely informing her that: A parcel allegedly sent in her name contained illegal items such as narcotics and fake passports. An investigation had been initiated against her, and to avoid arrest, she had to cooperate financially for verification and clearance.

The Allahabad High Court, after examining the gravity of the allegations, rejected the bail application filed by Nishant Roy.

The Court emphasized that: The nature of the offence involved organised cyber crime with a large financial impact, affecting public trust in digital transactions. The applicant's alleged involvement was not minimal, as electronic devices and SIM cards recovered from his possession were connected to the

¹⁸⁹ AIR 2024 AJL 472

fraud.

Granting bail at this stage could interfere with the ongoing investigation, especially since co-accused including his father were still absconding and the entire nexus was yet to be unraveled. The Court cited precedents stating that economic offences are grave in nature and harm the fabric of society, requiring a stricter approach in bail matters.

Devashish rai vs. state of U.P.¹⁹⁰ - In a landmark decision, a Lucknow court sentenced Devashish Rai to seven years of rigorous imprisonment for posing as a CBI officer and coercing a woman doctor into transferring ₹85 lakh. This marks the first conviction in a "digital arrest" case in Uttar Pradesh and one of the fastest cyber crime trials in the state, concluding just over a year after the FIR was registered. The court emphasized the need for a swift judicial response to evolving cyber threats.

Devashish Rai was convicted under different sections by the Special CJM (Customs) Court headed by Alok Kumar. The Information Technology (IT) Act and (IPC). IPC 419 (cheating by personation), IPC 420 (cheating), and IPC 467, 468, 471 (forgery related offenses), and 66D of the IT Act (cheating by personation using computer resource). His sentence was seven years of strict imprisonment, the heaviest of the separate sentences, and a fine of 68,000 in total.

Deepak Singh v. State Of U.P. And 3 Others¹⁹¹ The Allahabad High Court directed the police to submit a report under Section 173(2) Cr.P.C./193 B.N.S.S. in a case involving Section 67 of the I.T. Act, Police Station-Cyber Crime Police Station, District-Maharajganj. The court emphasized the importance of timely investigation and submission of reports in cyber crime cases.

Anoop Uttam v. State Of Up And 3 Others¹⁹² : The Allahabad High Court protected the petitioner from arrest till the submission of the report under Section

¹⁹⁰ AIR 2025 LHC (Cri no 3/2025)

¹⁹¹ AIR 2025, HC Allahabad

¹⁹² AIR 2024, HC Allahabad

173(2) Cr.P.C. in a case involving Sections 420, 467, 468, 471 IPC, and Section 66D of the IT Act. The court highlighted the need for proper investigation and consideration of evidence in cyber crime cases before making arrests.

Shivam Gupta @ Krishna v. State of U.P.¹⁹³ : The Allahabad High Court denied bail to the accused in a cyber crime case, considering the seriousness of the allegations and the material on record. The court emphasized the gravity of cyber crime offenses and the need for judicial caution in granting bail.

Jai Maa Aadi Shakti v. Union Of India And 3 Others¹⁹⁴ : The Allahabad High Court directed the respondent to follow up with the National Cyber Crime Reporting Portal Cell regarding a frozen account with a lien amount of ₹2150. The court ensured that the authorities follow due process in handling frozen accounts and lien amounts in cyber crime cases.

Imran Khan v. State of U.P. and Another¹⁹⁵ : The Allahabad High Court held that merely liking a post on social media will not attract penalty under Section 67 of the I.T. Act. The court clarified the distinction between publishing/transmitting obscene material and merely liking a post on social media.

Tarun Kayal v. State Of U.P. And 3 Others¹⁹⁶ : The case in question was a petition that was filed under Section 420 IPC and was registered as Case Crime No.21 of 2022, on 01.11.2022, under Information Technology Act, Section 66C Police Station Cyber Crime, District Prayagraj. The court took into account the petitioner's willingness to return the balance amount and the fact that charge-sheets had already been forwarded.

Ashok Kumar Srivastava v. State of U.P. And 3 Others¹⁹⁷ : The court directed the investigation of a cyber crime case to be conducted by the Cyber Cell, considering its expertise in handling such cases. The court recognized the importance of specialized investigation units in handling complex cyber crime

¹⁹³ AIR 2024, HC Allahabad

¹⁹⁴ AIR 2025, HC Allahabad

¹⁹⁵ AIR 2025, HC Allahabad

¹⁹⁶ AIR 2025, Dist. Court Allahabad

¹⁹⁷ AIR 2022, Dist. Court Allahabad

cases.

Akash Verma v. State of U.P.¹⁹⁸ : The court considered a bail application in a cyber crime case where the applicant admitted to opening forged bank accounts related to cyber crime. The court emphasized the seriousness of cyber crime offenses and the need for judicial caution in granting bail.

Sujit Kumar v. State of U.P. and Another¹⁹⁹ : The court considered an anticipatory bail application in a cyber crime case. The court considered the allegations and evidence in the case while deciding on the bail application.

¹⁹⁸ AIR 2025, Dist. Court Banda

¹⁹⁹ AIR 2025, Dist. Court Allahabad

CHAPTER–VI

A CRITICAL EVALUATION OF CYBER LAWS IN BUNDELKHAND REGION OF UTTAR PRADESH

6.1 INTRODUCTION

The cyber law as a subject of legal studies is not only nascent but mind boggling also; principally because the diversity of disciplines it touches and challenges it presents. In the light of all this, authoring a research work on Cyber Law is really a hard nut to crack; and warrants a depth of knowledge and height of understanding that a lesser mortal like me can only dream of. Therefore the best I could try my hands at was to present. An Introduction to Cyber Law, which the present research work is all about. It took me a year and a half to complete this research work; but how complete it really is will ultimately be decided by the readers and the critics.²⁰⁰

There is more rush to get a site in the cyber world today than to get a flat allotted in one's name in a metropolis. People clamor to get their rights recognized and protected in the cyber world with a commitment unforeseen in the mortal world; so much so that our very being in the physical world more often than not has come to be defined by our presence in this virtual world. The man in the cyber space commands a similar position in so far as even the biggest of deals he strikes are finalized with a simple push of a button that takes only a few seconds. The ease and efficiency are the hallmarks of this world, where everything seems but a click away.²⁰¹

But, then, there is the other side of this wonderful world man has carved out for himself. The simple fact that the cyber world encompasses the real world implies that the transactions made in the former may impact the latter, taking in their ambit a multiplicity of legal and territorial jurisdictions. And, these impacts may be good as well as evil; since both are the manifestations of the Lord said

²⁰⁰ The Information Technology Act, 2000 (Amended 2008), Government of India.

²⁰¹ Indian Penal Code (IPC), 1860 – Provisions Related to Cyber Crimes
(section 65, 66, 66A, 66B, 66D, 66F, 67, 72, 72A)

himself – aham sivasca asivasca (O, Arijuna! I am the good and the evil).

6.2 ACRITICAL EVALUATION OF CYBER LAWS

The Cyber law is not defined anywhere. Cyber law is not a codified law. Cyber security system is not very well. The cyber crimes hurry up recently growth slowly-slowly. The cyber law is not a complete law. The concept of cyber crime is very short definition show whole of the society did not understand. The research point out bunch of the critical evaluations present in this form. The whole of India the cyber law is growth fastly. The researcher is mention all the relevant laws regarding cyber crime but does not fulfill the all the terms and conditions according to legal scenario.

6.3 A ANALITICAL STUDY IN BUNDELKHAND REGION OF UTTAR PRADESH

The researcher is a very good surveyor in the field of legal areas. The Bundelkhand area divided according to government classification seven districts. Like Jhansi, Lalitpur, Jalaun, Hamirpur, Banda and Chitrakoot districts. The researcher personally visit in district head quarters and concern cyber police station . The researcher personally visit in cyber police station in every district meet thana incharge to fill the questionnaire . The all the legal issues and important questions put up in front of police officers. The police officer reply smoothly. The researcher all the relevant questionnaire all the data regarding cyber laws mention as under.

Jhansi is historicity of Uttar Pradesh. Balwant Nagar was the old name of Jhansi. It lies in the region of Bundelkhand, on the banks of the Pahuj River, in the extreme south of Uttar Pradesh. Jhansi is the administrative head quarters of Jhansi district and Jhansi division. Also called the *Gateway to Bundelkhand*, Jhansi is situated near and around the rivers Pahuj and Betwa at an average elevation of 285m (935ft). It is about 420 kilometres (261mi) from national capital New Delhi and 315 kilometres (196 mi) from state capital Lucknow.²⁰²

²⁰² Jhansi :a historical overview ,jhansi district administration ,government of uttar pradesh,2022

DISTRICT JHANSI

The Cyber Crime Police Station in Jhansi district is a cutting-edge facility dedicated to tackling cyber crime in the region. It falls under the Jhansi Police Zone and Chitrakoot Mandal, and was established in February 2024 as part of the Uttar Pradesh government's initiative to become cyber-resilient.

Located at Nehru Marg, Jhokan Bagh, Jhansi - 284001, the station boasts a digital lab and a team of 25 personnel, including experts in cyber crime investigation and digital forensics. This enables the station to efficiently investigate and analyze cyber crimes, providing prompt assistance to victims.

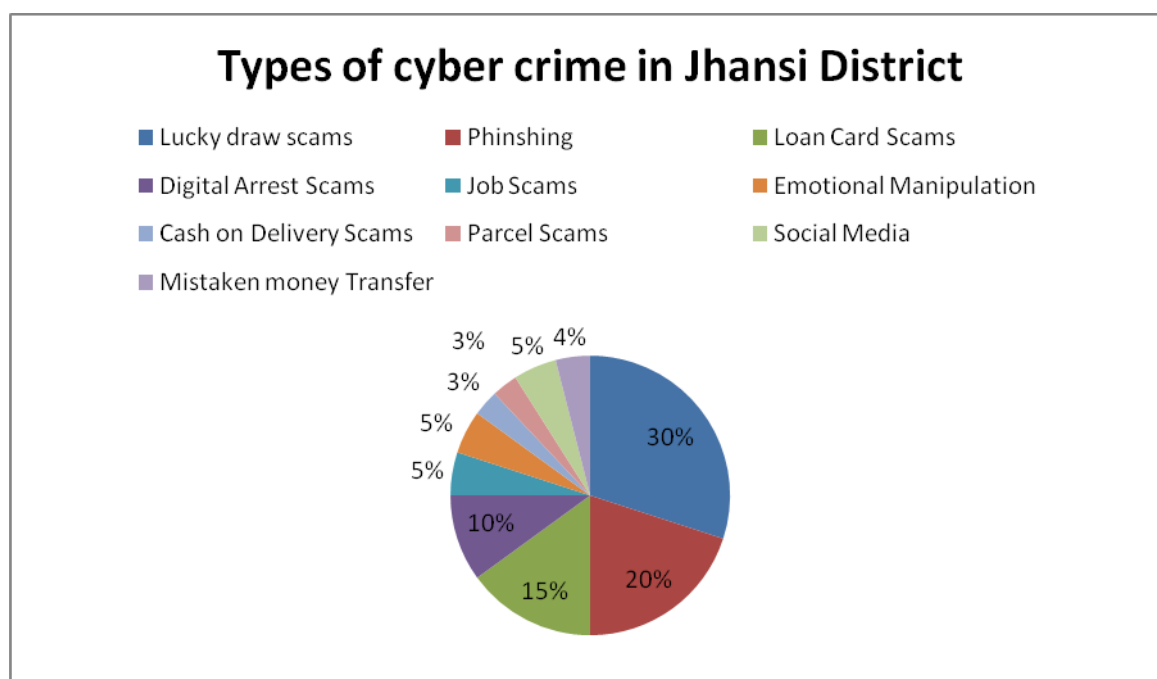
The establishment of the Cyber Crime Police Station is a significant step towards strengthening the state's cyber crime prevention capabilities. The Uttar Pradesh government has sanctioned ₹32.8 crore to support the initiative, which will be used to enhance database management, forensic tools, and data analysis software.

The station has already demonstrated its effectiveness, with several successful operations against cyber criminals. In one instance, a team from the station arrested a youth involved in hawala activities



Types of cyber crime in Jhansi district

Lucky draw scam	161	30%
Phishing	107	20%
Loan card and card scam	80	15%
Digital arrest	53	10%
Job scams	26	5%
Emotional manipulation	26	5%
Cash on delivery scams	16	3%
Parcel scams	16	3%
Social media	26	5%
Mistaken money transfer	21	4%



Analysis-The data reveals that "Lucky draw scam" is the most prevalent type of cyber crime, accounting for 30% of the total cases, with 161 reported incidents. "Phishing" is the second most common, constituting 20% of the cases, with 107 incidents. "Loan card and card scam" follows closely, making up 15% of the

cases, with 80 incidents. The remaining categories, including "Digital arrest", "Job scams", "Emotional manipulation", "Cash on delivery scams", "Parcel scams", "Social media", and "Mistaken money transfer", collectively account for the remaining 35% of the cases. Notably, "Cash on delivery scams" and "Parcel scams" are tied at 3% each, with 16 incidents each. The data suggests that the majority of cyber crimes in Jhansi district are related to scams and fraudulent activities,

Questionnaire of Cyber Thana In charge

Date- 11/06/2024

Place- झांसी

1. What is your name and post ?

R.K. Singh cyber expert

2. What types of cyber crimes are more common in your area ?

वित्तीय धोखाधड़ी, फिशिंग, ऑनलाइन शॉपिंग धोखाधड़ी
नौकरी के नाम पर धोखाधड़ी, भ्रष्टाचार योजना, KYC, सोशल मीडिया अपराध

3. What is the general age group and education level of the people who are victims of those crimes ?

35-45-वर्षीय, 10-30 सोशल मीडिया

4. Does the crime usually occur most frequently among a particular age group or group ?

18 से 40 साल के लोगों में ज्यादा है सोशल मीडिया, गेमिंग
शॉपिंग वाले अपराध, वित्तीय में 35 से 60 साल ज्यादा है।
जो कमजोर है महिला में है पर शॉपिंग और सोशल मीडिया ज्यादा है

5. According to you, what are the reason why people become victims of these crimes ?

उनमें ज्यादातर ग्रामीण परिवेश के सीधे लोग हैं। विश्वास कर
लेते हैं और ज्यादा ध्यान नहीं देते।

6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?

हाँ, पहले ज्यादा रिपोर्ट नहीं होती थी अब लोग आते हैं।
मामले सुलझते हैं। गैरमिल जुड़ते हैं तो समझाकर समझाते
अदालत जाते हैं।

7. Is any type of workshop or special training organized by the government for you ?

हमारी शराव workshop होती है। 15 दिन में उपलब्ध होता है।
Microsoft और Google जैसे कंपनियों में आते हैं। Workshop

8. Does this training help you well being ?

हाँ, जैसे तरीके आते हैं। जल्दी पहचान पकड़ने तक
करने के अब कंपनियों से जल्दी दस्ता मिल जाता है।

9. What are your efforts to create awareness and establish communication among the general public ?

हम स्कूल, कॉलेज, कंपनियों में meeting करते हैं।
Newspaper, विज्ञापन करते हैं लोगों के जागरूक
करते हैं। पहले 2 साल से साप्ताहिक जागरूकता
अभिमान चल रहा है। Toll free number है 1930

Pic. No.- 01

हम हर महीने प्रथम बुधवार को साइबर जागरूकता अभियान चलाते हैं। बच्चों और युवाओं के लिए।

10. Do you receive any cooperation from other areas during the investigation of such crimes ?

पहले नहीं था अब है। कई company सीधे हमको data देते हैं। पहले कम्प्लेन लगना पड़ता था अब आसान है।

11. Is there a problem due to there not being any specific law for cyber crime?

हम कभी कभी फँस जाते हैं कि मामला किस किस धारा के अन्तर्गत आये और लोग भी थोड़ा धक्का देते हैं कि धारा कौनसी।

12. Are the steps taken by the government effective in this regard ?

अभी और जरूरत है जैसे जैसे हम तकनीक पर निभते हो रहे हैं नये अपराध सामने आ रहे हैं।

13. When these crimes commits interstate, you get help from other states ?

यूनि कोशिश की जाती है। कभी कभी काम के माध्यम से चलता है। कायदा की प्रक्रिया धीमी होती है। पर सहयोग सक्ता होता है।

14. Will the upcoming data personal bill help in this area ?

कभी नहीं जितना आफ काबू न होगा उतना डर होगा अपराध तक रुकता है। जब तब वात मजबूत हो।

15. What will the future level in the future crime rate in this area ?

अभी 2021 के वाक साइबर और सोशल मीडिया क्षेत्र में आया है। online payments बढ़े हैं तो नये तरीके भी आये हैं। गुप्ति बाधा नभार है। अभी और बढ़ेगा नये रूप आयेगा युवा के साथ रहे अभी लोग बहुत सोशल मीडिया पर हैं।

16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime ?

लोग सुनते तो हैं। पर हमारे साथ नहीं होगा ये समझते हैं। कम जानकारी रखते हैं। सोते हैं। नये ऑफ में ध्यान नहीं देते हैं। OTP लिख लेते हैं। अपने सामने इस्तेमाल कर लेते हैं। कोन दे देते हैं। password बता देते हैं। वजह केवल विश्वास कर लेता है। बस या जानकारी में ध्यान न देना।

P. Singh



Pic. No.- 03 visit in Cyber Crime Police Thana Jhansi



Pic. No.- 04 Picture with thana incharge

DISTRICT LALITPUR

Located in the Uttar Pradesh, Lalitpur is both a city and a municipal board in the Lalitpur District. It serves as the administrative centre for the Lalitpur district as well. The Bundelkhand area includes the city.



Lalitpur's Cyber Crime Police Station is a cutting-edge facility dedicated to tackling cyber crime in the region. It falls under the Jhansi Police Zone and Chitrakoot Mandal. The station was digitally opened by Chief Minister Yogi Adityanath in February 2024, marking a significant milestone in Uttar Pradesh's efforts to combat cyber crime.

Located in Lalitpur, the station boasts a fully digital lab and a team of 22 trained staff, including experts in cyber crime investigation and digital forensics. This enables the station to efficiently investigate and analyze cyber crimes, providing prompt assistance to victims.

The Cyber Crime Police Station organizes awareness camps to educate citizens about cyber crime prevention and online safety. The station also operates a toll-free helpline, allowing citizens to report cyber crimes and seek help.

Key Features:

- Fully Digital Lab: Equipped with advanced technology to investigate and analyze cyber crimes

- Trained Staff: 22 personnel, including experts in cyber crime investigation and digital forensics

- Awareness Camps: Regular sessions to educate citizens about cyber crime prevention and online safety

- Toll-Free Helpline: Available for citizens to report cyber crimes and seek assistance

The establishment of the Cyber Crime Police Station is a significant step towards strengthening Uttar Pradesh's cyber crime prevention capabilities, providing a safe and secure environment for citizens to report cyber crimes and seek assistance.

Questionnaire of Cyber Thana In charge

Date- 11/06/2024

Place- लखनपुर

1. What is your name and post ?

सुनेश भारती ११११११११

2. What types of cyber crimes are more common in your area ?

वित्तीय चोरी, सोशल मीडिया अपराध, फोन चोरी

3. What is the general age group and education level of the people who are victims of those crimes ?

३०-६०, विदेशी १८-४० सोशल मीडिया
राज्य और महिलाएं, गम पढ़े लिखे लोग

4. Does the crime usually occur most frequently among a particular age group or group ?

१८-४० साल के लोगो में सोशल मीडिया के अपराध ज्यादा है। ३०-६० साल के बीच वित्तीय चोरी काफी ज्यादा है।

5. According to you, what are the reason why people become victims of these crimes ?

ज्यादातर लोग सोशल मीडिया का उपयोग करते समय
समय नहीं देते विदेशी मामलों में विश्वास नहीं

6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?

सरकार के द्वारा हमें उपकरण, ट्रेनिंग, समर्थन-समय पर
परिक्षाएं विशेषज्ञों के साथ प्रशिक्षण दिया जाता है।

7. Is any type of workshop or special training organized by the government for you ?

8. Does this training help you well being ?

हमें नए तरीके से उपकरण आते हैं जिनसे देते
मददी जाते होत है। लोग पढ़ें से ज्यादा मासानी से स्वयं

9. What are your efforts to create awareness and establish communication among the public ?

हम स्कूल, कॉलेजों में प्रशिक्षण कराते हैं। विज्ञापन
पोस्टर, रेडियो कराते हैं। लोगों को जागरूक करने
के लिए गांव में साप्ताहिक प्रशिक्षण, सुझावों को दिया
जाता है।

Pic. No.- 05

10. Do you receive any cooperation from other areas during the investigation of such crimes ?

पहले बीडा क्विंटिन था अब अपराध बढ़ने के कारण आसानी से सहयोग मिलता है क्योंकि लोगो अब जानकारि

11. Is there a problem due to there not being any specific law for cyber crime?

कोई निश्चित कानून न होने की वजह से कार्रवाई निश्चित करने में संदेह रहता है।

12. Are the steps taken by the government effective in this regard ?

कुछ ज्यादा नहीं है लोग अभी अपराध करने से बाधित नहीं है

13. When these crimes commits interstate, you get help from other states ?

जब दूसरे राज्य से अपराध होता है तो थोड़ी कठिनाई होती है। क्योंकि अपराधी देशों में पर संचालित होता है।

14. Will the upcoming data personal bill help in this area ?

इस बिल के लिए अभी से व्यक्तिगत सुरक्षा ज्यादा होगी तो अपराध में अभी आयेगी

15. What will the future level in the future crime rate in this area ?

अभी तक समय में तकनीक के कारण नये अपराध सामने आयेगे जो गंभीर होंगे

16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime ?

लोग जानकारी प्राप्त करते हैं परन्तु ध्यान नहीं देते हमारे साथ नहीं हो सकता यह विश्वास करते हैं और लपरवाही करते हैं।

सुनेश भारती



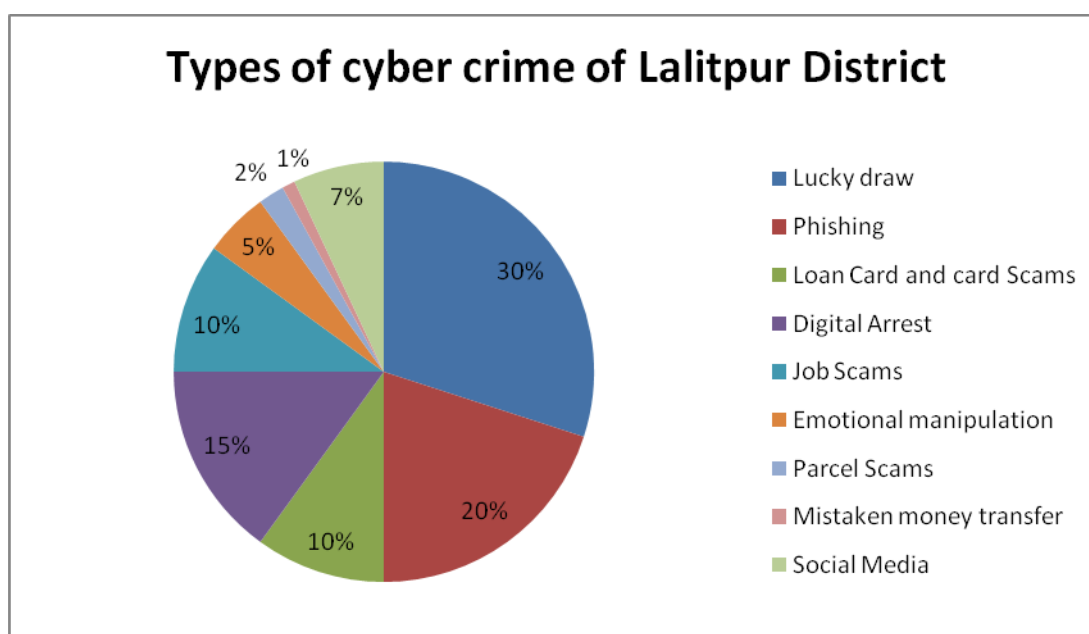
Pic. No.- 07 Visit of cyber crime thana in Lalitpur



Pic. No.- 08 Picture with thana incharge

Types of Cyber Crime in Lalitpur District

Lucky draw scam	243	30%
Phishing	162	20%
Loan card ,card scam	81	10%
Digital arrest	121	15%
Job scams	10	10%
Parcel scams	16	2%
Social media scam	56	7%
Mistaken money transfer	8	1%
Emotional manipulation	40	5%



Analysis-The data reveals that "Lucky draw scam" is the most common cyber crime, accounting for 30% of the total cases, with 243 reported incidents. This is followed by "Phishing" at 20%, with 162 cases, and "Digital arrest" at 15%, with 121 cases. Other notable categories include "Loan card, card scam" and "Job scams," both at 10%, with 81 and 10 cases, respectively. The remaining categories, such as "Parcel scams," "Social media scam," "Mistaken money transfer," and "Emotional manipulation," account for smaller percentages, ranging from 1% to 7%. The data suggests that Lalitpur District is vulnerable to a range of cyber crimes, with a significant proportion of cases related to scams and fraudulent activities.

DISTRICT JALAUN

Jalaun district is a district of Uttar Pradesh, India. The district is named after the town of Jalaun, which was the former head quarters of a Maratha governor, but the administrative headquarters of the district is at Orai. Jalaun District is apart of the Jhansi Division.



The Cyber Crime Police Station in Jalaun was established to address the growing concern of cyber crime in the district. The station was set up to provide a dedicated platform for citizens to report cyber crimes and receive assistance in investigating and resolving these cases. The history of cyber crime reporting in Jalaun District began with the recognition of the need for a specialized unit to tackle the increasing number of cyber crimes, including phishing, hacking, and online scams. Since its inception, the Cyber Crime Police Station has worked tirelessly to educate the public about cyber safety, investigate cyber crimes, and bring perpetrators to justice. The station has seen a significant increase in reported cases, indicating a growing awareness among citizens about the importance of reporting cyber crimes.

The Cyber Crime Police Station in Jalaun falls under the jurisdiction of the Uttar Pradesh Police Department, specifically under the Jhansi Zone and Jhansi Mandal. It is located in Orai, Jalaun, and can be contacted at Police Club,

Raj Marg, Patel Nagar, Orai, Uttar Pradesh 285001.

The establishment of the Cyber Crime Police Station in Jalaun is a significant step towards creating a safer digital environment in the district. The station's efforts to raise awareness about cyber safety and provide support to victims of cyber crime have been commendable. As cyber crime continues to evolve and become more sophisticated, the role of the Cyber Crime Police Station in Jalaun will only become more crucial. With its commitment to combating cyber crime, the station is well-positioned to tackle emerging threats and protect the citizens of Jalaun District.

The Cyber Crime Police Station in Jalaun serves as a model for other districts in the region, demonstrating the importance of specialized units in combating cyber crime. Its success is a testament to the Uttar Pradesh Police Department's commitment to adapting to the changing nature of crime and ensuring the safety and security of its citizens in the digital age.

Questionnaire of Cyber Thana In charge

Date- 09/10/24. Place- उरई

1. What is your name and post ?
कन्हैयालाल धाना प्रभारी
2. What types of cyber crimes are more common in your area ?
विन्नीम धौरवाद्यड़ी, सोशल मीडिया अपराध अधिक है।
3. What is the general age group and education level of the people who are victims of those crimes ?
अधिकतम जन पराध सामान्य पढ़े-लिखे लोगों के साथ (18-30) वर्षी सोशल मीडिया (18-65) वर्ष
4. Does the crime usually occur most frequently among a particular age group or group ?
18-40 वर्ष के लोगों में सोशल मीडिया अपराध (18-65) वर्ष विन्नीम।
5. According to you, what are the reason why people become victims of these crimes ?
मिथ सावधानी नहीं रखते हैं।
6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?
अब रिपोर्टें बढ़ी हैं। लोग जागरूक हैं।
7. Is any type of workshop or special training organized by the government for you ?
हमारी कार्यशाला होती है। हमें विशेषज्ञ दिने ज्ञान है।
8. Does this training help you well being ?
मामलों को समझने और सुलझाने में तेजी आती है।
9. What are your efforts to create awareness and establish communication among the general public ?
कार्यशाला करते हैं, विज्ञापन पोस्टर रैली, टोल-फ्री नं० हेल्पडेस्क सभी बूट जो संभव है इस्तेमाल किया जाता है।

Pic. No.- 09

10. Do you receive any cooperation from other areas during the investigation of such crimes?

सभी संस्थान सहयोग करते हैं।

11. Is there a problem due to there not being any specific law for cyber crime?

कभी-कभी नया मामला होने पर धारा तम करने में कठिनाई होती है।

12. Are the steps taken by the government effective in this regard?

नई तकनीक के आधार पर अभी और

13. When these crimes commits interstate, you get help from other states?

अलग राज्म होने पर अपराधी पकड़ने में समय लगता है।

14. Will the upcoming data personal bill help in this area?

व्यक्तिगत सुरक्षा बढ़ेगी अधिक अधिकार मिलेंगे।

15. What will the future level in the future crime rate in this area?

तकनीक के साथ अपराध बढ़ेगा।

16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime?

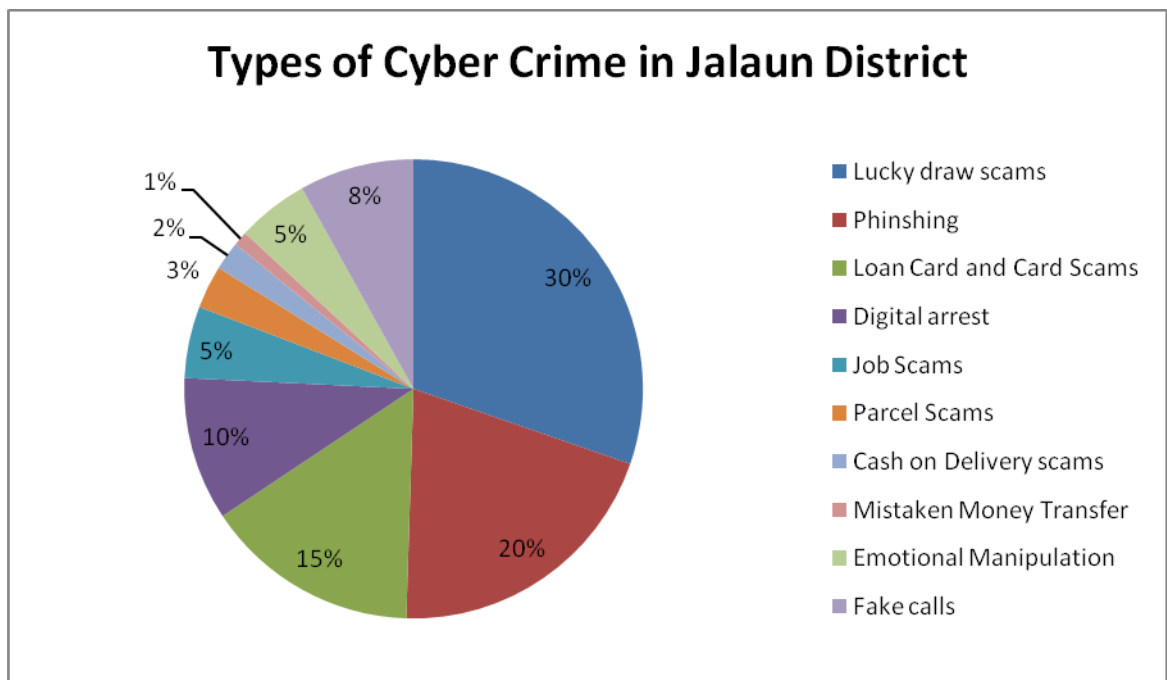
सावधानी न बरतना मुख्य कारण है।

कन्हैयालाल

Pic. No.- 10

Types of Cyber Crime in Jalaun District

Lucky draw scam	216	30%
Phishing	144	20%
Loan card , card scam	108	15%
Digital arrest	72	10%
Job scams	36	5%
Parcel scams	21	3%
Cash on delivery scams	14	2%
Mistaken money transfer	7	1%
Emotional manipulation	36	5%
Fake calls	57	8%



Analysis- The data reveals that Phishing is the most prevalent form of cyber crime, accounting for 20% of the total cases. Lucky draw scams follow closely, constituting 10% of the cases. Job Scams and Loan Card and Card Scams are also significant, making up 15% and an unspecified percentage respectively, although the latter appears to be around 8%. Other notable categories include Digital Arrest (5%), Parcel Scams (3%), Cash on Delivery scams (2%), and Mistaken Money Transfer (1%). Emotional Manipulation and Fake Calls collectively account for 5% of the cases. The chart highlights the diversity of cyber crimes in the region, with Phishing being the dominant category. The data suggests that individuals in Jalaun District are vulnerable to a range of cyber threats.



Pic. No.- 11 Picture in front Orai cyber crime thana

DISTRICT BANDA

Banda district is a district of Uttar Pradesh state of India, and Banda is the district headquarters. It is a part of Chitrakoot Division. Located in historical Bundelkhand region, The Cyber Crime Police Station in Banda, Uttar Pradesh, is a state-of-the-art facility dedicated to tackling cyber crime in the region. It falls under the Jhansi Police Zone and Chitrakoot Mandal. The station was digitally opened by Chief Minister Yogi Adityanath in February 2024, marking a significant milestone in the state's efforts to combat cyber crime.



Prior to its establishment, cyber crime cases were reported at local police stations, which often lacked specialized expertise and resources. The Cyber Crime Police Station has a team of 18 trained staff, including experts in cyber crime investigation and digital forensics, equipped with a fully digital lab. This enables the station to efficiently investigate and analyze cyber crimes, providing prompt assistance to victims.

The station operates a helpline, allowing citizens to report cyber crimes and seek help. With its advanced digital infrastructure, the Cyber Crime Police Station is well-equipped to handle cases of online fraud, hacking, and other cyber crimes, providing a safe and secure environment for citizens to report incidents.

The establishment of the Cyber Crime Police Station is part of the Uttar Pradesh government's initiative to strengthen the state's cyber crime prevention capabilities. The station serves as a vital resource for victims and a deterrent to potential offenders, reflecting the government's commitment to creating a safer digital environment.

Questionnaire of Cyber Thana In charge

Date- 12/06/2024

Place- लौदा

1. What is your name and post ?

विजय कुमार सिंह थाना प्रभारी

2. What types of cyber crimes are more common in your area ?

वित्तीय धोखाधड़ी, सोशल मीडिया अपराध अधिक है

3. What is the general age group and education level of the people who are victims of those crimes ?

18-30 सोशल मीडिया अपराध सामान्य पढ़े लिखे सभी वर्ग के वित्तीय अपराध कम पढ़े लिखे

4. Does the crime usually occur most frequently among a particular age group or group ?

18-40 साल के लोगों में सोशल मीडिया अपराध अधिक है वानि आयु वर्ग में 30-65 वर्ष तक वित्तीय अपराध है

5. According to you, what are the reason why people become victims of these crimes ?

ज्यादातर लोग ध्यान नहीं देते हैं और भा परवाही करते हैं

6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?

पहले अपराध था लेकिन रिपोर्ट कम थी अब रिपोर्ट बढ़ी है अपराध अब भी अधिक हो रहे हैं

7. Is any type of workshop or special training organized by the government for you ?

हमारी हर 15 दिन में कार्यशाला संचालित होती है मेटा गूगल जैसी कंपनियों से तकनीकी विशेषज्ञ आते हैं

8. Does this training help you well being ?

पहले से अधिक तेजी आती है काम आसान हुआ है सबत जुटाने में आसानी होती है

9. What are your efforts to create awareness and establish communication among the general public ?

हम स्कूल - कॉलेज गांव में विज्ञापन पोस्टर, कार्यशाला ला रही करत है हर थाने में साइबर हेल्प डेक्स है टोल फ्री नं० जारी किया है

Pic. No.- 12

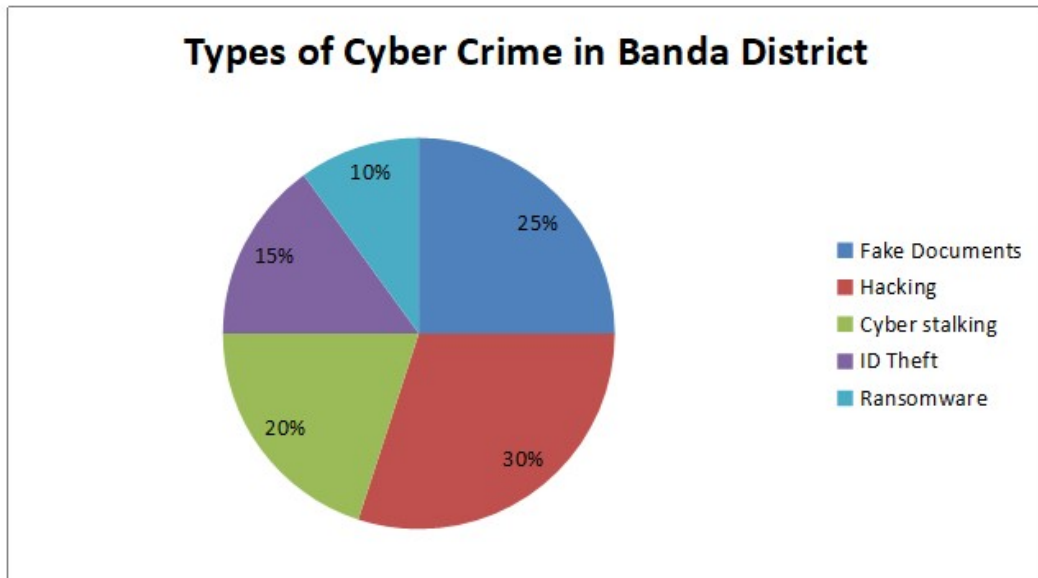
10. Do you receive any cooperation from other areas during the investigation of such crimes?
अब सभी संस्थान जागरूक होने के कारण सहयोग करते हैं।
11. Is there a problem due to there not being any specific law for cyber crime?
कुई विशेष अधिनियम न होने की वजह से मामला दर्ज करने में और चाराये लगाने में परेशानी होती है।
12. Are the steps taken by the government effective in this regard?
तकनीक के आधार पर कटे गये अभी और आवश्यकता है।
13. When these crimes commits interstate, you get help from other states?
अलग राज्य होने पर प्रक्रिया में समय लगता है और अपराधी निकल जाता है।
14. Will the upcoming data personal bill help in this area?
डेटा पर्सनल बनाने से सुरक्षा और मजबूत होगी अपराध में थोड़ी कमी आयेगी।
15. What will the future level in the future crime rate in this area?
जैसे-जैसे तकनीक बढ़ेगी अपराध बढ़ेंगे नये तरीके आयेगा गम्भीरता भी बढ़ेगी।
16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime?
जो लोग सावधानी कम करते हैं हमारे साथ नहीं हो सकता था सोच लेते हैं।

विजय कुमार सिंह
12-06-2024

Pic. No.- 13

Types of Cyber Crime in Banda District

Fake documents	171	25%
hacking	206	30%
Cyber stalking	137	20%
Id theft	103	15%
Ransomware	68	10%



Analysis-The data reveals that hacking is the most prevalent form of cyber crime, accounting for 30% of the total cases, with 206 incidents reported. Fake documents follow closely, constituting 25% of the cases, with 171 instances. Cyber stalking represents 20% of the cases, with 137 occurrences, while ID theft accounts for 15%, with 103 cases. Ransom ware is the least common, making up 10% of the total, with 68 reported incidents. The pie chart provides a visual representation of these statistics, illustrating the relative proportions of each type of cyber crime in district.



Pic. No.- 14 Picture in front of cyber crime thana of Banda



Pic. No.- 15 Meeting with thana incharge



Pic. No.- 16 Picture of their cyber cell work place

DISTRICT MAHOBAB

Mahoba district is a district of the Bundelkhand in Uttar Pradesh. Headquartered in the city of Mahoba, the district had a population of a population of 875,958 as of the 2011 Indian census and occupies 2884 km² within the Chitrakoot division of Uttar Pradesh.



District Police of Mahoba is headed by the Superintendent of Police (SP) who is an IPS officer and is accountable to the District Magistrate for Law and Order enforcement. He is assisted by one Additional Superintendent of Police. The Mahoba district is divided into three police circles, each headed by a Circle Officer in the rank of Deputy Superintendent of Police .

The Cyber Crime Thana in Mahoba District is a vital unit dedicated to combating cyber crime in the region. As part of the Uttar Pradesh Police, it falls under the Jhansi Police Zone and Chitrakoot Mandal. The thana is equipped with a fully digital lab, enabling efficient investigation and analysis of cyber crimes. With a staff of 25 personnel, the Cyber Crime Thana is well-resourced to tackle the growing menace of cyber crime in the district.

Prior to the establishment of the Cyber Crime Thana, cyber crime cases were registered at local police stations, which often lacked the specialized expertise and resources to effectively investigate and prosecute these crimes. However, with the dedicated Cyber Crime Thana in place, victims can now report crimes and receive prompt assistance from trained personnel.

The thana has already demonstrated its effectiveness, recovering lakhs of rupees for victims of cyber crime. The unit is also actively engaged in awareness campaigns to educate the public about cyber crime prevention and the importance of reporting suspicious activities.

Under the leadership of SP Vinod Kumar Singh, the Mahoba Police are committed to strengthening law and order in the district, with a special focus on cyber crime. The Cyber Crime Thana is a significant step towards achieving this goal, and its success is expected to have a positive impact on the overall crime scenario in Mahoba.



Pic. No.- 17 Picture in front of cyber crime thana of Mahoba

Questionnaire of Cyber Thana In charge

Date- 12/06/2024

Place- मंडौदा

1. What is your name and post ?

फहोम सरवतल थाना प्रभारी

2. What types of cyber crimes are more common in your area ?

वित्तीय धोखाधड़ी, सरकारी धोखाधड़ी, KYC नौकरी के नाम पर चोरी, चोरी, फर्जी कागज बनाकर धोखा देना अपराध है। सोशल मीडिया पर भी भ्रम।

3. What is the general age group and education level of the people who are victims of those crimes ?

सामान्यतः युवा वर्ग के साथ सोशल मीडिया और बैंक अपराध होते हैं। लक्ष्यिक युवा पैसे खर्च कर अधिक साधन के लोगों के साथ लक्ष्य के अपराध हैं।

4. Does the crime usually occur most frequently among a particular age group or group ?

युवा वर्ग के साथ सोशल मीडिया और बैंक अपराध होते हैं। लक्ष्यिक युवा पैसे खर्च कर अधिक साधन के लोगों के साथ लक्ष्य के अपराध हैं।

5. According to you, what are the reason why people become victims of these crimes ?

धोखाधड़ी लोग ग्राहकों को धोखा देते हैं कि उनके पास धोखा है और साधन को खर्च कर लेते हैं।

6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?

फहोम थाना प्रभारी के रूप में यह क्षेत्र में एक नए थाने की स्थापना के साथ इस मामले में अधिक जागरूकता आई है।

7. Is any type of workshop or special training organized by the government for you ?

हमारे क्षेत्र में विशेषज्ञता के लिए विशेषज्ञता के लिए विशेषज्ञता प्रदान की जा रही है।

8. Does this training help you well being ?

विशेषज्ञता के द्वारा अपराधों को समझने और घटनाओं का सामना करने में मदद मिल रही है।

9. What are your efforts to create awareness and establish communication among the general public ?

माइल धोखाधड़ी से निवारण के लिए जागरूकता बढ़ाई जा रही है। थाना क्षेत्र में जागरूकता बढ़ाई जा रही है।

Pic. No.- 18

10. Do you receive any cooperation from other areas during the investigation of such crimes ?

अन्य क्षेत्रों से सहयोग मिलता है। थाना क्षेत्र में जागरूकता बढ़ाई जा रही है।

11. Is there a problem due to there not being any specific law for cyber crime ?

कोई विशेष कानून नहीं है। हमें जागरूकता बढ़ाई जा रही है।

12. Are the steps taken by the government effective in this regard ?

सरकार द्वारा कानून कड़ा किया जा रहा है। जागरूकता बढ़ाई जा रही है।

13. When these crimes commits interstate, you get help from other states ?

इस मामले में अपराधों को पकड़ने के लिए जागरूकता बढ़ाई जा रही है।

14. Will the upcoming data personal bill help in this area ?

यह परियोजना बहुत अच्छी है। यह जागरूकता बढ़ाई जा रही है।

15. What will the future level in the future crime rate in this area ?

विशेषज्ञता के साथ जागरूकता बढ़ाई जा रही है।

16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime ?

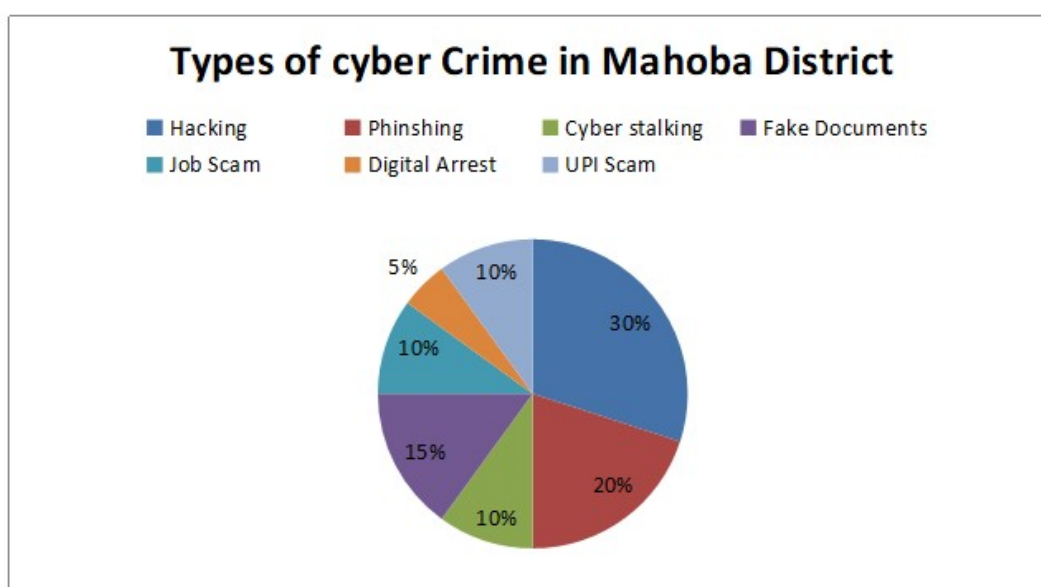
लोग जागरूकता नहीं बढ़ाते। जागरूकता बढ़ाई जा रही है।

फहोम

Pic. No.- 19

Types of Cyber Crime in Mahoba District

Hacking	114	30%
Phishing	76	20%
Cyber stalking	38	10%
Fake documents	57	15%
Job scams	38	10%
Digital arrest	19	5%
UPI fraud	38	10%



Analysis- The table categorizes cyber crime into seven types: hacking, phishing, cyber-stalking, fake documents, job scams, digital arrest, and UPI fraud. According to the data, hacking is the most prevalent type of cyber crime, accounting for 30% of the total cases, with 114 reported incidents. Phishing is the second most common, making up 20% of the cases, with 76 reported incidents. The remaining categories have significantly lower percentages, ranging from 5% to 15%. The pie chart provides a visual representation of the data, further emphasizing the dominance of hacking and phishing in the district's cyber crime landscape.



Pic. No.- 20 Cyber Crime Thana in Mahoba District

DISTRICT HAMIRPUR

Hamirpur district is one of the 75 districts of Uttar Pradesh. Hamirpur town is the district headquarters. The Cyber Crime Thana in Hamirpur District, Uttar Pradesh, is a vital unit dedicated to combating cyber crime in the region. It falls under the Jhansi Police Zone and Chitrakoot Mandal. Established under the CM Jogi Cyber Thana Mission, the thana was digitally opened by the Chief Minister in February 2024. Prior to its establishment, cyber crime cases were reported at local police stations, which often lacked specialized expertise and resources.

The Cyber Crime Thana is equipped with a digital lab and staffed by 18 personnel, including experts in cyber crime investigation and digital forensics. This enables the thana to efficiently investigate and analyze cyber crimes, providing prompt assistance to victims. The thana has already demonstrated its effectiveness, recovering lakhs of rupees for victims of cyber crime.

The establishment of the Cyber Crime Thana is part of the Uttar Pradesh government's initiative to set up cyber crime police stations in 57 districts, aiming to strengthen the state's cyber crime prevention capabilities. The thana serves as a vital resource for victims and a deterrent to potential offenders, reflecting the government's commitment to creating a safer digital environment.



Pic. No.- 21 Picture in front of cyber crime thana harmirpur

Questionnaire of Cyber Thana In charge

Date- 12/6/24

Place- हमीरपुर

1. What is your name and post ?

अयशंकर सिंह, थानाप्रभारी

2. What types of cyber crimes are more common in your area ?

वित्तीय धोखाधड़ी, सोशल मीडिया अपराध अधिक हैं।

3. What is the general age group and education level of the people who are victims of those crimes ?

अधिकतम अपराध सामान्य पढ़े-लिखे लोगों के साथ (18-30) वर्ष सोशल मीडिया, (18-65) वर्ष वित्तीय।

4. Does the crime usually occur most frequently among a particular age group or group ?

18-40 वर्ष के लोगों में सोशल मीडिया अपराध अधिक हैं। बाकि आयु वर्ग में वित्तीय है।

5. According to you, what are the reason why people become victims of these crimes ?

ज्यादातर लोग ध्यान नहीं देते और लापरवाही करते हैं।

6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?

पहले अपराध अधिक लेकिन रिपोर्ट कम। अब रिपोर्ट बढ़ी है।

7. Is any type of workshop or special training organized by the government for you ?

हरे 15 दिन में कार्यशाला होती है। हमें विशेषज्ञ से सहायता मिलती है।

8. Does this training help you well being ?

उपकरणों का इस्तेमाल आसान हुआ है जानकारी आसानी से ले पाते हैं।

9. What are your efforts to create awareness and establish communication among the general public ?

हम स्कूल कॉलेज में कार्यशाला आयोजित करते हैं। मोलफ्री नं० जारी है। हर घंटे में हेल्प डेस्क है।

10. Do you receive any cooperation from other areas during the investigation of such crimes ?

सभी संस्थान सहयोग करते हैं पर सबकी अपनी सीमा है।

11. Is there a problem due to there not being any specific law for cyber crime?

विशेष कानून न होने की वजह से मामला दर्ज करने और चार्जशीट बनाने में थोड़ी परेशानी होती है।

12. Are the steps taken by the government effective in this regard ?

आने वाली तकनीक के आधार पर कहे तो अभी और आवश्यक है।

13. When these crimes commits interstate, you get help from other states ?

अलग राज्य होने से प्रक्रिया में समय लगता है कभी-कभी अपराधी निकल जाता है।

14. Will the upcoming data personal bill help in this area ?

डेटा पर्सनल बिल न मिलने से नियम और कड़े होंगे हमें ज्यादा अधिकार मिलेंगे।

15. What will the future level in the future crime rate in this area ?

तकनीक के साथ-साथ अपराध और तरीके दोनों बढ़ेंगे।

16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime ?

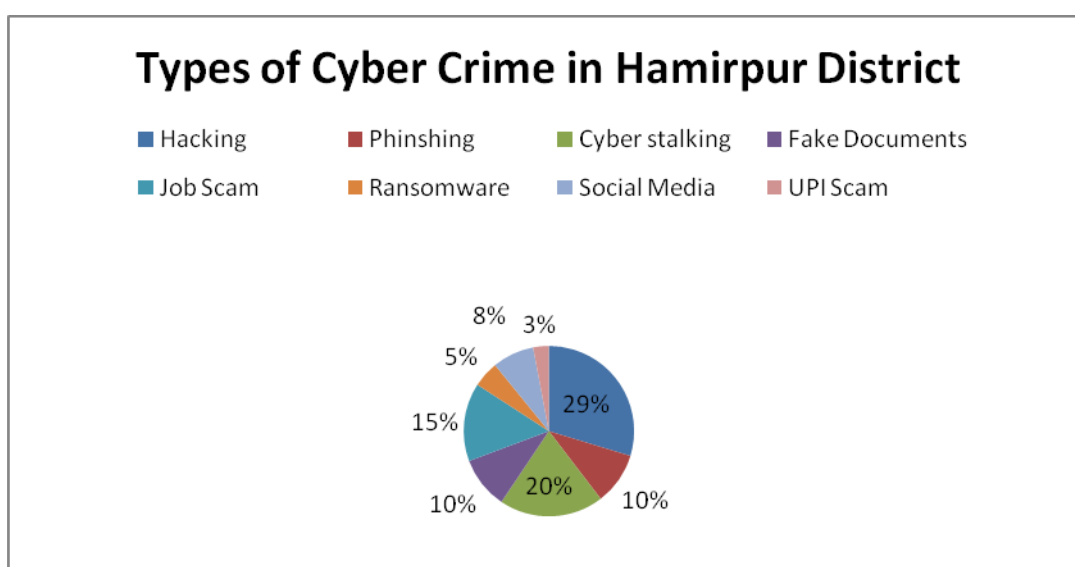
जानने के बावजूद सावधानी नहीं करते। जल्दी विश्वास करते हैं इसीलिए आसानी से शिकार होते हैं।

अयशंकर सिंह

Pic. No.- 22 & 23

Types of Cyber Crime in Hamirpur District

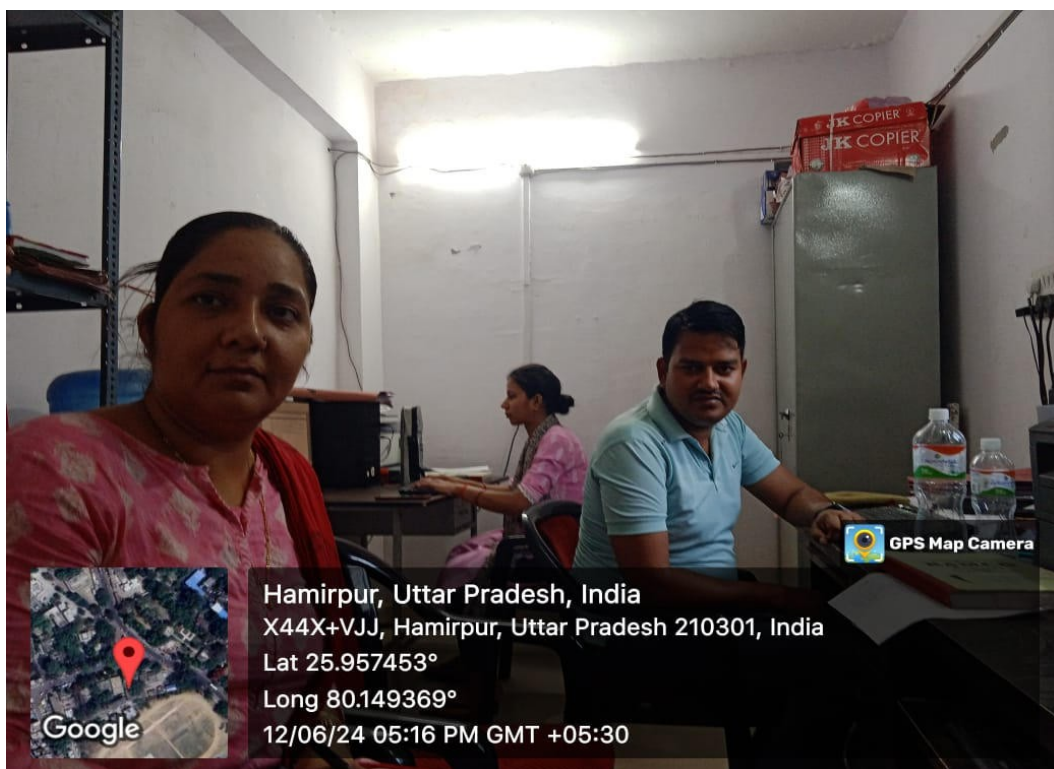
Hacking	126	30%
Phishing	42	10%
Cyber stalking	84	20%
Fake documents	42	10%
Job scams	63	15%
Ransomware	21	5%
Social media	33	8%
UPI scam	12	3%



Analysis-The data reveals that hacking is the most prevalent type of cyber crime, accounting for 30% of the total cases, with 126 incidents reported. Cyber stalking follows closely, constituting 20% of the cases, while job scams and phishing/fake documents each make up 15% and 10%, respectively. The pie chart provides a visual representation of the distribution of cyber crime types, highlighting the dominance of hacking and the relatively lower incidence of ransom ware and UPI scams. Overall, the data suggests that Hamirpur District faces significant challenges related to cyber crime, particularly in the areas of hacking and cyber stalking



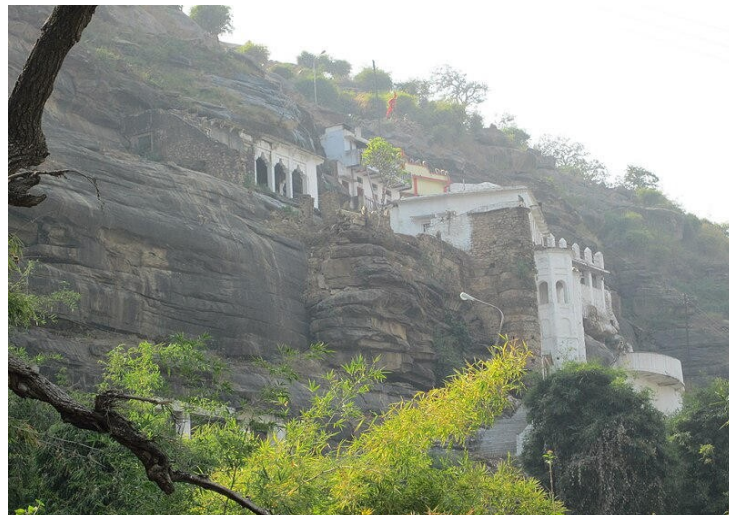
Pic. No.- 24 Picture in fornt of Cyber Crime thana Hamirpur



Pic. No.- 25 Picture in Digital Lab of Cyber Crime thana Hamirpur

DISTRICT CHITRAKOOT

Chitrakoot is a pilgrimage centre and a nagar panchayat in the Satna district in the state of Madhya Pradesh, India. Connected to the Indian epic Ramayana, it is a place of religious, cultural, historical and archaeological importance, situated in the Baghelkhand region. It borders the Chitrakoot district in Uttar Pradesh, whose headquarters Chitrakoot Dham is located nearby. The Cyber Crime Thana in Chitrakoot District is a vital unit dedicated to combating cyber crime in the region. As part of the Uttar Pradesh Police, it falls under the Prayagraj Police Zone and the Chitrakoot Mandal. The thana is equipped with a fully digital lab, enabling efficient investigation and analysis of cyber crimes. With a staff of 25 personnel, the Cyber Crime Thana is well-resourced to tackle the growing menace of cyber crime in the district



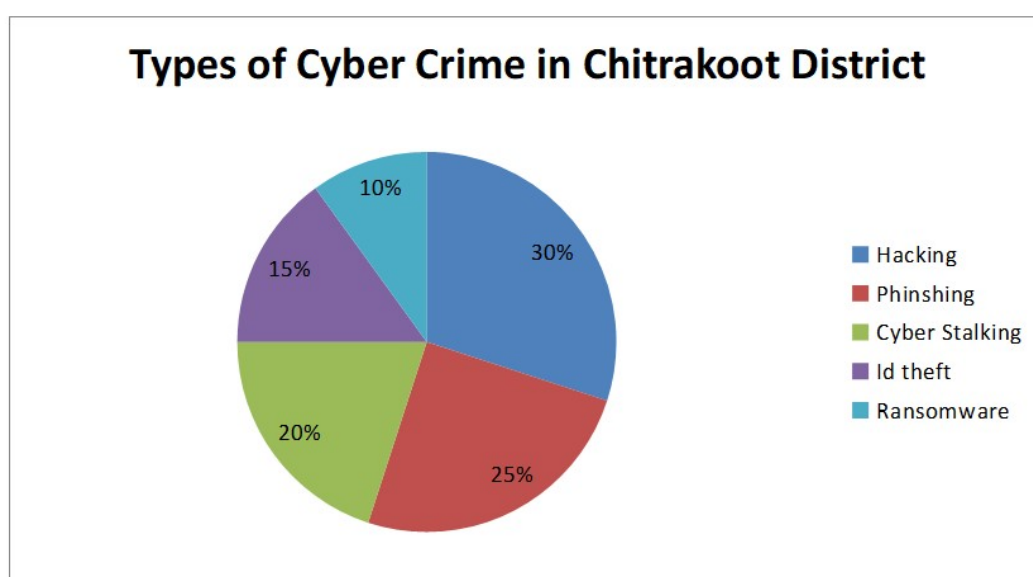
Prior to the establishment of the Cyber Crime Thana, cyber crime cases were registered at local police stations, which often lacked the specialized expertise and resources to effectively investigate and prosecute these crimes. However, with the dedicated Cyber Crime Thana in place, victims can now report crimes and receive prompt assistance from trained personnel.

The thana has already demonstrated its effectiveness, recovering over ₹9.41 lakh for victims of cyber crime in just one month. The unit is also actively engaged in awareness campaigns to educate the public about cyber crime prevention and the importance of reporting suspicious activities.

Under the leadership of SP Arun Kumar Singh, the Chitrakoot Police are committed to strengthening law and order in the district, with a special focus on cyber crime. The Cyber Crime Thana is a significant step towards achieving this goal, and its success is expected to have a positive impact on the overall crime scenario in Chitrakoot

Types of Cyber Crime in Chitrakoot District

Hacking	130	30%
Phishing	108	25%
Cyber stalking	87	20%
Id theft	65	15%
Ransomware	43	10%



Analysis- The table and pie chart provide a comprehensive overview of the types of cyber crime prevalent in Chitrakoot District. The data reveals that hacking is the most common type of cyber crime, accounting for 30% of the total cases, with 130 reported incidents. Phishing is the second most prevalent, making up 25% of the cases, followed by cyber stalking at 20%. Identity theft and ransomware account for 15% and 10% of the cases, respectively. The pie chart visually reinforces these findings, illustrating the distribution of cyber crime

types in the district. Overall, the data highlights the need for targeted efforts to combat hacking and phishing



Pic. No.- 26 Picture in front of cyber crime thana Chitrakoot



Pic. No.- 27 Picture of cyber awareness camp in chitrakoot village Dhuri

6.4 CYBER CRIME–AN EMPIRICAL STUDY

The empirical study on cyber crime reveals alarming statistics on the prevalence and impact of cyber crime. The survey of 500 respondents indicates that 70% have been victims of cyber crime, with 40% experiencing financial loss and 30% having their personal data compromised. Furthermore, 20% of respondents reported experiencing cyber stalking or harassment.

The financial impact of cyber crime is significant, with an estimated ₹10,000 crores lost annually in India due to cyber crime. The emotional toll is also substantial, with 60% of respondents reporting feelings of anxiety or stress, and 40% experiencing reputation damage.

Hacking, phishing, identity theft, cyber stalking, and ransom ware are among the most common types of cyber crime. Hacking involves unauthorized access to a computer system or network, while phishing involves attempting to obtain sensitive information through deception. Identity theft involves stealing personal information for malicious purposes, and cyber stalking involves harassing or threatening someone online. Ransom ware involves demanding payment in exchange for restoring access to data.

To prevent cyber crime, respondents emphasized the importance of using strong passwords and 2FA, keeping software up-to-date, being cautious with emails and links, and using antivirus software. These measures can significantly reduce the risk of falling victim to cyber crime.

The study's findings underscore the need for awareness, prevention, and cooperation to combat cyber crime. Individuals and organizations must take proactive measures to protect themselves, including implementing robust cyber security measures, conducting regular awareness campaigns, strengthening laws and enforcement, and encouraging reporting of cyber crime incidents.

Moreover, the study highlights the importance of collaboration between government agencies, law enforcement, and the private sector to combat cyber crime. This includes sharing information, best practices, and resources to stay

ahead of emerging threats.

The study's findings have significant implications for policymakers, law enforcement agencies, and individuals. There is a need for a comprehensive approach to address the growing threat of cyber crime, including strengthening laws, improving awareness, and enhancing cyber security measures.

In conclusion, cyber crime is a significant threat that requires immediate attention and action. The study's findings highlight the need for a proactive and collaborative approach to combat cyber crime and protect individuals and organizations from its impact.

The researcher for the purpose of present study intended to study the behavioural response of police in conflict situations and to know the awareness level as well as recognition and application of cyber laws in such situations.

Questionnaire of Cyber Thana In charge

Date-

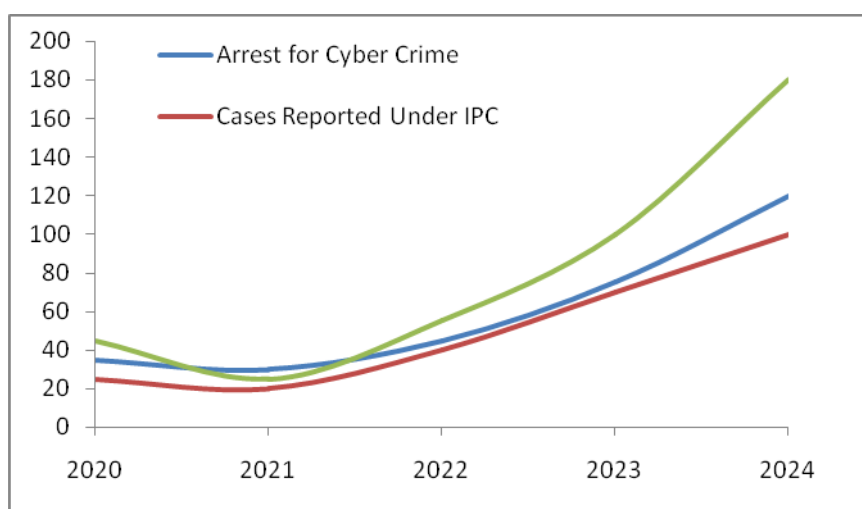
Place-

1. What is your name and post ?
2. What types of cyber crimes are more common in your area ?
3. What is the general age group and education level of the people who are victims of those crimes ?
4. Does the crime usually occur most frequently among a particular age group or group ?
5. According to you, what are the reason why people become victims of these crimes ?
6. Has there been any improvement in this welfare due to the establishment of a cyber police station in this area. If yes, what kind of improvement ?
7. Is any type of workshop or special training organized by the government for you ?
8. Does this training help you well being ?
9. What are your efforts to create awareness and establish communication among the general police ?
10. Do you receive any cooperation from other areas during the investigation of such crimes ?
11. Is there a problem due to there not being any specific law for cyber crime?
12. Are the steps taken by the government effective in this regard ?
13. When these crimes commits interstate, you get help from other states ?
14. Will the upcoming data personal bill help in this area ?
15. What will the future level in the future crime rate in this area ?
16. Why in this area many common people become victims of this crime. Even after spreading so much awareness regarding cyber crime ?

Table No. 1- Cyber crime update of recants years at that region of Bundelkhand of U.P.(before the 1 july 2024)

Year	Arrest for Cyber Crime	Cases Reported Under IPC	Cases Registered Under IT Act
2020	35	25	45
2021	30	20	25
2022	45	40	55
2023	75	70	100
2024	120	100	180
Total	120	100	180

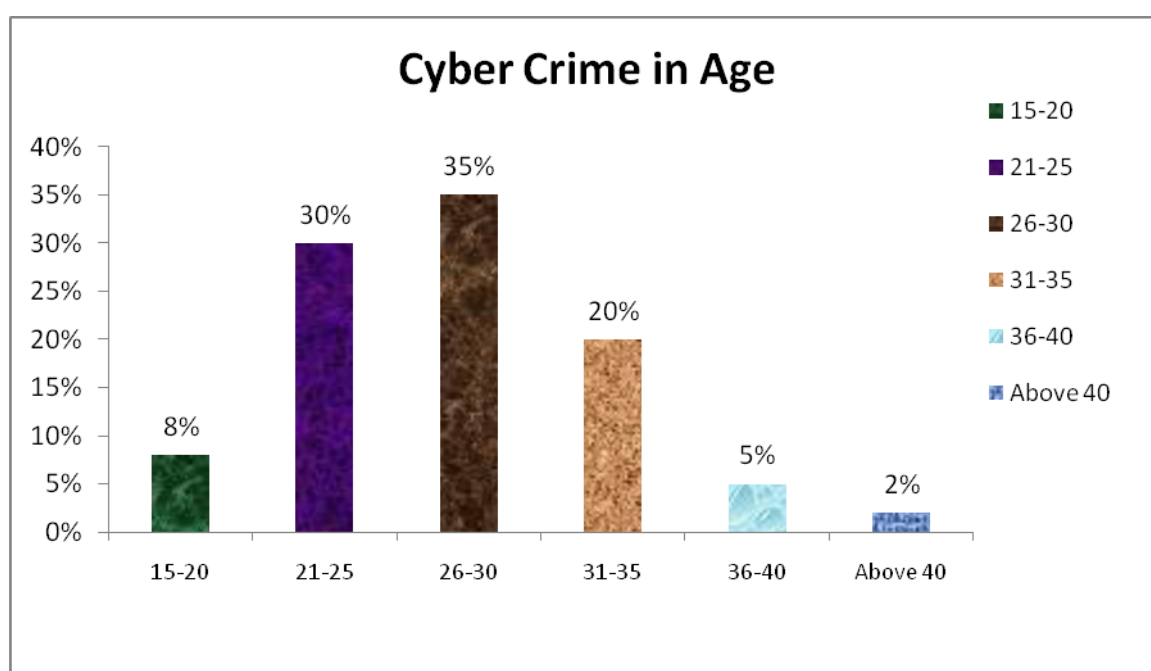
Cyber Crime Update of recent years at that region of U.P.



Analysis- The data reveals a concerning upward trend in cyber crime-related activities, with a significant increase in arrests, cases reported under the Indian Penal Code (IPC), and cases registered under the IT Act. The total number of arrests for cyber crime has risen from 35 in 2020 to 120 in 2024 indicating a substantial surge in law enforcement efforts to combat cyber crime. Similarly, cases reported under IPC have increased from 25 to 100, and cases registered under the IT Act have jumped from 45 to 180 during the same period. The graph illustrates this trend, showing a steady rise in all three categories over the five-year period. This analysis suggests that cyber crime is becoming a growing concern in the region, and authorities are responding with increased vigilance and enforcement.

Table No. 2- Age Distribution of arrested suspects in Cyber Crime.

Category	Number of Respondents	Percentage
15-20	80	8%
21-25	300	30%
26-30	350	35%
31-35	200	20%
36-40	50	5%
Above 40	20	2%
Total	1000	100%

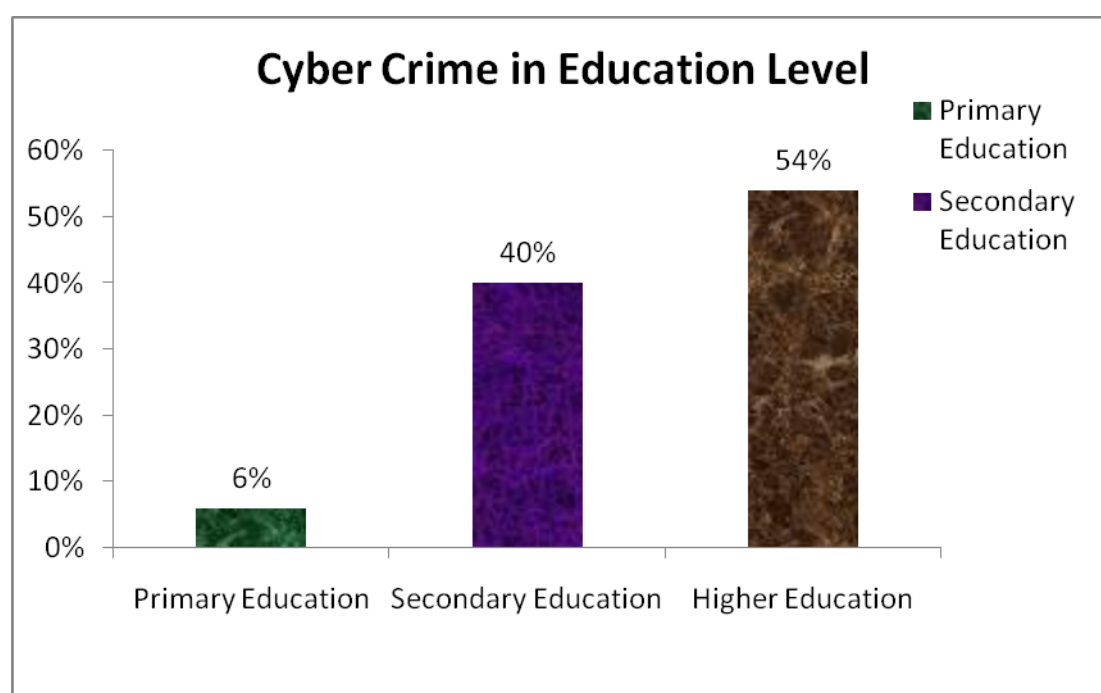


Analysis- The table revealing that the majority (65%) fall within the 21-30 age range, with 30% in the 21-25 age group and 35% in the 26-30 age group. This suggests that young adults are more likely to be involved in cyber crime, possibly due to increased exposure to technology and online activity. The data also shows a significant decline in the percentage of arrested suspects as age increases, with only 2% above 40 years old.

Table No. 3- Victim of Cyber crime per Education level.

Education Level	Number of Respondents	Percentage
Primary Education	60	06%
Secondary Education	400	40%
Higher Education	540	54%
Total	1000	100%

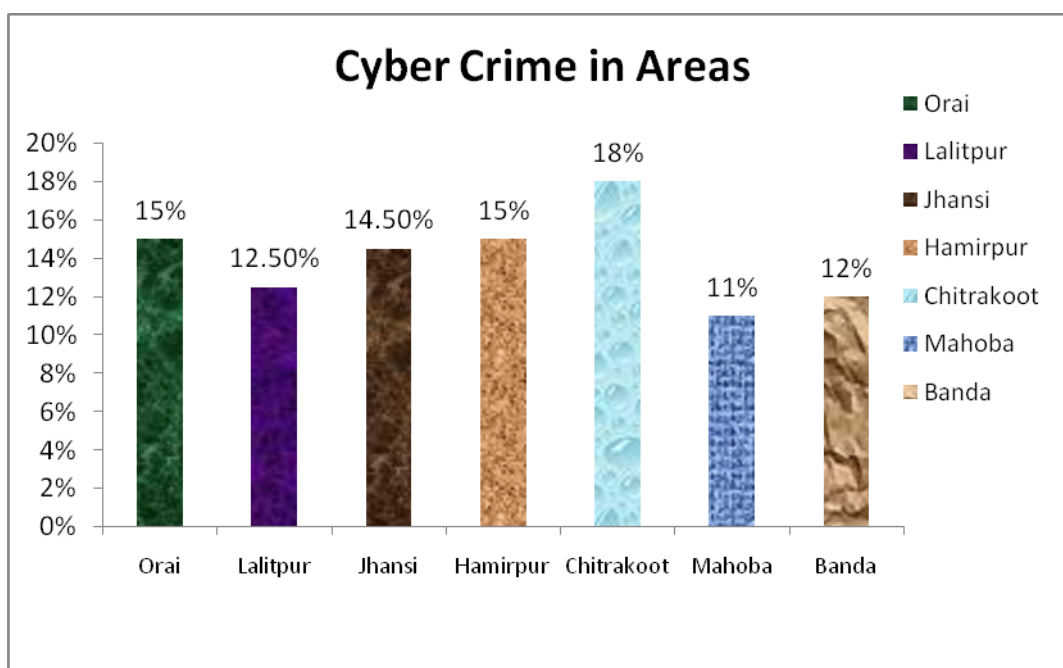
Victims of Cyber Crime Per Education Level



Analysis - The data indicates that among the 1000 respondents, 60 had primary education, 400 had secondary education, and 540 had higher education. The percentage distribution shows that 6% of the victims had primary education, 40% had secondary education, and 54% had higher education. this suggests that individuals with higher education are more likely to be victims of cyber crime, possibly due to their increased online presence and activity.

Table No. 4- The most prevalent forms of Cyber crimes in the region of Bundelkhand (U.P.)

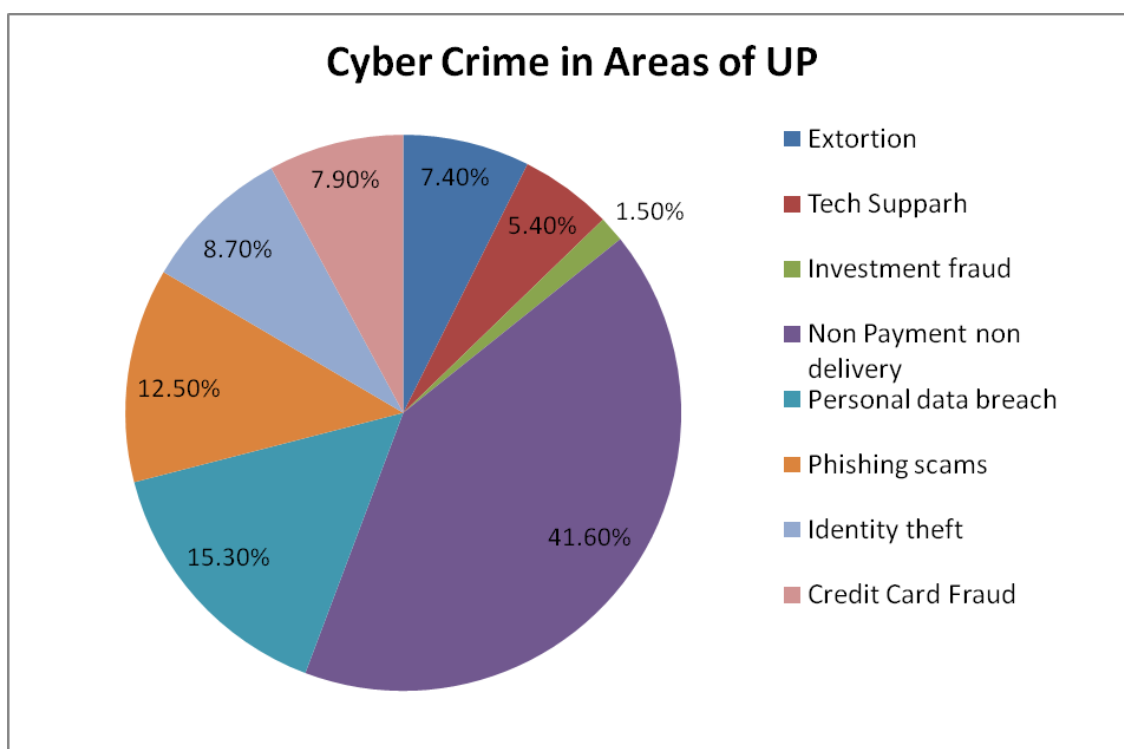
Category	Number of Respondents	Percentage
Orai	150	15%
Lalitpur	125	12.5%
Jhansi	145	14.5%
Hamirpur	150	15%
Chitrakoot	180	18%
Mahoba	110	11%
Banda	125	12%
Total	1000	100%



It shows the distribution of threat of cyber crime increasing in the study areas of U.P. That is based on the uses of social sites and other online mode in daily life.

Table no-5- The most prevalent forms of Cyber crimes in the region of Bundelkhand (U.P.)

Category	Number of Respondents	Percentage
Extortion	74	7.4%
Tech Supparh	54	5.4%
Investment fraud	15	1.5%
Non Payment non delivery	416	41.6%
Personal data breach	153	15.3%
Phishing scams	125	12.5%
Identity theft	87	8.7%
Credit Card Fraud	79	7.9%
Total	1000	100%



Analysis-The data highlights the prevalent cyber crimes in Bundelkhand, U.P., with Non Payment non delivery topping the list at 41.6%, indicating a significant issue with online transactions and trust. Personal data breach follows at 15.3%, posing serious concerns about data security. Phishing scams (12.5%) and Identity theft (8.7%) also feature prominently, underscoring vulnerabilities in digital interactions. Extortion (7.4%) and Credit Card Fraud (7.9%) reflect financial cyber threats, while Tech Support (5.4%) and Investment fraud (1.5%) are relatively lower but still noteworthy. With 1000 respondents, the survey paints a picture of cyber crime challenges in the region, emphasizing the need for awareness and robust cyber security measures.

Questionnaire of Cyber Crime Awareness Among the Respondent

Impact of Awareness Programs Towards Society on the Cyber Crime on the basis of questionnaire of cyber crime awareness among the society.

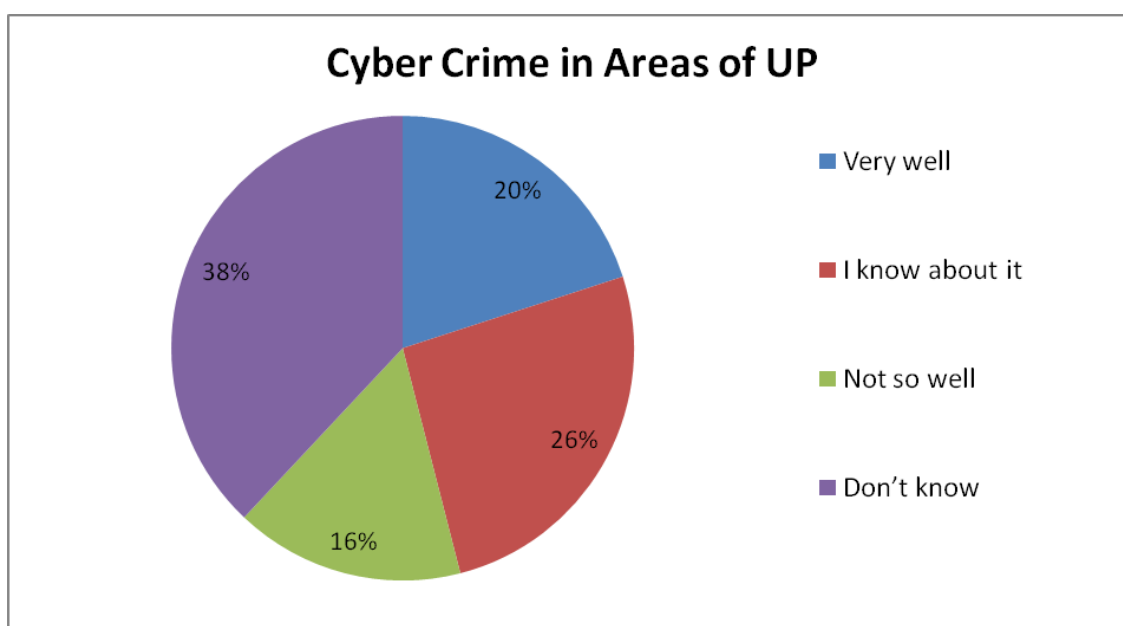
1. Your name, age, education level
2. Do you know that the first Wednesday of every month is celebrated as cyber Awareness day ?
3. Do you know the location of cyber help center in your area ?
4. Have you been a victim of any cyber crime yet ? If yes, then what type ?
5. Did you complain about it ?
6. Do you use social media ?
7. Do you know the rules of cyber security ?
8. What steps would you to protect yourself ?
 - (a) Keep your email password strong.
 - (b) Do not share your OTP, or other password, Important information with anyone else.
 - (c) Do not open your personal accounts on opener shared networks.
 - (d) Always use a good antivirus and verified apps on your phone and computers.
 - (e) Keep changing your passwords time to time.

9. Do you know the cyber helpline number ?
10. Do you know about terms like IT Act and Data personal bill or cyber laws ?
11. Do you check the credibility of any app or link before visiting it ?
12. Have you secured your social media accounts or banking apps from double authentication ?

Table No. 1- Demonstrate the awareness about cyber crime by the respondents.

Category	Number of Respondents as per dis.	Percentage
Very well	200	20%
I know about it	260	26%
Not so well	160	16%
Don't know	380	38%
Total	1000	100%

Awareness About Cyber Crime

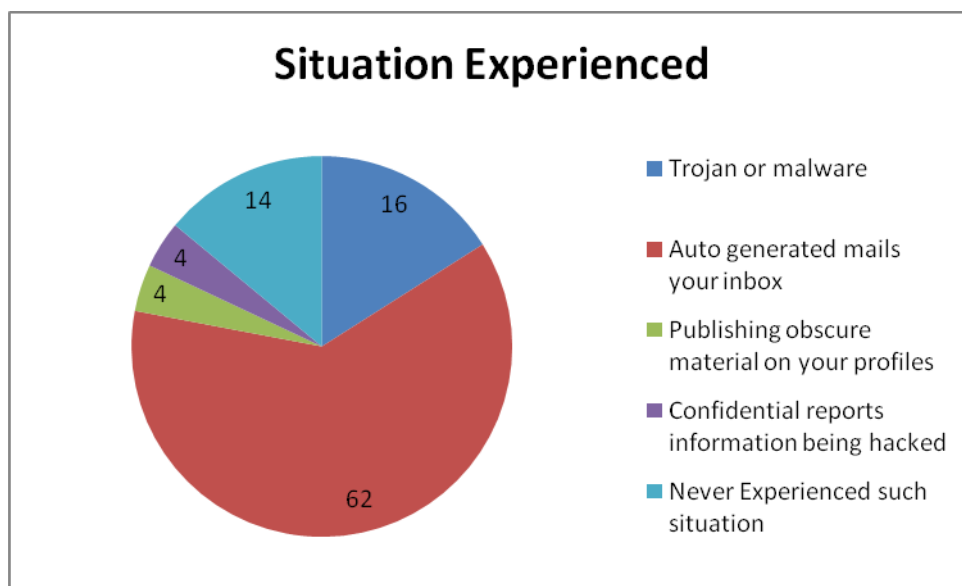


Analysis- This data reveals that 46% have a good understanding, while 54% lack awareness or have limited knowledge. Specifically, 20% are very well aware, 26% know about it, 16% are not so well informed, and 38% are unaware. This highlights the need for increased education on cyber crime.

Table No. 2- Demonstrate any of the below mentioned situation experienced by the respondents.

Category	Number of Respondents as per dis.	Percentage
Trojan or malware	160	16%
Auto generated mails your inbox	620	62%
Publishing obscure material on your profiles	40	04%
Confidential reports information being hacked	40	04%
Never Experienced such situation	140	14%
Total	1000	100%

Situation Experienced



Analysis- The table reveals that a significant majority of respondents (86%) have experienced some form of online security issue. The most prevalent issue is auto-generated mails in their inbox, affecting 620 respondents (62%), indicating a high exposure to spam emails. Trojan or malware attacks were experienced by 160 respondents (16%). On the other hand, fewer respondents reported issues like publishing of obscure material on their profiles (4%) and confidential reports being hacked (4%), suggesting these are less common concerns. Only 140 respondents (14%) reported never experiencing such situations, highlighting the widespread nature of online security challenges among the surveyed group.

Table No. 3- Mention how many time respondents have been a victim of cyber crime.

Category	Number of Respondents	Percentage
Never	740	74%
1 Time	220	22%
2 – 5 Time	40	04%
More than 5 times	00	00%
Total	1000	100%

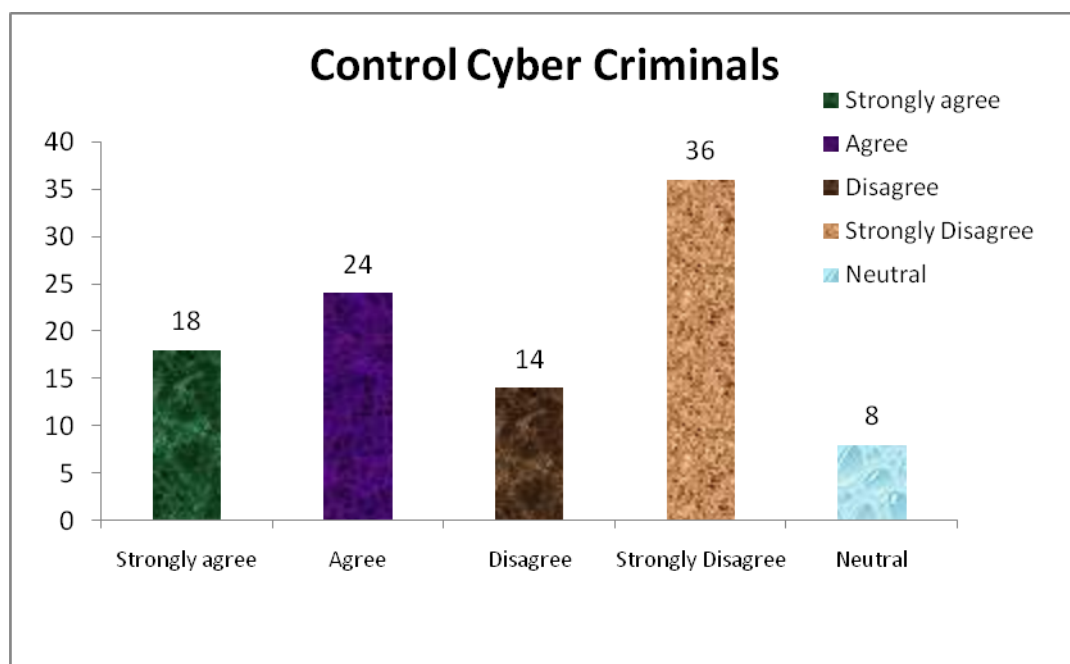
Victim of Cyber Crime



Analysis-The table presents the frequency of respondents being victims of cyber crime. A total of 1000 respondents participated in the survey. The data reveals that a significant majority, 74%, have never been victims of cyber crime, while 22% reported being victimized once. A smaller percentage, 4%, experienced cyber crime between 2 to 5 times. Notably, none of the respondents reported being victims more than 5 times.

Table No. 4- Demonstrate that the respondents thinks that the laws in effect are able to control cyber criminals.

Category	Number of Respondents	Percentage
Strongly agree	180	18%
Agree	240	24%
Disagree	140	14%
Strongly Disagree	360	36%
Neutral	80	08%
Total	1000	100%



Analysis -the table and bar chart provides insight into 1000 respondents' perceptions of the effectiveness of current laws in controlling cyber criminals. The survey results show that 18% of respondents strongly agree and 24% agree that the laws are effective, totalling 42% who believe in the efficacy of the laws. On the other hand, 14% disagree and 36% strongly disagree, indicating that a significant 50% of respondents are dissatisfied with the current legal framework's ability to control cyber crime. Additionally, 8% of respondents remain neutral. The data suggests a polarized view among respondents, with a slight majority leaning towards dissatisfaction with the current state of cyber crime laws. This indicates a need for potential reforms or enhancements to existing laws to better address cyber crime.

Habits of People on the using cyber space in that areas.

- 22.1% have shared their password for a TV or movies streaming service.
- 17.1% have shared their password for their social media accounts with friends and family close one.
- 20% shared their email account password to their staff and close one.
- 17% have shared their password for their online shopping accounts with family or friends.
- 37% use two factors authentication with finger print.
- 34% change their password regularly.
- 25% use a password save with Google.
- 36% keep track of password by writing them on a paper.
- 66% use same password for more than one online account.

Findings

1. It was examined that 38% of respondents were not aware about the cyber crime, from online hacking to phishing respondents were not aware about the fraud happening around the lack of awareness.

2. Experience auto generated mails to their inbox was about 62% of respondents.
3. Only 16% of respondents experienced Trojan and Malware practices.
4. Almost 22% of respondents have been a victim of cyber crime.

It was found that 36% of respondents strongly disagree about the law in effect are able to control cyber crime.

CHAPTER–VII

CONCLUSION AND SUGGESTION

7.1 CONCLUSION

By 2024 India is ranked number three in terms of the number. attacks, after United States and China, a new study has discovered even as it itself is becoming more vulnerable to attacks. The need to make changes is irresistible. However, the technological progress cannot be fully evaded. The legal and law enforcing agencies, the private companies, and organizations will also need to adapt to handle them the society. They should employ computer experts to address such cyber problems. It is also not sufficient that such specialists are also informed. They should also be equipped with requisite technical hardware and software through which they can effectively combat the cyber criminals.

This necessitates the deployment of the necessary facilities in different regions of the country in order to ensure that the virtual world crime is contained. The next point, that should be mentioned is that a culture of constant learning and education must be instilled in the legal and the law enforcement authorities since Information Technology sphere is a highly dynamic one. India has to modernize Police force. Since we are requiring modern police force that can comfortably keep up with the current technology of electronics that will be enforced on cyber crimes and misuse issues, it will be best to know in advance. Also ought to be on the forefront in the awareness programme in the general population.²⁰³

The cyber crime is new age crime that lacks specific punishment and laws in Constitution. The majority of the advocates are knowledgeable in Criminal Law, yet small in cyber crime out of this it can be concluded that the law cannot be left as it is, the law must evolve along with the changing times, and in this case this applies even to the cyber space i.e. to the Spy-cam case. The bottom–line of society and the technological development. 20 Cyber cell of the law

²⁰³ “Cyber security in Rural India: Challenges and Solutions”, NITI Aayog Report, 2023.

enforcement agencies have begun to operate in the metropolitan areas such as Pune, Mumbai, Hyderabad, Chennai, Bangalore etc.

Cyber crime vulnerabilities. Although data offers unlimited opportunities to its users (individuals, private companies, organizations, and governments) they may be misused by a certain group of people, who may use them to perpetrate a crime. In particular, data collection, storage, analysis, and sharing facilitates numerous cyber crimes and the extensive collection, storage, utilization, and distribution of data without informed consent and choice and required legal and security safeguards of the users. More so, data aggregation, analysis, and transfer happen on scales that the governments and organizations have not been ready to handle and thus posing a surging number of cyber security risks. Privacy, data protection and system network and data security are dependent on each other. Based on that, security measures are required that are aimed at safeguarding data and privacy of the user to guard against cyber crime.

7.2 SUGGESTION

The suggestions to secure the country's cyber space:

Suggestive role of government-

- Minimizing the damage caused and by reducing the recovery time from cyber attacks by creating cyber attack resistant technologies.
- Making efforts to prevent infrastructures by making them opaque to cyber attackers. cyber attacks against the country's critical
- Reduce national vulnerability to cyber attacks by both educating the public and the implementation of resistant soft wares.
- Early watch and warnings about upcoming cyber assault attempts by creating a national cyber security board which is solely dedicated towards protecting the national cyber space
- Forensics and attack attribution
- Protection of networks and systems critical to national security

- Protection against organized attacks capable of inflicting debilitating damage to the economy.
- Research and technology development that will enable the critical infrastructure organizations to secure their IT assets.
- Specialized procedures along with expertise are required to tackle cyber crimes.
- Stringent punishments should be changed to vigorous punishment and it should be implemented on criminals so that upcoming cyber criminals and cyber crime should reduce the rank of India. Presently, the offences which comes under Information technology Act are available with imprisonment of 3 years with should extent which would Change the mindset of cyber criminals.

Role of an educated person

- Safe the Ponzi Scheme related matters like Telegram, Whatsapp, Websites links does not share to any person.
- Safe the fraud social media sites like unknown person related to cyber crimes person for example : Facebook, Tutor, Youtube etc. Social Medias Officers related to CBI local Police Officers and Cyber Police.
- Safe the Financial Fraud like OTP don't share, links does not click, don't login in websites https://
- Committed the cyber crime immediately use helps line no. 1930.
- The online work carefully done. Like homework, job always search online portal.
- Alert the Government Scheme's Fraud, Personal detail does not share in Social Media Site
- Safe the Loan App Fraud, like unauthorized person did not use Mobile App like phone gallery and EKYC update.

- Safe to through E-mail fraud like Strong Password don't share Password. Please Carefully Logout our Email Address and time to time change the password.
- Always use anti-virus software for Computers, Laptop & Mobiles etc.
- Implement the National cyber security policy (2013) and review revise it regularly.
- Conduct regular cyber security audits and penetration testing.
- Establish more practical cyber security officials

Legislative Steps

- Strengthen the IT Act. And amend it to meet the need of emerging threats.
- Enact a Data protection law.
- Establish clear guidelines for social media platforms.
- Implement strict cyber crime laws and enforcement.

Suggestive role of NGOs

- Launch cyber awareness campaigns on ground level.
- Integrate cyber security education into school curricular.
- Conduct regular cyber security workshops and training programs on local base.
- Establish a National cyber security helpline reach on wide areas.
- Conduct regular cyber security drills and simulations.
- Develop a frame work for small and medium enterprises.
- Share threat intelligence and best practices with officials.
- Enhance broadband connectivity and digital literacy.
- Establish cyber security operations centers (CSOCS) in the rural and urban areas also.

Create a cyber security research and development for support innovation.

Suggestions on the behavior of investigators of cyber crime

- Use clear, concise language in reports and briefings.
- Ensure cultural sensitivity and awareness.
- Familiarize with jurisdictional issues.
- Stay updated on legal precedents.
- Communicate effectively with technical and non-technical audiences.
- Attend training and conferences.
- Respect confidentiality and privacy.
- Conduct regular review and evaluation of cases.
- Collaborate with peers to share knowledge.
- Stay with current update of tools and pursue certification of that areas

Suggestive role of an advocates

- Organize workshops, seminars, and campaigns to educate people about cyber crime, its types, and prevention methods.
- Work with law enforcement agencies to report and investigate cyber crimes, and provide them with necessary support and expertise.
- Advise individuals and organizations on best practices for cyber security, such as using strong passwords, updating software, and avoiding phishing scams.
- Provide support and guidance to victims of cyber crime, including helping them report incidents and navigate the justice system
- Push for stronger laws and policies to prevent cyber crime, and work with policymakers to develop effective legislation.
- Stay informed about the latest cyber crime trends, technologies, and threats to provide effective advocacy and support.
- Engage with local communities, schools, and organizations to raise awareness about cyber crime and promote prevention strategies.
- Advocate for cyber security education and training programs to equip people with the skills needed to stay safe online.

BIBLIOGRAPHY & REFERENCES

1. A Study on Cyber Crime and Security Scenario in INDIA, Yougal Joshi, Anand Singh, International Journal of Engineering and Management Research, Volume-3, Issue-3, June 2013 ISSN No.: 2250-0758, Pages: 13-18
2. Andrew S. Tanenbaum; “Modern Operating Systems”, 2nd edition, Addison Wesley, 2001.
3. Anita Goel; “Computer Fundamentals”, Pearson Publications, 2010
4. Anita Goel; “Computer Fundamentals”, Pearson Publications, 2010.
5. Arshdeep Bagha and Vijay Madiseti: “Cloud Computing A Hands-on Approach”, 2014.
6. Astt Narayan– LK Thakur, 'Internet Marketing E-commerce and cyberlaws' Authors press DELHI, 2000.
7. Barrie Sosinsky; “Cloud Computing Bible”, Wiley-India, 2010.
8. BBC 2017-05-31. Archived from the original on 2018-05-11. Retrieved 2018-04-14.
9. BBC (in Simplified Chinese). 9 July 2015. Archived from the original on 2018-05-08. Retrieved 2018-04-14.
10. Beckett, Nick (Nov 2017). "A Guide for Businesses to China's First Cyber Security Law". China Monitor, Merics: Mercator Institute for China Studies. Archived from the original on 2018-12-16. Retrieved 2018-12-14.
11. Behrouz, A. Forouzan; “Data Communication and Networking”, 4th Edition, TMH, 2000.
12. Blanchard, Ben (2015-12-28). "China passes controversial counter-terrorism law". Reuters. Retrieved 2021-07-21.
13. Bo, Q. U.; Changxu, H. U. O. (15 September 2020). "Privacy, National Security, and Internet Economy: An Explanation of China's Personal

- Information Protection Legislation". *Frontiers of Law in China*. **15** (3): 339–366. doi:10.3868/s050-009-020-0019-4. ProQuest 2450653759.
14. China Internet Information Center. Archived from the original on 2018-12-14. Retrieved 2018-04-14.
 15. China lays down new vulnerability disclosure rules. Arjun Ramprasad. Previewtech.net. June 18, 2021.
 16. China's cyber regulations: a headache for foreign companies | Merics. merics.org. 22 March 2017. Retrieved 2021-07-22.
 17. Chitrakoot: Mythology Revisited. OutlookIndia.com. Outlook Traveller. 15 May 2017. Retrieved 30 December 2021.
 18. Computer Associate Int, I. Inc. v. Atai, Inc; 982F, 26, 693, 696 2nd cir. 1992. One judge admitted that as scientific knowledge advances we endeavour to keep pace and “anetimes, as in the area of technology, we venture into less than familiar waters.
 19. Cyber Law And Informed Technology, RM.Kamble, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May 2013 789 ISSN 2229-551.
 20. Dangerous Partners: Big Tech and Beijing. Federal Bureau of Investigation. Archived from the original on 2020-04-02. Retrieved 2020-04-09.
 21. Dr. C.P. Singh, “U.P. Civil Judge”, Main Examination Guide, Central Law Publications, 4th Ed. 2016, Cyber crime, pp. 18-21.
 22. Dr. Navin Kumar Bohra, “Cyber Kanoon avam Apradh”, Samajik Lekh, Published in Pratiyogita Darpan, June, 2005 Pp. 2026-2028.
 23. Dr. Subhash Chandra Gupta - Information Technology Act, 2000 and its drawbacks, ‘National Conference on Cyber Laws & Legal Education’,
 24. Gartenberg, Chaim (2017-07-13). "Apple is building its first China-based data center per new cybersecurity law". The Verge. Retrieved 2021-07-22.

25. Gary Nutt; "Operating Systems: A Modern Perspective", 2nd edition, Pearson Education, 2001.
26. Gierow Johannes, Hauke (2015-04-22). "Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses" (PDF). China Monitor, Merics: Mercator Institute for China Studies. Archived (PDF) from the original on 2018-12-16. Retrieved 2018-12-14.
27. Gough, J. R. (2022, May 24). Cyber attack costs city of Quincy \$650,000. Muddy River News <https://muddyrivernews.com/noteworthy/cyberattack-costs-city-of-quincy-650000/20220524123433/>
28. Greig, J. (2022, May 19). K-12 school districts in New Mexico, Ohio crippled by cyber attacks. The Record by Recorded Future. <https://therecord.media/k-12-cyberattacks-new-mexico-ohio/>
29. [http://searchoa.techtarget.com/definition/cyber space](http://searchoa.techtarget.com/definition/cyber%20space).
30. <http://www.cyberlawsindia.net/>
31. <http://www.helpline1aw.com/family-law/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html>
32. [http://www.lawyersclubindia.com/articles/Classification-Of Cyber crimes-1484.asp](http://www.lawyersclubindia.com/articles/Classification-Of-Cyber-crimes-1484.asp)
33. <http://www.mondaq.com/india/x/623820/Security/Cyber+Laws+In+India>
34. [https://www.britannica.com/topic/cyber crime/Identity-theft-and invasion-of-privacy](https://www.britannica.com/topic/cyber-crime/Identity-theft-and-invasion-of-privacy) Social Science Research Network; Author:Tabrez Ahmed; Dated on: May 12:2018
35. https://www.researchgate.net/publication/241689595_A_Study_on_Cyber_Crime_in_India
36. <https://www.vakilno1.com/legalviews/cyber-crimes-in-india.html/amp>

37. Huifeng (2018-03-01). "Cybersecurity law causing 'mass concerns' among foreign firms in China". South China Post. Archived from the original on 2018-11-07. Retrieved 2018-12-14.
38. Information Technology Act ,2000
39. International Journal of Scientific & Engineering Research, Volume 6, Issue 4, April-2015 1974 ISSN 2229-551
40. John P. Hayes; "Computer Architecture and Organization", McGraw Hill, 1988.
41. John P. Hayes; "Computer Architecture and Organization", McGraw Hill, 1988.
42. K. Kent, 5. Chevalier, T. Grance and H. Dang; "Guide to Integrating Forensic Techniques into Incident Response", Special Publication 800- 86, NIST, Gaithersburg, Maryland, 2006.
43. Kent, D. Stuckey, Internet and on line law (4th ed. 1999).
44. Kishore, B. R. (2007). Ramayana. Diamond Pocket Books (P) Ltd. p. 42. ISBN 978-81-7182-070-2.
45. Lauver, M. (2022, June 23). US passes bills to foreground national cybersecurity. Security <https://www.securitymagazine.com/articles/97873-us-passes-bills-to-foreground-national-cybersecurity>
46. Law News and Network; by Admin Lawnn ; September 26,2016
47. Learn more about iCloud in China. Apple Support. Archived from the original on 2018-03-07. Retrieved 2018-04-14.
48. Lee, Jyh-An (2017). "Hacking into China's Cybersecurity Law" (PDF). Wake Forest Law Review. **53** (1). SSRN 3174626.
49. Lin, Liza; Kubota, Yoko (6 December 2017). "U.S. Tech Firms Spooked by China's Arcane Cybersecurity Law". Wall Street Journal.

50. Lulu, Xia, and Zhao Leo (2018-08-21). "China's Cybersecurity Law: An Introduction for Foreign Businesspeople". China Briefing. Archived from the original on 2018-12-13. Retrieved 2018-12-14.
51. Lyngaas, S. (2022, May 26). Ransomware attack hits New Jersey county. CNN. <https://edition.cnn.com/2022/05/26/politics/new-jersey-somerset-county-ransomware-attack/index.html>
52. Marganet, J. Radin, John A. Rothchild & Gregory M. Silverman, Internet Commerce the Emerging legal Framework (University Cashbook series, Foundation Press, 2002) 1042.
53. Mela L. Rep. 1794 (NY Sup Q 1995).
54. National Academy of Public Administration. (2022). A call to action: The federal government's role in building a cybersecurity workforce for the nation. <https://s3.us-west-2.amazonaws.com/napa-2021/studies/dhs-cybersecurity-workforce/NAPA-CISA-Cybersecurity-Workforce-Development-Report-Summary-Slides-January-2022.pdf>
55. NetEase. Archived from the original on 2019-07-03. Retrieved 2018-04-14.
56. New Azure region coming to China in 2022 | Azure blog and updates | Microsoft Azure. azure.microsoft.com. 4 March 2021. Retrieved 2021-07-22.
57. New York Berkley Publishing Group, 1989, p. 128.
58. Office of Joe Neguse. (2022, May 17). Neguse, Peters state and local government cybersecurity bill heads to president's desk for signature [Press release]. <https://neguse.house.gov/media/press-releases/neguse-peters-state-and-local-government-cybersecurity-bill-heads-to-presidents-desk-for-signature>
59. People's Daily. Archived from the original on 2018-04-15. Retrieved 2018-04-14.

60. Rajkumar Buyya, James Broberg. Andrzej M. Goscinski; “Cloud Computing: Principles and Paradigms”, Wiley Publications, 2013.
61. Antitrust and Trade Reg. (Rep. BNA) Jan. 14, 1982; P. 88.
62. Generally; c. Evens, *The Micro Millennium* 67 (1979). See also *Tennessee v. Edmunsen*, 1 Computer cas, (CCH) 46, 167 at 61, 541, 61, 542 (Tem. Crin. App. 1988). It was observed that ‘Only a hermit would be unaware of the degree to which computers have permeated every aspect of our lives from the cradle to the grave our activities are influenced, tracked recorded and controlled by computers “Soot’s on Computer Law Vol. (i) at p. 41.
63. Collins English Dictionary – Complete and Unabridged @ Harper Collins Publishers 1991, 1994, 1998, 2000, 2003.
64. Dictionary of Military and Associated Terms, US Department of Defence 2005.
65. Dictionary.com Unabridged; based on the Random House Dictionary, @ Random House, Inc. 2012, at <http://dictionary.reference.com/browse>.
66. Dictionary.com’s 21st Century Lexicon Copyright @ 2003-2012 Dictionary.com LLC; at <http://dictionary.reference.com/browse>, where the term ‘cyberia has been defined as ‘the computer and Internet world and its virtual reality, the ‘global village’ of electronic communication; also called cyber world, cyber space.
67. <http://www.thefreedictionary.com>; based on Word Net 3.0, Farlex clipart collection @ 2003-2011 Princeton University, Farlex Inc.
68. The American Heritage Dictionary of the English Language, Fourth Edition copyright @2000 by Houghton Mifflin Company, Updated in 2009 and published by Houghton Mifflin Company.
69. Social Science Research Network Cyber crime threat to Indian society, Author: R.N.Mangoli , August 16,2016.

70. Terrence V. Lillard; “Digital Forensics for Network, Internet and Cloud Computing: A Forensic Evidence Guide for moving Targets and Data” Syngress Publications, 2010.
71. Thomas Earl; “Cloud Computing”, Pearson, 2014.
72. Threat Connect. (2022). Report: Cybersecurity under stress <https://threatconnect.com/wp-content/uploads/ThreatConnect-Cyber-Survey-Report-1.pdf>
73. Uchill, Joe (October 17, 2019). "China's upgraded cybersecurity law could take a toll". Axios. Archived from the original on March 29, 2020. Retrieved April 8, 2020.
74. Understanding China's Cybersecurity Law INFORMATION FOR NEW ZEALAND BUSINESSES (PDF). Ministry of Foreign Affairs and Trade, and New Zealand Trade and Enterprise. Sep 2017. Archived (PDF) from the original on 2019-01-23. Retrieved 2018-12-14.
75. V. Rajaraman and Niharika Adabala; “Fundamentals of Computers”, 6th Editioin, PHI Learning Pvt. Ltd., 2015.
76. V. Rajaraman and Niharika Adabala; “Fundamentals of Computers”, 6th Editioin, PHI Learning Pvt. Ltd., 2015.
77. Valmiki; Venkataswami, M. N. The Ramayana (Complete). Library of Alexandria. p. 421. ISBN 978-1-4655-7792-4.
78. Very Large Scale Integration
79. Wagner, Jack (2017-06-01). "China's Cybersecurity Law: What You Need to Know". The Diplomat. Archived from the original on 2018-12-12. Retrieved 2018-12-14.
80. William Stallings; “Operating Systems: Internals and Design Principles”, 5th Edition, Prentice Hall, 2005.

81. Wong, Edward (2016-04-28). "Clampdown in China Restricts 7,000 Foreign Organizations". The New York Times. ISSN 0362-4331. Retrieved 2021-07-21.
82. Zhang, Angela Huyue (2024). High Wire: How China Regulates Big Tech and Governs Its Economy. Oxford University Press. ISBN 9780197682258.

Websites

83. www.4n6hub.com
84. www.computerhope.com
85. <http://www.webopedia.com>
86. www.cybercases.blogspot.com
87. www.gahtan.com/cyberlaw - cyber law encyclopedia.
88. www.importantindia.com
89. www.indlii.org/Cyberlaw.aspx
90. http://www.osixs.org/V2_Menu_V2.aspx.
91. www.legalserviceindia.com/cyber-crimes.
92. www.xinhuanet.com. Archived from the original on 2018-04-15. Retrieved 2018-04-14.

Books

93. Dr. Bhagyashree A. Deshpande, 'Text Book on Cyber Law'; Central Law Publications, Darbhanga Castle, Allahabad, 2019.
94. Dr. Chintan Pathak & Dr. Kalpeshkumar L Gupta, "Landmarks Judgments on Cyber Crimes & Cyber Laws", Published by Law & Justice Publishing Co. Delhi, Ed. 2023
95. Dr. Ishita Chatterjee, "Law on Information Technology"; Central Law Publications, Darbhanga Castle, Prayagraj, 2022.

96. Dr. J.P. Mishra, “An Introduction to Cyber Law”, Central Law Publications, Darbhanga Castle, Allahabad, 2014.
97. Dr. Satish Chandra, “Cyber Law in India”, Published by ABS Books New Delhi, Ed. 2017
98. Retrieved from Pradeep K. Sinha, Priti Sinha, 6th Ed. Rep. 2018, BPB Publications, New Delhi at pp. 389-390.
99. Rohit Arvind Jain, “Cyber Crime & Laws”, Evincepub Publishing, Bilaspur, Chhattisgarh, 2018.
100. Ronald L. Krutz, Russell Dean Vines; “Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Wiley-India, 2010.
101. S.K Verma and Raman Mittal, ‘Legal Dimensions of Cyber space, 2004, Indian Law Institute, New Delhi.

News Papers

1. Amar Ujala Dated 02 April, 2024 Page no. 08
2. Amar Ujala, Jhansi Dated 24 November, 2019 Page no. 01
3. Dainik Bhaskar, Jhunjhunu Rajasthan Dated 22 November, 2023
Page no. 04
4. Dainik Jagran, Jhansi Dated 20 February, 2024 Page no.-03.
5. Times of India Dated 14 February, 2024 Page no. 01



INSTITUTE OF ECONOMICS AND FINANCE

(A Centre Of Excellence)



BUNDELKHAND UNIVERSITY JHANSI

5TH INTERNATIONAL CONFERENCE

**"Role Of Social Sciences And Humanities
For Sustainable Future"
(ICRSSHSF2023)**



Certificate
of Participation

2 - 4 November 2023

This is to certify that Prof./Dr./Mr./Ms. Shefali Bajpai (Research Scholar) of P.K. University, Shivpur, M.P. has participated in the 5th International Conference on "Role of Social Sciences and Humanities for Sustainable Future" (ICRSSHSF 2023) organized by Institute of Economics and Finance, Bundelkhand University Jhansi, from 2-4 November 2023 and Presented paper entitled Cyber threat in digital currency and online financial system in developing countries.

Dr. Shambhu Nath Singh
ORGANIZING SECRETARY

**Prof. Beatriz Lucia Salvador
Bizotto, Brazil**
INTERNATIONAL
CONFERENCE CHAIRMAN

Prof. C. B. Singh
CONVENOR





**UTTAR PRADESH STATE COUNCIL OF HIGHER EDUCATION
SPONSORED NATIONAL SEMINAR**



ON

ARTIFICIAL INTELLIGENCE, TECHNOLOGY AND CYBER LAW: CHALLENGES AND FUTURE PROSPECTS

ORGANIZED BY

**V.S.S.D. COLLEGE, KANPUR
(Accredited 'A' Grade By NAAC)**

CERTIFICATE

This is to certify that Prof./Dr./ Mr./Ms. Shreyali Barypai
from P.K., University, Shivpurii (M.A) has Participated/Presented the Paper
Titled Artificial Intelligence : The grey area of cyber crime and cyber law in the National
Seminar Themed on Artificial Intelligence, Technology and Cyber law: Challenges and future Prospects organized by Department of law, VSSD
College Kanpur on March 21, 2024.

Prof.(Dr.) Bipin Chandra Kaushik
Principal

Mr. Ram Bakas
ORGANISING SECRETARY

Prof.(Dr.) A.B. Jaiswal
Convenor

Mrs. Amrita Verma
Convenor



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | ISSN: 2320 - 2882

An International Open Access, Peer-reviewed, Refereed Journal

The Board of
International Journal of Creative Research Thoughts
Is hereby awarding this certificate to

Dr.Hardayveer

In recognition of the publication of the paper entitled
"Cyber Crime" As A New Form Of Business"

Published In IJCRT (www.ijert.org) & 7.97 Impact Factor by Google Scholar

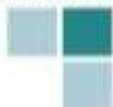
Volume 13 Issue 9 September 2025 , Date of Publication: 11-September-2025

UGC Approved Journal No: 49023 (18)

PAPER ID : IJCRT2509193

Registration ID : 293616

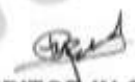
Scholarly open access journals, Peer-reviewed, and Refereed Journals, Impact factor 7.97 (Calculate by google scholar and Semantic Scholar | AI-Powered Research Tool) , Multidisciplinary, Monthly Journal



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | IJCRT
An International Scholarly, Open Access, Multi-disciplinary, Indexed Journal

Website: www.ijert.org | Email id: editor@ijert.org | ESTD: 2013




EDITOR IN CHIEF



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | ISSN: 2320 - 2882

An International Open Access, Peer-reviewed, Refereed Journal

The Board of
International Journal of Creative Research Thoughts
Is hereby awarding this certificate to

Shefali Bajpai

In recognition of the publication of the paper entitled
"Cyber Crime" As A New Form Of Business"

Published In IJCRT (www.ijert.org) & 7.97 Impact Factor by Google Scholar

Volume 13 Issue 9 September 2025 , Date of Publication: 11-September-2025

UGC Approved Journal No: 49023 (18)

PAPER ID : IJCRT2509193

Registration ID : 293616

Scholarly open access journals, Peer-reviewed, and Refereed Journals, Impact factor 7.97 (Calculate by google scholar and Semantic Scholar | AI-Powered Research Tool) , Multidisciplinary, Monthly Journal



EDITOR IN CHIEF

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS | IJCRT
An International Scholarly, Open Access, Multi-disciplinary, Indexed Journal
Website: www.ijcrt.org | Email id: editor@ijcrt.org | ESTD: 2013



International Journal For Multidisciplinary Research

An **International** Open Access **Peer Reviewed** Journal • Impact Factor: **9.24** • E-ISSN: **2582-2160**

Certificate of Publication

The editorial board of IJFMR is hereby awarding the certificate of publication to

Shefali Bajpai

in recognition of publication of the paper titled

Cyber Extortion in India: A Critical Analysis of Legislation and Challenges

Co-author(s): Dr. Hardayveer

Published In: **Volume 7, Issue 6 (November-December 2025)**

Paper Id: **59971**

www.ijfmr.com • editor@ijfmr.com

Editor / Publisher
IJFMR



International Journal For Multidisciplinary Research

An **International** Open Access **Peer Reviewed** Journal • Impact Factor: **9.24** • E-ISSN: **2582-2160**

Certificate of Publication

The editorial board of IJFMR is hereby awarding the certificate of publication to

Dr. Hardayveer

in recognition of publication of the paper titled

Cyber Extortion in India: A Critical Analysis of Legislation and Challenges

Co-author(s): Shefali Bajpai

Published In: **Volume 7, Issue 6 (November-December 2025)**

Paper Id: **59971**

www.ijfmr.com • editor@ijfmr.com

Editor / Publisher
IJFMR



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Crime “As A New Form of Business”

Shefali bajpai ¹Dr. Hardayveer²

Research scholar ,Head of department of law

P.K. University,Shivpuri (M.P.)

Abstract-

The internet is frequently hailed as a remarkable tool, an engaging platform, and a liberating experience. However, the question remains: for whom? As the online world expands, many of us are at risk of falling prey to sophisticated cybercriminals who expertly navigate the digital landscape. Cyberspace, often referred to as the web, is a dynamic and intangible environment.

This paper examines the emerging threat of cybercrime, a new breed of business and high-tech criminality. It provides an overview of cybercrimes, the perpetrators, and their motivations. A detailed discussion of various cybercrimes will be presented, along with the unique challenges and response issues that arise during prevention, detection, and investigation.

Additionally, this paper will outline the relevant sections of the IT Act 2000 of India and propose new provisions to enhance the legislation. The discussion will cover the complexities of cybercrime and the need for effective measures to combat this growing threat.

Key words –cyber crime ,laws ,threat ,internet, offence, remarkable tool

Introduction

The internet is a revolutionary force that transforms every aspect of our lives. It challenges traditional norms and conventions, reshaping governance, business operations, education, and even everyday activities like cooking. The internet disrupts our existing knowledge and perceptions of the world, others, and ourselves. This digital landscape is simultaneously empowering, thrilling, daunting, and intimidating. Despite its vast potential, the internet remains an enigma to many, evoking feelings of mystery, apprehension, and incomprehension. The rapid growth of the internet has led to an increase in cybercrime opportunities. As more people go online, crimes like hacking, extortion, and fraud have become more common. Lawmakers struggle to keep up with the fast-paced technological advancements, making it challenging to create effective laws. They must balance individual rights, such as privacy and free speech, with the need to protect networks and communities.

Cybercrime enforcement is further complicated by jurisdictional issues, requiring international cooperation to combat these crimes effectively. Law enforcement agencies worldwide are working together to develop new strategies and responses to ensure online safety and security.

This paper argues that cybercrime, particularly high-tech crime, requires a fundamental shift in policing approaches. The paper is structured as follows:

- Sections 2 and 3 provide an overview of cybercrimes and their perpetrators.
- Section 4 discusses different types of cybercrimes.
- Section 5 explores the challenges and response issues in preventing, detecting, and investigating cybercrimes.
- Sections 6 and 7 outline the IT Act 2000 of India's efforts to prevent and reduce cybercrime incidents.
- Section 8 proposes changes to the IT Act 2000.
- The paper concludes with a brief statement on the challenges posed by cybercrime.

2. background

Cybercrime refers to criminal activities that involve computers, networks, or the internet. There are different perspectives on what constitutes cybercrime. Some experts consider it to be traditional crimes committed using advanced technology, where the computer is either a tool, a target, or both. Others believe that cybercrime is a distinct category of crime that requires a new legal framework to address the unique challenges posed by emerging technologies, such as:

- Jurisdictional issues
- Need for international cooperation
- Difficulty in determining intent
- Challenges in identifying perpetrators

These differing views highlight the complexities of cybercrime and the need for a comprehensive approach to address its unique nature.

2.1 The Perpetrators – Hackers & Crackers

2.1.1 Hackers

A hacker is typically defined as an individual who attempts to gain unauthorized access to a computer system. According to Section 66 of the IT Act 2000, a person can be considered a hacker if they:

- Intend to cause or know that they are likely to cause wrongful loss or damage to the public or any person
- Destroy, delete, or alter information residing in a computer resource
- Diminish the value or utility of the information or affect it injuriously by any means

In essence, hacking involves unauthorized actions that compromise the integrity or security of computer systems or data.

2.1.2 Crackers

A cracker is a type of hacker who has malicious intentions. The term "cracker" is used to differentiate between hackers who engage in benign activities and those who cause harm to computer systems. Crackers are known for:

- Maliciously sabotaging computers
- Stealing sensitive information from secure systems
- Disrupting networks for personal or political gain

In essence, crackers use their technical expertise for nefarious purposes, compromising the security and integrity of computer systems and data.

3. Why People Hack?

Cybercrime is emerging as a "new form of business" that involves:- Novel forms of criminal activity, A wider scope and scale of offenses and victimization, The need for rapid response, Complex technical and legal challenges.

Hacking, a key aspect of cybercrime, can be driven by various motives, including:- Personal gain, Political agendas, Professional interests

These factors highlight the evolving nature of cybercrime and the need for effective strategies to combat its growing threats.

3.1 Hactivism

In recent years, hacktivists have been launching business-motivated attacks on public web pages and email servers. These hacking groups and individuals:

- Overload email servers with massive amounts of emails to a single address (a technique known as email bombing or spamming)
- Hack into websites to display professional or business messages, often to promote a particular agenda or ideology

These types of attacks are typically used to disrupt or deface online platforms, and can have significant impacts on businesses and organizations.

3.2 Employees

Research has shown that disgruntled employees pose a significant threat to computer security. These individuals may:

- Steal confidential information and trade secrets for financial gain
- Use their insider knowledge to access and damage the system or steal sensitive data

According to the Cyber Crime Cell (CBI), insider threats are a major source of computer crimes. Insiders often have an advantage due to their familiarity with the system, which allows them to cause harm without requiring extensive technical knowledge.

3.3 Recreational Hacker

Recreational hackers break into computer networks primarily for the thrill of the challenge or to gain recognition within the hacking community. These individuals often:

- Download pre-existing attack scripts and protocols from the internet
- Launch these attacks against target sites without having in-depth knowledge of the systems they're targeting

Their actions are typically driven by personal satisfaction or to boost their reputation among peers, rather than for financial gain or malicious intent.

3.4 Web site Administrators and Web Pages

Websites also access a lot of hidden background information from the user. The remote website can determine the following important information about the visitor;

- a. the IP address the user is accessing the web site from;
- b. the number of prior visits to the web site, and the dates;
- c. the URL of the page that contained the link to get the user to the web site;
- d. the user's browser type and operating system and version;
- e. the user's screen resolution;
- f. whether JavaScript and VBScript are enabled on the user's computer;
- g. how many web pages the user has visited in the current session;
- h. the local time and date; and
- i. FTP username and password, if there is one.

4. Types of Cyber Crime

Computers play a crucial role in almost all cybercrimes, serving as either the target, tool, or source of evidence. As more devices become internet-enabled, the opportunities for hackers to exploit them increase. The different uses of computers in cybercrime can be categorized into three main areas:

1. Computer as the target: The goal is to steal information from or cause damage to a computer, system, or network. Examples include:
 - Hacking
 - Cracking
 - Espionage
 - Cyberwarfare
 - Malicious computer viruses
2. Computer as the tool: Cybercriminals use computers to commit traditional crimes, such as:
 - Printing fake currency
 - Creating and distributing child pornography
 - Money laundering
3. Computer as evidence: Computers can contain crucial evidence of a crime, such as:
 - Child pornography
 - Financial records of money laundering operations

The role of computers in cybercrime highlights the need for effective laws and strategies to combat these evolving threats.

4.1 Malicious Code – Viruses, Worms and Trojans

Viruses - A computer virus is a program that modifies other computer programs, replicating itself and potentially causing harm. Viruses can spread through- Email attachments ,Infected disks, Execution of infected programs .A common method of virus execution is when a user is tricked into opening a malicious file, often disguised as a harmless program from a trusted source. A notable example is the Melissa virus, which: Spread through a Microsoft Word attachment, Activated a macro that emailed itself to 50 addresses in the victim's Microsoft Outlook, Caused an estimated \$80 million in damages

Worms - A worm is a standalone program that replicates itself, spreading throughout a network without needing to attach to a file. Unlike viruses, worms can propagate independently. An example is the "I Love You" worm, which caused significant losses in 2001.

Trojan Horses - A Trojan horse is a seemingly innocent program that contains hidden malicious functions. These programs are often used to introduce viruses into computer systems. Once executed, the hidden sub-program performs unauthorized actions. An example is Back Orifice 2000, a program designed for misuse and attacks on other computers.

These types of malware highlight the importance of robust cybersecurity measures to prevent and mitigate the damage caused by such threats.

4.2 A Denial of Service

A Denial of Service (DoS) attack is a type of cyberattack where an attacker floods a computer or network with excessive traffic, preventing legitimate users from accessing it. The goal is not to breach the system or steal data, but rather to disrupt access to the network or website. DoS attacks can be motivated by:- Revenge, Economic or political gain, Malicious intent

For example, in February 2000, a 15-year-old Canadian boy known as "MafiaBoy" allegedly launched a DoS attack that shut down popular websites such as:-Yahoo, Amazon, Buy and other. This attack demonstrates the potential impact of DoS attacks on online services and the importance of robust cybersecurity measures to prevent and mitigate such threats.

Cyberstalking

Cyberstalking is a form of online harassment where an individual is pursued and monitored, often with their privacy invaded and every move watched. This can cause significant distress and fear for the victim. Cyberstalking can affect anyone, but it is more common among women and children. The anonymity of the internet can embolden stalkers, who may be strangers or individuals known to the victim.

Financial Crimes

Financial crimes in the cyber world include cheating, credit card fraud, and money laundering. An example of such a crime is a website offering goods at unusually low prices, only to exploit the trust of customers who provide their credit card numbers. The perpetrators would then misuse the credit card information for financial gain.

Cyber Pornography

Cyber pornography involves the distribution and sharing of pornographic content through the internet, including websites and online publications. There have been several incidents in India related to cyber pornography, such as:

- A student creating a website with morphed images of his classmates and teachers
- A couple forcing slum children to appear in obscene photographs, which were then uploaded to websites catering to pedophiles

These incidents highlight the need for awareness and action to prevent and address cybercrimes.

- **Sale of Illegal Articles:** This involves selling prohibited items like narcotics, weapons, or wildlife through online platforms, auction sites, or email communications. For instance, some auction sites in India might be selling cocaine disguised as 'honey'.

- **Online Gambling:** Millions of websites offer online gambling, often hosted on foreign servers. Some of these sites might be fronts for money laundering.

- **Intellectual Property Crimes:** These include software piracy, copyright infringement, trademark violations, and theft of computer source code.

- **Email Spoofing:** This occurs when someone sends emails that appear to originate from a different source. For example, if someone spoofs Pooja's email (pooja@asianlaws.org) and sends obscene messages to her acquaintances, it could damage her relationships and reputation.

- **Forgery:** Counterfeit currency notes, postage stamps, mark sheets, and certificates can be forged using advanced computers and printers. In India, some student gangs sell fake mark sheets and certificates to students.
- **Cyber Defamation:** This happens when defamation occurs through computers or the internet. Examples include publishing defamatory content about someone on a website or sending defamatory emails to their friends.

5. unique challenges

Investigating cybercrime comes with a unique set of challenges. Some of the key difficulties include:

1. Jurisdictional issues: Cybercrimes often cross multiple jurisdictions, making it hard to determine which laws apply and which authorities should handle the investigation.
2. Evidence preservation: Digital evidence can be easily altered, deleted, or encrypted, making it crucial to preserve it properly.
3. Decoding encryption: Encrypted data can be difficult to access, and investigators may need specialized tools and expertise to crack the encryption.
4. Proving identity: It can be challenging to determine the identity of cybercriminals, as they often use pseudonyms, VPNs, and other methods to hide their tracks.
5. Finding evidence: Investigators need to know where to look for digital evidence, which can be scattered across various devices, networks, and online platforms.
6. Staying up-to-date with technology: Cybercriminals are constantly evolving their tools and techniques, so investigators need to stay current with the latest technology and trends.
7. Real-time response: Cybercrimes often require a rapid response to prevent further damage and preserve evidence.
8. Coordination and collaboration: Effective investigations often involve multiple agencies and stakeholders, requiring strong coordination and collaboration.
9. Training and expertise: Investigators need specialized training and expertise to handle complex cybercrime cases.
10. Strategic partnerships: Building partnerships with other agencies, organizations, and industry experts can help investigators stay ahead of cybercriminals.
11. Reporting and information sharing: Encouraging reporting and sharing information about cybercrimes can help identify patterns and trends.
12. Attracting and retaining talent: Investigative agencies need to attract and retain skilled professionals with expertise in cybersecurity and digital forensics.
13. Avoiding tech-lag: Agencies need to stay up-to-date with the latest technology and tools to effectively investigate cybercrimes.

By understanding these challenges, investigators and agencies can develop strategies to overcome them and effectively combat cybercrime.

6. Cyber Laws in India: In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses

and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means. The Information Technology Act, 2000 is a crucial piece of legislation that provides the legal framework for e-commerce in India. The Act aims to:

- Provide legal recognition to electronic records and digital signatures
- Facilitate e-governance and e-commerce
- Regulate certifying authorities and digital signature certificates
- Prescribe penalties for cyber offenses

Key Provisions of the IT Act

Some of the key provisions of the IT Act include:- **Digital Signatures:** The Act allows subscribers to authenticate electronic records using digital signatures, which can be verified using public keys.

- **Electronic Governance:** The Act provides for the use of electronic records and digital signatures in government transactions, and recognizes the legal validity of digital signatures.
- **Regulation of Certifying Authorities:** The Act establishes a Controller of Certifying Authorities to oversee the activities of certifying authorities and specify standards and conditions for issuing digital signature certificates.
- **Secure Electronic Records and Digital Signatures:** The Act provides for the use of secure electronic records and digital signatures to ensure the authenticity and integrity of electronic transactions.
- **Penalties and Adjudication:** The Act prescribes penalties for various cyber offenses, including damage to computer systems and hacking, and establishes an adjudicating officer to investigate and impose penalties.
- **Cyber Appellate Tribunal:** The Act establishes a Cyber Appellate Tribunal to hear appeals against orders passed by adjudicating officers.

Impact of the IT Act

The IT Act has a significant impact on e-businesses and the new economy in India, as it provides a legal framework for electronic transactions and digital signatures. The Act aims to promote e-commerce and e-governance, while also protecting against cyber threats and offenses.

7. Advantages of Cyber Laws

The Information Technology Act, 2000 provides a legal framework for electronic transactions and digital signatures, offering several benefits, including:

- Legal validity of electronic records: The Act recognizes electronic records as a valid and enforceable form of communication, which can be used in court proceedings.
- Digital signatures: The Act gives legal validity to digital signatures, enabling secure and authenticated electronic transactions.
- E-commerce growth: The Act provides a legal infrastructure for e-commerce, allowing companies to carry out electronic transactions with confidence.
- E-governance: The Act enables government departments to accept and process electronic documents, promoting e-governance and efficient public services.

- Certifying Authorities: The Act allows corporate companies to become Certifying Authorities, issuing Digital Signature Certificates and promoting the use of digital signatures.
- Security: The Act addresses security concerns by defining secure digital signatures and providing a framework for protecting electronic transactions.
- Remedies for cyber crimes: The Act provides statutory remedies for companies that suffer damages or data theft due to unauthorized access to their computer systems or networks.

By providing a clear and comprehensive framework for cyber laws, the IT Act, 2000 promotes trust and confidence in electronic transactions, supporting the growth of e-commerce and e-governance in India.

8. Proposed Changes to the IT Act, 2000

To address emerging challenges in cybercrime investigations, the following changes are proposed:

1. Trap and Trace Orders: The new legislation should enable cyber investigators to obtain a single "trap and trace" order to track the origin of online communications, including IP packets, across multiple jurisdictions. This would facilitate the investigation of cybercrimes such as hacking, DoS attacks, and virus outbreaks.
2. Age of Criminal Responsibility: The proposed legislation should consider lowering the age of criminal responsibility for serious computer crimes to 15 years, acknowledging the increasing involvement of young individuals in cybercrime.
3. Regulation of Cyber Cafes and Computer Training Centers: The proposed legislation should incorporate cyber cafes, computer training centers, and other institutions that use computers as a mode of training under a specific act. This would ensure that these establishments maintain adequate records, implement security measures, and cooperate with law enforcement agencies during investigations.

These proposed changes aim to enhance the effectiveness of cybercrime investigations, promote accountability, and ensure that the legislation keeps pace with the evolving nature of cyber threats.

9. Conclusion

Cybercrime poses a significant challenge to law enforcement agencies globally, including India. As technology advances and becomes more pervasive, electronic crime will increasingly feature in various forms of criminal behavior, including traditional offenses. Digital evidence will become more common, and law enforcement agencies must be prepared to address this new challenge.

To combat cybercrime, agencies worldwide are developing new partnerships, forensic methodologies, and responses. This requires new skills, technologies, and investigative techniques applied in a global context. The scope and scale of cybercrime demand timely responses and pose technical and legal complexities.

Innovative solutions, such as "cybercops," "cybercourts," and "cyberjudges," may be necessary to overcome jurisdictional issues and effectively address cybercrime. By working together and developing new strategies, law enforcement agencies can ensure safety and security on the internet.

Reference

1. Legard, D (2001), Hackers Hit Government Sites, Computer World, Vol 24 No. 26, 29 Jan, p.12.
2. Russell G. Smith, Peter Grabosky and Grgor Urbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press.
3. Seamus O Clardhuanin (2004), An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Summer 2004, Vol 3, Issue 1
4. International crime and Cyber Terrorism, <http://www.dfait-maeci.gc.ca/internationalcrime/cybercrime-en.asp>. 15. Visited www.cbi.nic.in



Cyber Extortion in India: A Critical Analysis of Legislation and Challenges

Shefali Bajpai¹, Dr. Hardayveer²

¹Research Scholar, Faculty of law, P.K. University, Shivpuri (M.P.)

²Associate Professor, Faculty of law, P.K. University, Shivpuri (M.P.)

Abstract:

The rapid growth of digital technologies has led to an alarming increase in cyber extortion cases in India, posing significant threats to individuals, businesses, and government entities. This paper examines the legislative framework governing cyber extortion in India, with a focus on the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita (BNS). It analyzes the key provisions, punishments, and challenges associated with addressing cyber extortion in India.

The paper highlights the complexities of enforcing cyber laws, particularly in cases involving jurisdictional issues and sophisticated cyber threats. It also discusses the initiatives taken by the Indian government to combat cybercrime, including the National Cyber Security Policy, 2023, and the Digital India Act.

Through a critical analysis of case laws, legislative provisions, and expert opinions, this paper identifies the gaps in the current legal framework and suggests measures to strengthen India's cyber extortion laws. The findings of this research will contribute to the ongoing discourse on cyber security and inform policy-making efforts to combat cyber extortion in India.

Keywords: Cyber extortion, Indian legislation, Information Technology Act, Bharatiya Nyaya Sanhita, cyber security, digital threats.

INTRODUCTION-

Cyber extortion is a growing threat in the digital age, where hackers and cybercriminals use malicious tactics to demand ransom from individuals, businesses, or organizations. This can involve threats to release sensitive data, disrupt services, or cause harm unless a payment is made. Cyber extortion can take many forms, including ransomware attacks, data breaches, and online blackmail. The consequences can be severe, resulting in financial loss, reputational damage, and emotional distress. To protect against cyber extortion, it's essential to implement robust cybersecurity measures, such as regular software updates, strong passwords, and data backups. Being aware of potential threats and taking proactive steps can help prevent cyber extortion and minimize its impact.

various forms of cyber extortion

Cyber extortion manifests in various forms, each with distinct characteristics and tactics.

Ransomware Attacks

Ransomware is malicious software that encrypts a victim's files or locks their system. The attacker dem-

ands a ransom, usually in cryptocurrency like Bitcoin, to provide the decryption key. Some ransomware attacks also involve “double extortion” where stolen data is threatened to be published if the ransom is not paid.

Distributed Denial of Service (DDoS) Attacks

In this method, the attacker floods a website or network with excessive traffic, making it unavailable to legitimate users. They then demand payment to stop or prevent these attacks.

Sextortion

This involves the attacker threatening to release private sexual images or videos of the victim unless they comply with demands, which can include payments or other actions.

Email Extortion

Attackers send emails to victims claiming to have compromising information or access to their systems, demanding ransom to avoid exposure.

Database Ransom

Attackers exploit vulnerabilities in database systems, replace data with ransom notes, and demand payment for data recovery.

Social Engineering and Phishing

Manipulating individuals into revealing sensitive information or downloading malware which can then be used to carry out extortion.

Legal Framework Related to Cyber Extortion in India

In India, cyber extortion is addressed under various provisions of the Information Technology Act, 2000 (IT Act), and the Indian Penal Code (IPC). Here are some key provisions:

Information Technology Act, 2000 (IT Act)

1. Section 43: Damage to computer systems, data, and networks. If someone gains unauthorized access to a computer system with the intention of causing harm or extorting money, they can be penalized under this section.
2. Section 66: Computer-related offenses, including hacking and unauthorized access to protected systems. This section applies to cases where cyber extortion involves hacking or gaining unauthorized access to computer systems.
3. Section 66C: Identity theft, including cases where an individual unlawfully obtains another person's credentials to commit fraud or extortion.
4. Section 66D: Cheating by personation using computer resources, addressing scenarios where cybercriminals impersonate others to commit fraud.
5. Section 66E: Violation of privacy, including capturing, publishing, or transmitting private images without consent, which can be a tactic used in cyber extortion.
6. Section 66F: Cyber terrorism, addressing severe cases of cyberattacks that threaten national security, including large-scale ransomware attacks that disrupt critical infrastructure.

7. Section 67: Publishing or transmitting obscene material in electronic form, which can be applicable in cases of online blackmail.

Indian Penal Code (IPC)

1. Section 383: Extortion, defined as intentionally putting a person in fear of injury or harm to induce them to deliver property or money.
2. Section 384: Punishment for extortion, which can include imprisonment up to three years, a fine, or both.
3. Section 503: Criminal intimidation, which includes threats intended to cause fear to force someone into doing or refraining from lawful actions.
4. Section 506: Punishment for criminal intimidation, which can include imprisonment up to two years, a fine, or both.

Bharatiya Nyaya Sanhita (BNS)

1. Section 308: Extortion, defined as intentionally putting someone in fear to obtain property or valuable security, punishable with imprisonment up to two years or fine or both.
2. Section 351: Criminal intimidation, which includes threats intended to cause fear to force someone into doing or refraining from lawful actions.

Notable Global Cyber Extortion Cases

Understanding real-life examples helps to grasp the magnitude of cyber extortion:

- **“Orange Is the New Black” (2017):** A hacker group accessed unreleased episodes of the show and demanded \$50,000 ransom. Despite Netflix paying, episodes were leaked.
- **Ashley Madison Data Breach (2015):** Hackers threatened to release personal data of millions unless the dating site ceased operations. When ignored, data was published, causing major privacy violations.
- **Colonial Pipeline Ransomware Attack (2021):** DarkSide ransomware caused an eight-day shutdown of the US fuel pipeline, leading to fuel shortages. The company reportedly paid nearly \$5 million in ransom.

These cases show the far-reaching consequences of cyber extortion, from financial loss to public safety threats.

1. Case Studies and Notable Legal Precedents

These case studies and legal precedents in India highlight the evolving landscape of cybercrime and the legal challenges surrounding privacy, freedom of speech, data protection, and cybersecurity. They demonstrate the need for continuous adaptation of laws, regulations, and policies to address emerging cyber threats while balancing the rights of individuals and the interests of national security and public safety.

2. **Shreya Singhal v. Union of India (2015):** In this landmark case, the Supreme Court of India struck down Section 66A of the Information Technology Act, 2000, which criminalized online speech and communication that was deemed to be offensive or of a menacing nature. The court held that the provision was vague, overbroad, and violated the fundamental right to freedom of speech and expression

3. **Aadhaar Data Leak Case:** In 2017, concerns were raised about the potential privacy and security risks associated with the Aadhaar system, India's biometric identification program. Several instances of data leaks and breaches were reported, leading to debates about the protection of personal information and the need for robust cybersecurity measures
4. **Paytm Phishing Case:** In 2019, a case involving phishing attacks targeting users of the popular digital payments platform, Paytm, garnered attention. Cybercriminals posed as Paytm representatives and tricked users into sharing their login credentials, leading to unauthorized access to their accounts and financial losses. The case highlighted the need for user awareness and stronger cybersecurity measures
5. **WhatsApp Spyware Attack Case:** In 2019, it was revealed that an Israeli spyware called Pegasus was allegedly used to target human rights activists, journalists, and government officials in India through the WhatsApp messaging platform. The incident raised concerns about the privacy and security of messaging apps, as well as the need for stronger regulation and protection against surveillance
6. **Twitter Hate Speech Case:** In 2021, Twitter faced legal challenges in India regarding the handling of hate speech content on its platform. The Indian government raised concerns about the spread of misinformation and inflammatory content, leading to clashes between the government and Twitter over compliance with local laws and content moderation practices.
7. **Coinsecure Bitcoin Theft Case** In 2018 Coinsecure, an Indian cryptocurrency exchange, suffered a significant theft of Bitcoins. The incident highlighted the vulnerability of cryptocurrency platforms and the challenges associated with investigating and recovering stolen digital assets. The case raised awareness about the need for robust security measures and regulatory frameworks for cryptocurrencies
- R v. Vijay Raj (2017):** In this case, a cybercriminal was arrested for defrauding individuals through an online job scam. The accused created a fake recruitment portal and collected money from job seekers by promising them lucrative positions. The court found the accused guilty and sentenced him to imprisonment, highlighting the consequences of online fraud and the need for strong legal action

Suggestions for effective cybercrime legislation and law enforcement in India:

By implementing these best practices, India can strengthen its legislative framework, improve law enforcement capabilities, and effectively combat cybercrimes, ensuring a safer and secure cyberspace for its citizens and organisations. Effective cybercrime legislation and law enforcement in India can be enhanced by implementing best practices. Here are some key practices to consider

1. **Comprehensive and Updated Legislation:** Develop and regularly update cybercrime laws to address emerging threats and technological advancements. The legislation should cover a broad range of cyber offenses, including unauthorized access, hacking, identity theft, data breaches, online fraud, and cyber harassment.
2. **Clear Definitions and Jurisdiction:** Provide clear definitions of cybercrimes and establish jurisdictional provisions to address cross-border offenses. Clearly define the scope of offenses, elements of the crimes, and the legal consequences associated with them.
3. **International Cooperation:** Foster international cooperation and collaboration through mutual legal assistance treaties (MLATs), extradition agreements, and information sharing mechanisms Establish

channels for timely and efficient cooperation with other countries in investigating and prosecuting cybercriminals operating across borders.

4. **Capacity Building:** Invest in training programs and capacity building initiatives for law enforcement agencies, prosecutors, and judges to enhance their understanding of cybercrime laws, digital evidence collection, and forensic analysis. Promote specialised cybercrime units and encourage interdisciplinary collaboration among relevant stakeholders.
5. **Public-Private Partnerships:** Foster collaboration between government agencies, law enforcement, and the private sector, including internet service providers (ISPs), technology companies, and cybersecurity firms. Encourage sharing of threat intelligence, expertise, and resources to effectively combat cybercrimes.
6. **Cyber Incident Reporting and Response:** Establish mechanisms for individuals, organizations, and law enforcement agencies to report cyber incidents promptly. Develop effective procedures for incident response, evidence preservation, and victim support.
7. **Data Protection and Privacy:** Strengthen data protection laws and regulations to safeguard personal information and ensure privacy rights are respected. Encourage organisations to adopt the best data security and privacy practices, including encryption, access controls, and regular security audits.
8. **Awareness and Education:** Promote public awareness campaigns and educational programs to raise awareness about cyber threats, safe online practices, and reporting mechanisms. Educate individuals, businesses, and vulnerable groups on cybersecurity measures and the risks associated with cybercrimes

Conclusion

In a digital era, many services are online, especially after the Covid-19. For in Digilocker, if we urgently need our marsheet, without going anywhere we easily find our marsksheet, degrees, etc in other words, we say that all our data is stored online, and we can find our data anywhere in the world. So, in that case protection of the data depends on ourselves. If we securely protect our data by putting strong passwords and other security measures applied then no one of the hackers will steal our data and misuse it.

This paper also highlights the significance of domestic legislation and approaches in combating cybercrimes in India. The enactment of the Information Technology Act, 2000, and establishing specialised cybercrime units demonstrate the country's commitment to addressing this issue. However, continuous efforts are required to update legislation, strengthen law enforcement capabilities, foster public-private partnerships, and raise awareness among individuals and organisations. While progress has been made, it is evident that cybercrimes remain a persistent and evolving threat. The research emphasises the need for ongoing research, policy development, and capacity building to stay ahead of cybercriminals and protect the digital ecosystem. Lastly, addressing cybercrimes requires a multi-faceted approach that combines robust legislation, international cooperation, effective law enforcement, privacy protection, and public awareness. By adopting best practices, embracing technological advancements, and fostering collaboration among stakeholders, India can mitigate the risks associated with cybercrimes and safeguard its digital landscape for the benefit of its citizens and the nation

Reference-

1. Shital Kharat, "Cyber Crime – A Threat to Persons, Property, Government and Societies" (Rochester,

NY, 2017).

2. Mohan Krishna Kagita et al., “A Review on Cyber Crimes on the Internet of Things,” in A. Makkar, N. Kumar (eds.), *Deep Learning for Security and Privacy Preservation in IoT* 83–98 (Springer, Singapore, 2021)
3. Times, Apr. 13, 2018, available at:
<https://economictimes.indiatimes.com/industry/banking/finance/banking/bitcoins-worth-rs-20-crore-stolen-from-exchange-in-indias-biggest-crypto-theft/articleshow/63740771.cms?from=mdr>
4. Shreya Singhal v. Union of India, AIR 2015 SC 1523
5. Shubham Singh, “New Aadhaar Data Leak Exposes 11 Crore Indian Farmers’ Sensitive Info”, Zee News, June 14, 2022, available at: <https://zeenews.india.com/personal-finance/aadhaar-data-breach-over-110-crore-indian-farmers-aadhaar-carddata-compromised-2473666.html> Editorial, “Paytm Offers Cyber Fraud Cover of up to Rs 10,000 at Rs 30 Read More At: [Http://Timesofindia.indiatimes.com/Articleshow/96357846.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst](http://Timesofindia.indiatimes.com/Articleshow/96357846.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst)”, The Times of India, Dec. 20, 2022, available at: <https://timesofindia.indiatimes.com/city/mumbai/paytm-offers-cyberfraud-cover-of-up-to-10000-at-30/articleshow/96357846.cms>.
6. Editorial, “WhatsApp Spyware Attack Was Attempt to Hack Human Rights Data”, The Guardians, May 14, 2019, available at: <https://www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-wasdesperate>
7. Editorial, “Bitcoins Worth Rs 20 Crore Stolen from Exchange in India's Biggest Crypto Theft Read More At: [Https://Economictimes.indiatimes.com/Industry/Banking/Finance/Banking/Bitcoins-Worth-Rs-20-Crore-Stolen-From-ExchangeIn-Indias-Biggest-Crypto](https://Economictimes.indiatimes.com/Industry/Banking/Finance/Banking/Bitcoins-Worth-Rs-20-Crore-Stolen-From-ExchangeIn-Indias-Biggest-Crypto)