Rivista Italiana di Filosofia Analitica Junior Vol 14, No. 1 (2023)
ISSN: 2037-4445

A Study Relating to Cyber Crimes in India During Covid-19 and the Regulations

Bhanu Gangwal[1], Prof. Mahesh Koolwal[2]

[1] Ph.D. Scholar, School of Law, JECRC University, Jaipur (Rajasthan), India

[2] Professor (Dean), School of Law, JECRC University, Jaipur (Rajasthan), India

Email: bhanugangwal9328@gmail.com; dean.law@jecrcu.edu.in

ABSTRACT

Cybercrime has increased because of digitalization, particularly during and after the COVID-19 pandemic. Between March and April of 2020, there was 86 percent increase in cybercrime in India. As the internet makes it possible for people to access everything, especially during and after the Pandemic, consumers are relying more on the internet for all their needs. Even though the internet has fundamentally altered our society, illegal access to information and harm remains. As a result, the most pressing issue of our time is ensuring the safety and security of information. Cases of cybercrime are rising at the same rate as the number of users, and there are no geographical or national boundaries to speak of. Additionally, it has a direct detrimental effect on people's social and economic lives, making it extremely concerning. The quantitative analysis of cybercrime cases in India's most vulnerable metropolises serves as the foundation for this study. This article analyses the numerous types of cybercrime that individuals are currently dealing with, focusing on the unique obstacles and issues that can be encountered, avoided, and remedied.

Keywords--- Internet-crime, IT Act, IPC, Online Offences

INTRODUCTION

India has the second-most critical client-put together web with respect to the planet in its emerging mechanized economy. Cybercrime is used to describe illegal PC exercises. In the new millennium, the transition of the world's population from the real world to the digital one has sparked yet another economic upheaval. While computer related crimes include more specific types of crimes like phishing schemes and viruses, traditional crimes can be carried out using or without a computer. Any criminal behavior done online is referred to as "cybercrime," often called as "online crimes" or "computer crimes." Cybercrime is a similarly nuance type of unlawful affair on the planet. Cybercrime refers to any offence performed on or through ‘personal computers’, the ‘internet’, or any innovation covered under the Data Innovation Act. Internet crime, which has a terrible and crushing impact, is the most pervasive and productive crime in India. In addition to causing serious and persistent harm to society and the government, criminals and wrongdoers frequently conceal their identities.

To tell you the truth, skilled con artists are involved in numerous illegal online activities. Any act that uses a computer or the internet as a tool, a target, or both in an illegal development is considered cybercrime, according to a broad definition.

The phrase "cybercrime" has been explained in a few Supreme and High Court rulings, but it does not appear to be stated in any Indian assembly law or regulation. Given the increasing reliance of modern culture on innovation, cybercrime is a relentlessly harmful activity. Users increasingly value the convenience provided by computers and other related technologies, which are becoming increasingly integrated into everyday life. It is a deep average that never ends. The internet has positive and negative effects on us at the same time. Examples of emerging cybercriminals include email spoofing, cyber

violence, and cyber damage. If they are approved to be spread across the Internet, some regular crimes may be classified as cybercrime.

At the end of the day, digital wrongdoing includes Theft of stored or online information, damage to hardware and information, and unauthorized entry into the PC environment or data base of another control are only a few instances of crimes that are directly related to the use of PCs. Cyberattacks are a real threat in today's world of online processing and information. Cybercrime is failing to follow internet or cyber laws. The phrase "cyber law" indicates to all the specific and legal facets of the Internet and the World Wide Web. Digital regulation is quite close to anything that is interested in, linked to, or arising from valid perspectives or issues involving any online movement of locals and others. Traditional crimes including theft, fraud, forgery, defamation, and mischief are governed by the Indian Penal Code, while cybercrimes like hacking, phishing, email spoofing, email spamming, and email bombing are dealt with by the Information Technology Act 2000.

REVIEW OF LITERATURE

Nappinai N. S. (2010): The author asks, "Has cybercrime law in India kept up with emerging trends?" in his paper. An Experimental Review" perceived explicit immense fragments of the criminal guidelines in India associating with data security, assurance, encryption, and other computerized bad behavior activities and how much those game plans are executed to fight both current and anticipated designs in cybercrime.

Rohas N. (2008): The author of the book "fundamentals of cyber law" goes over fundamental terms and definitions related to computers and the internet. In-depth explanations are provided for the Indian Cyber Law, the IT Act 2000, and the Indian Penal Code (IPC). Additionally, the author has discussed the applicable penalties for nearly 21 cybercrimes that are committed online. An overview of the operation of email systems, blogs, domain name spaces (DNS), and IP addresses is provided. The book offers exhaustive clarifications of digital regulation's basics.

Cassim F. (2009): "Formulating specialized legislation to address the growing spectra of cyber-crime: A comparative study" examines the cyber laws that have been developed to combat cybercrime in South Africa, India, the Gulf states, the United Kingdom, Australia, and the United States of America. The analysis says that specialized cyber legislation was created because national laws didn't deal with the problems caused by cybercrime. In light of the rapid growth of cybercrime and innovation, it is proposed that nations adopt new digital regulations. In order to keep them up to date with the rapidly changing technology, IT security personnel, financial services sector employees, police officers, prosecutors, and members of the judicial system ought to receive ongoing research and training.

Shrikant A. et al. (2010): The privacy issue is examined in light of legal, technical, and political obstacles in this paper from an Indian point of view. The framework that the authors have created to deal with these issues is discussed. There is no comparative overall set of laws to address protection issues in India. We now turn to the IT Act of 2003, which was created to make e-commerce easier and for which privacy was not the primary concern, to address the most pressing issues. As per the present and extended needs for security in the Indian situation, this study offers an answer.

Talwant S. (2004): The requirement of law enforcement and computer agencies to work together has been raised by an Additional District and Sessions Judge as a significant and uncommon issue of debate. Both components, in the author's opinion, are equally crucial for establishing strong national cyber security and ensuring that internet users are protected online. The author has also conducted a comparison of Indian and US legal definitions.

Ashwini B. (2012): The creator talks commonly on the pace of rising online crime and its effect on people, internet business, and other shop owners. The topic of online threats and scams, as well as the scope of internet use in India and its future, are briefly discussed in this article. In addition, the author

sheds light on the government's efforts to combat cybercrime and the challenges India must overcome to eliminate the threat.

RESEARCH OBJECTIVES

The following research article deals with the following things:

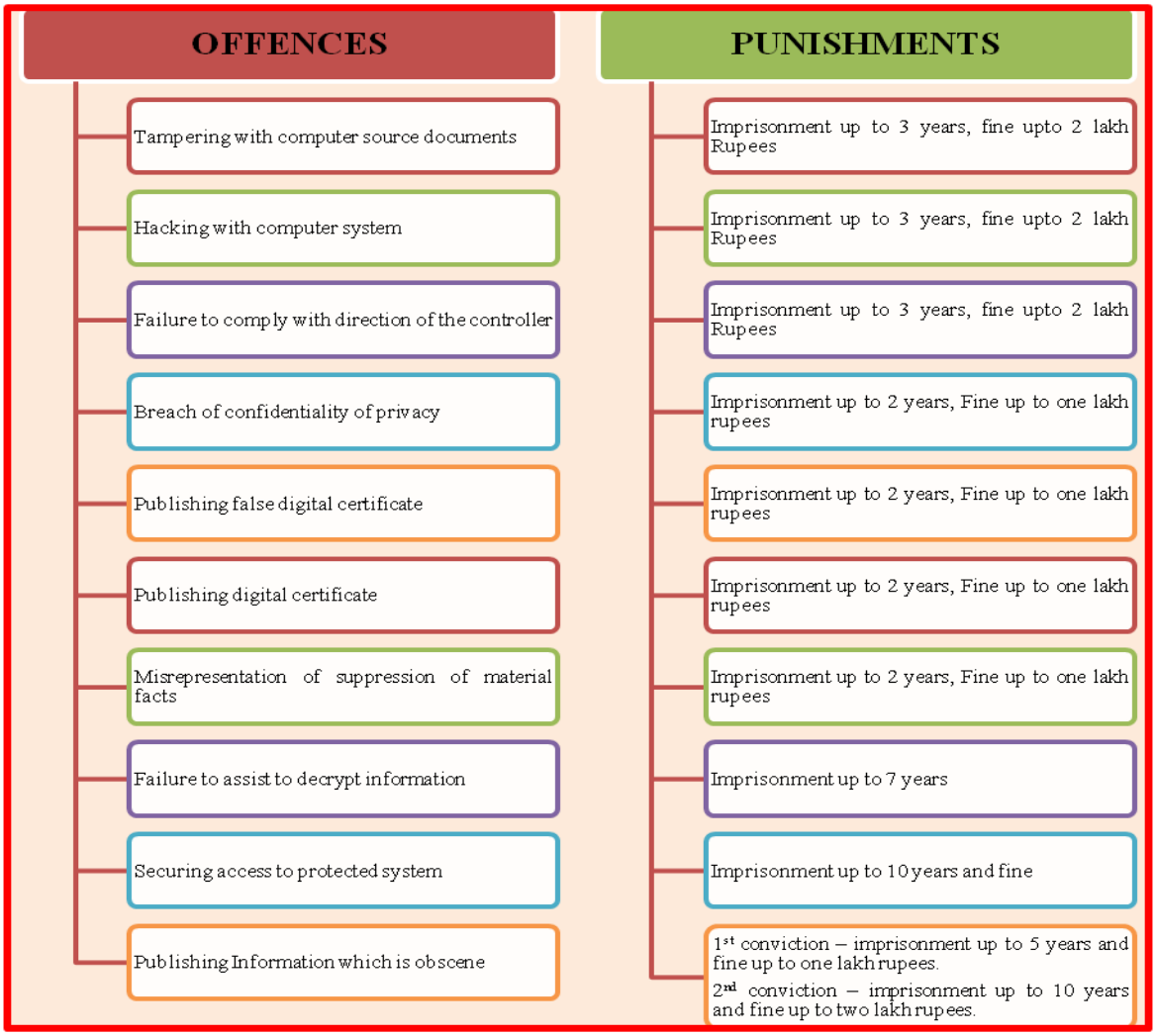
1. To study and analyze the various cyber-crimes occurring in India.
2. Also, to deal with the new age cyber laws and the remedies relating to these crimes.

RESEARCH METHODS

Methods of Data Collection: In order to attain both the research objectives, for the first objective primary data has been used as the data relating to the number of crimes occurring in different cities of India shall be gathered from the National Crime Records Bureau and other Regulating Agencies. And, for the second objective, the secondary data collection technique shall be used as the various Statutory Laws and prevalent remedial theories and methods has been studied as to mitigate the Cyber-crime in India and punish the offenders.

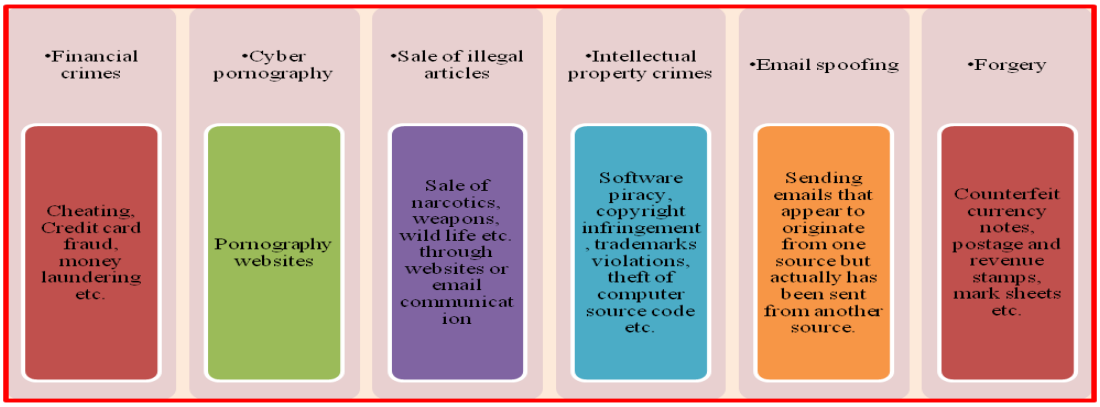
CYBER LAWS: OFFENCES AND PUNISHMENTS

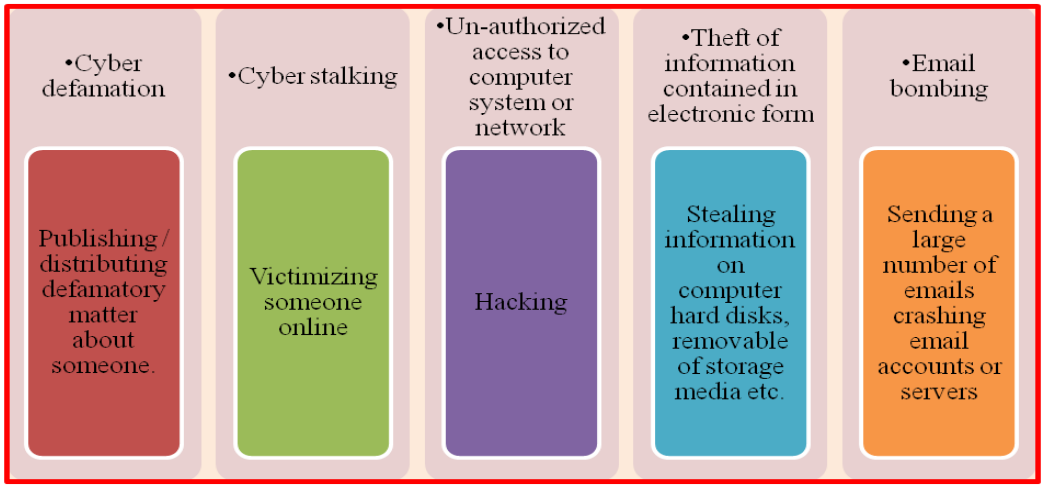
There are various kinds of digital wrongdoing exercises and offenses and accordingly, the discipline given to the lawbreaker additionally vary according to the wrongdoing perpetrated. The offences listed under the IT Act of 2000 and the associated sanctions are shown in table:



Prevalent Cyber-Crimes in India

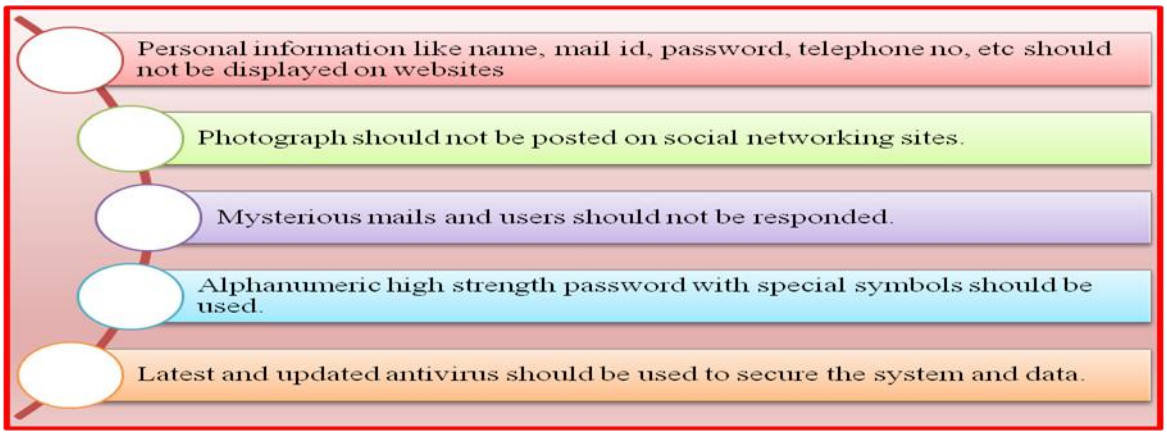
The most prevalent cyber- crime in India are being shown as under:-





SECURITY ACTIONS TO CONTROL CYBERCRIME

We can take a few steps to prevent digital misbehavior in our public despite the government's digital legislation and procedures. Not many of the following are ideas:



A Study of the Most Severe Cybercrimes in India

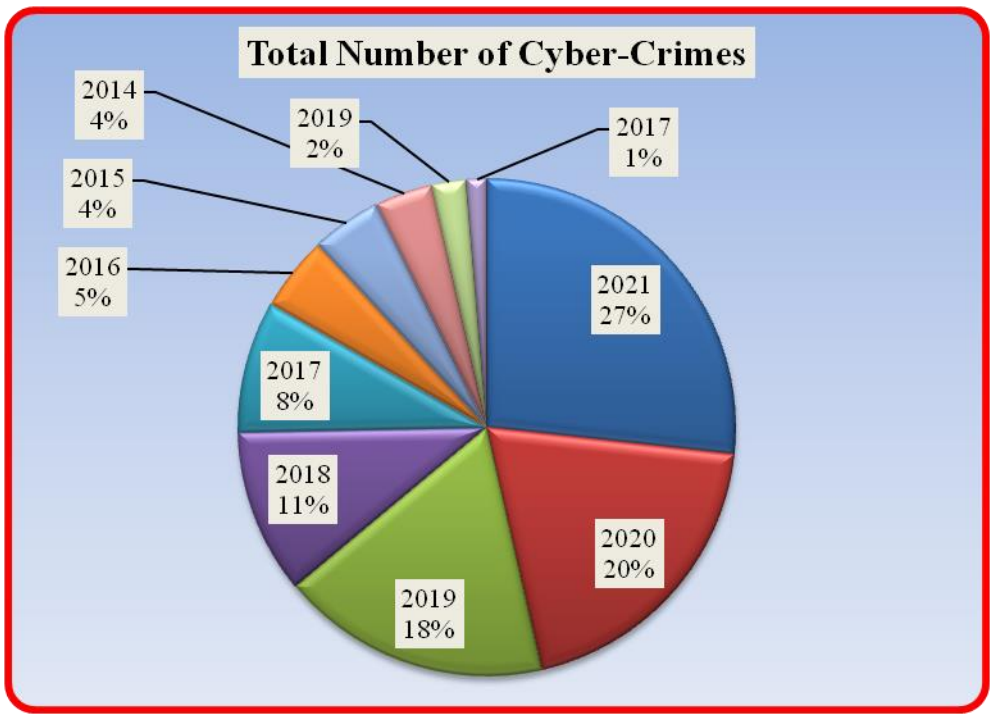
A total of 27,248 incidents of cybercrimes were reported in India, according to the most recent data from the National Crime Record Department (NCRB) (22Ap).

Table 1: India's total number of reported cybercrimes from 2017 to 2021

Year	Total number of cyber-crimes
2021	68,045
2020	50,035
2019	44,735
2018	27,248
2017	21,796

2016	12,317
2015	11,592
2014	9,622
2019	5,693
2017	3,377

Graph 1: Cyber-crimes reported in India from 2017-2021



The table above shows that there has obviously been an expansion in the quantity of cybercrime occurrences in India throughout the span of every year. The most prevalent sorts of digital crime are extortion, deception, Visa misrepresentation, wholesale fraud, online badgering, digital following, digital tormenting, and so on.

.Table 2: Cyber Crimes in Metropolitan Cities - 2017-2019

S. No	City	2017	2018	2019	Percentage Share of City (2019)	Actual Population (in Lakhs) (2011)+	Crime Rate (Col.5/ Col.7) (2019)++
1	Ahmedabad (Gujarat)	112	212	171	0.9	63.5	2.7
2	Bengaluru (Karnataka)	2743	5253	10555	57.5	85.0	124.2
3	Chennai (Tamil Nadu)	52	73	118	0.6	87.0	1.4
4	Coimbatore (Tamil Nadu)	19	15	8	0.0	21.5	0.4
5	Delhi	143	163	107	0.6	163.1	0.7
6	Ghaziabad (Uttar Pradesh)	118	191	347	1.9	23.6	14.7
7	Hyderabad (Telangana)	328	428	1379	7.5	77.5	17.8
8	Indore (Madhya Pradesh)	32	39	41	0.2	21.7	1.9
9	Jaipur (Rajasthan)	685	415	544	3.0	30.7	17.7
10	Kanpur (Uttar Pradesh)	229	229	365	2.0	29.2	12.5
11	Kochi (Kerala)	39	48	43	0.2	21.2	2.0
12	Kolkata (West Bengal)	196	32	32	0.2	141.1	0.2
13	Kozhikode (Kerala)	12	27	15	0.1	20.3	0.7
14	Lucknow (Uttar Pradesh)	608	962	1262	6.9	29.0	43.5
15	Mumbai (Maharashtra)	1362	1482	2527	13.8	184.1	13.7
16	Nagpur (Maharashtra)	82	106	119	0.6	25.0	4.8
17	Patna (Bihar)	79	115	202	1.1	20.5	9.9
18	Pune (Maharashtra)	318	153	309	1.7	50.5	6.1
19	Surat (Gujarat)	105	155	228	1.2	45.8	5.0
	TOTAL CITIES	**7262**	**10098**	**18372**	**100**	**1140.4**	**16.1**

'+' The crime rate is expressed as a percentage of one lakh people.

- Populace Source: Enlistment center General of India Genuine Populace in view of 2011 Evaluation.

- According to information given by the States/Union Territories.
- Information prepared for 2018 was used because information from Kolkata was not available in time for 2019.

Graph 2: Cyber Crimes in Metropolitan Cities - 2017-2019

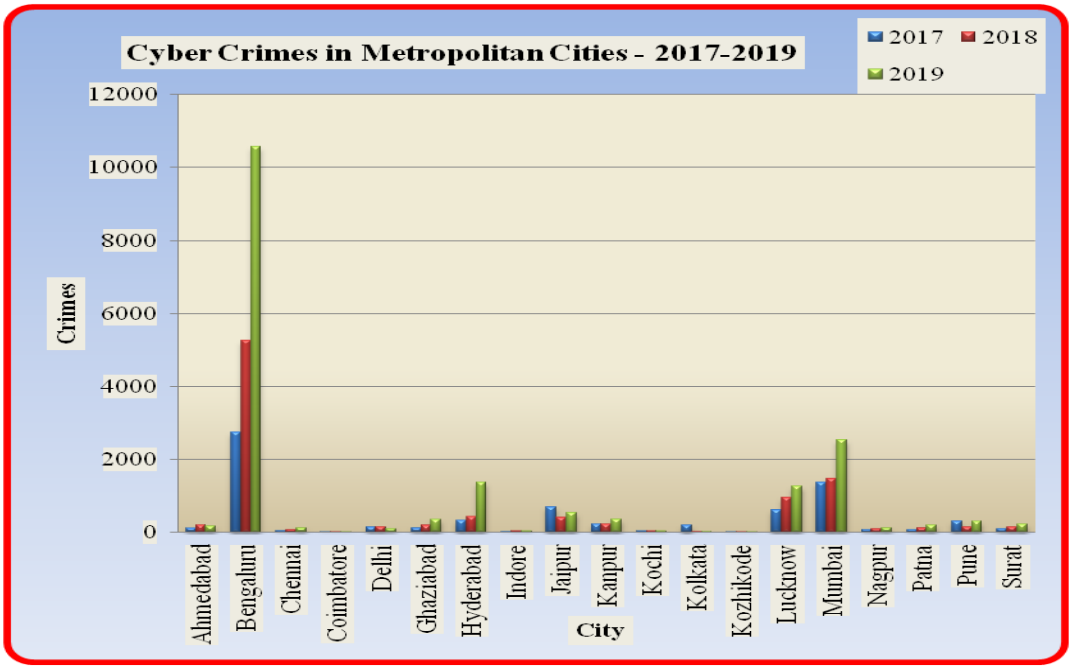


Table 3A: Cases under the IT Act involving cybercrimes in major cities in 2019

S. No	City	A. Offences under I.T. Act						
		Tampering computer source documents (Sec.65)	Computer Related Offences					
			Computer Related Offences	Computer Related Offences (Sec.66)			Dishonestly receiving stolen computer resource or communication device (Sec.66B)	Identity Theft (Sec. 66C)
				Computer Related Offences (Sec.66)	Ransomware	Offences other than Ransomware		
1	Ahmedabad	2	29	2	0	2	0	21
2	Bengaluru	10	10324	125	13	112	21	10000
3	Chennai	1	42	18	12	6	0	14
4	Coimbatore	0	0	0	0	0	0	0
5	Delhi	0	31	4	0	4	8	8
6	Ghaziabad	0	192	39	39	0	67	39
7	Hyderabad	0	1267	3	3	0	0	0
8	Indore	0	3	1	0	1	0	2
9	Jaipur	1	227	2	0	2	1	134
10	Kanpur	0	323	256	0	256	0	67
11	Kochi	0	10	2	0	2	2	1
12	Kolkata	0	7	5	0	5	0	2
13	Kozhikode	0	2	0	0	0	0	0
14	Lucknow	0	1143	557	544	13	0	72
15	Mumbai	0	25	2	1	1	1	17
16	Nagpur	0	5	0	0	0	0	0
17	Patna	0	0	0	0	0	0	0
18	Pune	0	43	0	0	0	0	19
19	Surat	0	141	0	0	0	0	140
	TOTAL CITIES	14	13814	1016	612	404	100	10536

- As per the information provided by the States/UTs

- As the data from Kolkata could not be accessed for 2019, the information provided for 2018 has been utilized.

Table 3B: Cyber Crimes - IT Act Cases in Metropolitan Cities – 2019

S. No	City	A. Offences under I.T. Act				
		Computer Related Offences		Cyber Terrorism (Sec.66 F)	Publication/ transmission of obscene / sexually explicit act in electronic form (Sec. 67)	
		Cheating by personation by using computer resource (Sec.66D)	Violation of Privacy (Sec.66E)		Publication/ transmission of obscene / sexually explicit act in electronic form (Total)	A) Publishing or transmitting obscene material in Electronic Form
1	Ahmedabad	5	1	0	17	16
2	Bengaluru	158	20	0	216	146
3	Chennai	9	1	0	29	9
4	Coimbatore	0	0	0	1	0
5	Delhi	8	3	0	12	4
6	Ghaziabad	47	0	0	28	17
7	Hyderabad	1264	0	0	112	0
8	Indore	0	0	0	0	0
9	Jaipur	88	2	0	23	9
10	Kanpur	0	0	0	42	42
11	Kochi	2	3	0	7	5
12	Kolkata	0	0	0	1	0
13	Kozhikode	1	1	0	2	1
14	Lucknow	512	2	0	119	83
15	Mumbai	5	0	0	8	0
16	Nagpur	5	0	0	6	1
17	Patna	0	0	0	0	0
18	Pune	23	1	0	9	3
19	Surat	0	1	0	2	1
	TOTAL CITIES	2127	35	0	634	337

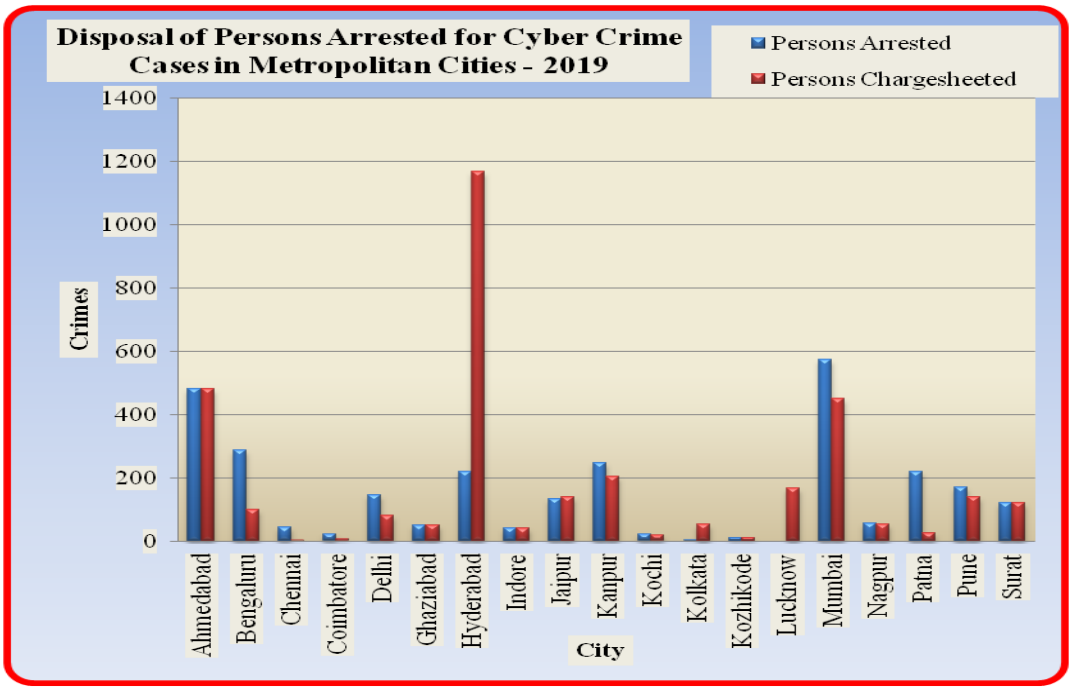
- As per data provided by States/UTs
- Due to unobtainability of data from Kolkata in time for 2019, Data furnished for 2018 has been used.

Table 4: Data of Persons Arrested for Cyber Crime Cases in Metropolitan Cities – 2019

S. No	City	Persons Arrested			Persons Charge sheeted			Persons Convicted			Persons Discharged			Persons Acquitted		
		Male	Female	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total	Male	Female	Total
1	Ahmedabad (Gujarat)	388	94	482	388	94	482	0	0	0	0	0	0	2	0	2
2	Bengaluru (Karnataka)	275	14	289	97	3	100	7	0	7	0	0	0	21	1	22
3	Chennai (Tamil Nadu)	42	2	44	2	0	2	0	0	0	0	0	0	0	0	0
4	Coimbatore (Tamil Nadu)	20	2	22	7	0	7	1	0	1	0	0	0	1	0	1
5	Delhi	143	2	145	79	1	80	2	0	2	1	0	1	12	0	12
6	Ghaziabad (Uttar Pradesh)	50	0	50	50	0	50	0	0	0	0	0	0	0	0	0
7	Hyderabad (Telangana)	204	17	221	559	610	1169	6	0	6	0	0	0	13	122	135
\8	Indore (Madhya Pradesh)	33	10	43	31	10	41	6	0	6	0	0	0	8	0	8
9	Jaipur (Rajasthan)	133	1	134	137	3	140	4	0	4	19	2	21	1	0	1
10	Kanpur (Uttar Pradesh)	249	0	249	204	0	204	15	0	15	0	0	0	3	0	3
11	Kochi (Kerala)	22	0	22	19	0	19	0	0	0	0	0	0	3	0	3
12	Kolkata (West Bengal)	5	0	5	54	0	54	3	0	3	0	0	0	7	0	7
13	Kozhikode (Kerala)	11	0	11	12	0	12	0	0	0	0	0	0	0	0	0
14	Lucknow (Uttar Pradesh)	0	0	0	168	0	168	0	0	0	0	0	0	0	0	0
15	Mumbai (Maharashtra)	543	30	573	444	8	452	3	0	3	2	0	2	13	2	15
16	Nagpur (Maharashtra)	56	1	57	53	1	54	0	0	0	0	0	0	5	0	5
17	Patna (Bihar)	219	0	219	26	0	26	0	0	0	0	0	0	0	0	0
18	Pune (Maharashtra)	158	14	172	128	12	140	0	0	0	0	0	0	1	0	1
19	Surat (Gujarat)	111	12	123	111	12	123	0	0	0	0	0	0	1	0	1
	TOTAL CITIES	2662	199	2861	2569	754	3323	47	0	47	22	2	24	91	125	216

- As per the information provided by the States/UTs
- Due to the late arrival of data from Kolkata for 2019, information provided for 2018 has been utilized.

Graph 4: Persons Released from Arrest in Cyber Crime Cases in Major Cities in 2019



ANALYSIS OF DATA

The National Crime Records Bureau Agency, various other Undertakings and Agencies and the Legislature of India provided the measurable data. According to the digital crime and wrongdoing cases enrolled and individuals captured under both the Data Innovation Act and the Indian Corrective Code, the information has been dissected and the weakest states, urban areas, and four metropolitan urban communities of India have also been identified. Figures 1 to 3 demonstrate that there were more cybercrime instances reported in 2017 than there were in 2016, demonstrating an increase in cases across all states and cities in India. According to the cybercrime cases registers for the years 2017 and 2019, it has been discovered that Mumbai, Bengaluru, and Maharashtra are the most vulnerable states and cities in India. Since the people arrested in 2019 are from cases that were registered up until 2019, figure 4 shows that there are more people arrested in Maharashtra in 2019 than there are cases. In any case, from figure-4 to figure-6 show that individuals caught against the advanced bad behavior cases enrolled are basically less in the year 2019. When compared to the cases enrolled in 2019, the number of people captured in Assam and Bengaluru is significantly lower.

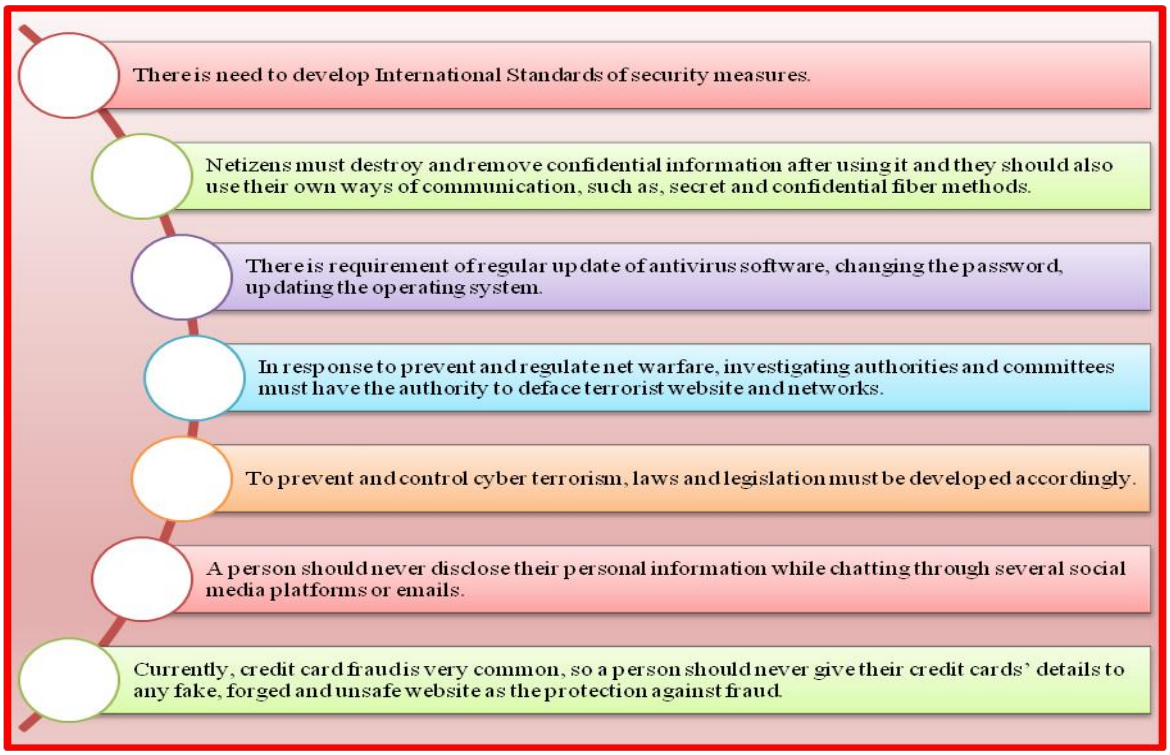
CONCLUSION

The primary goal of the research was to learn more about how the number of cases of digital wrongdoing in India has grown over time. This paper argues that in this innovation-based age, many forms of digital wrongdoing are winning. An examination reveals that the amount of cybercrime cases in various Indian states and cities has steadily increased over the past decade. The figure of individuals captured close to the digital wrongdoing cases register is phenomenally less. As a result, it became plainly evident that the Information Technology Act's incapacity to offer full cyber defence leaves our cyber frameworks and Indian cyber laws unresolved. As a result, it calls for the joint application of solid cyber laws and efficient regulation.

SUGGESTIONS

The legal executive can assume a significant part in digital policing, outfitted with high innovation. It could control the equity productively. E-equity can give a fast way to punishment of cybercriminals immediately. " Evidence is lost when follow-up is delayed. It is noteworthy that electronic records are not permanent in comparison to other types of records."

To forestall internet crimes, there are different methods that an individual ought to be aware for counteraction and controlling of cybercrime by regulation and public:



REFERENCES

1. Wow essay (2009), Top Lycos Networks, Available at: http://www.wowessays.com/dbase/ab2/nyr90.shtml.
2. A. Cruz, Cyber Crime and how it affects you, Cyber security tips, vol.7, issue1, January 2019.
3. K. Seth, IT Act 2000 vs. 2008-Implementation, Challenges, and the Role of Adjudicating Officers, National Seminar on Enforcement of cyber law, New Delhi,8th may 2010.
4. National Crime Records Bureau, Ministry of Home Affairs, Government of India, Crime in India 2017 Statistics.
5. Z. Mohiuddin, Cyber laws in Pakistan-a situational analysis and way Forward Ericsson Pakistan (Pvt.) Ltd, June 24, 2006.
6. H. Saini, Y.S. Rao, T.C. Panda, Cyber crime and Their Impacts: A Review, International Journal of Engineering Research and Application, vol.2, Issue2, pp.202-209, 2017.
7. Anil Lamba, 2014. "Uses Of Cluster Computing Techniques To Perform Big Data Analytics For Smart Grid Automation System", International Journal for Technological Research in Engineering, Volume 1 Issue 7, pp.5804-5808,2347-4718..

8. M. Olusola, O. Samson, A. Semiu, A. yinka, Impact on cyber crime on Nigerian Economy, The International journal of Engineering and Science,Vol.2,Issue4,pp.45-51,2019.
9. R. P. Kaur, Statistics of cyber crime in India: An overview, International journal of Engineering and Computer Science, vol.2, issue8, pp.2555-2559, 2019.
10. Computer Hope (2017), Data Theft, Available at: http://www.computerhope.com/jargon/d/datatheft.html.
11. R.S. Patel, D. Kathiria, Evolution of cyber crime in India, International Journal of Emerging Trends and Technology in Computer science,vol.2,issue 4,pp.240-243,2019.
12. National crime record bureau, Statistica 2019, http://ncrb.gov.in/CD-CII2019/home.asp.
13. The Gazette of India by ministry of law &justice. Part ii, sec-1.No-13, New Delhi, Feb 5, 2009.
14. R. Dubey, Cyber Crime "an unlawful act where in the computer is either a tool or a target or both", in Indian legal perspective, Sept 24, 2004.
15. Nappinai N.S., "Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study", in Journal of International Law and Technology, January 2010.
16. Nagpal Rohas, "Fundamentals of Cyber Law", Asian School of Cyber Laws, 2008.
17. Cassim F, "Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study", in Potchefstroom Electronic Law Journal, Vol. 12 No. 4 (2009).
18. Ardhapurkar Shrikant et al., "Privacy and Data Protection in Cyberspace in Indian Environment", in International Journal of Engineering Science and Technology, May 2010.
19. Singh Talwant, "Cyber Law & Information Technology".
20. B. Ashwini, "An Intelligent Analysis of Crime through Newspaper Articles – Clustering and Classification", in International Journal on Recent and Innovation Trends in Computing and Communication, February 2017.