ISSN : 2395-4132

THE EXPRESSION

An International Multidisciplinary e-Journal

Bimonthly Refereed & Indexed Open Access e-Journal

Impact Factor 3.9

Vol. 8 Issue 4 August 2022

Editor-in-Chief : Dr. Bijender Singh

Email : editor@expressionjournal.com

www.expressionjournal.com

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 3.9)
www.expressionjournal.comISSN: 2395-4132

LEGAL REGIME ON CYBER CRIME: AN ANALYSIS OF NCRB DATA

Ruchi Maurya, [LL.M. Qualified UGC NET & JRF]
Research Scholar, Department of Law, Central University of Punjab, Bathinda, India
Dr. Sukhwinder Kaur
Assistant Professor, Department of Law, Central University of Punjab, Bathinda, India
Mr. Sadanand Patel, [LL.M. Qualified UGC NET & JRF]
Research Scholar, Department of Law, Central University of Punjab, Bathinda, India

Abstract

The human race is currently connecting with each other at the fastest rate possible due to the rapid technological advancements. With the technical advances, what once looked like a dream has become a reality. Today, humans can operate anything at the tip of their fingers, including rockets, running trains, and mobile phones. The computer has improved our ability to store, retrieve, extract, and convey data as well as our access to information, enabling us to communicate with anyone, anywhere, at any time. It is an inventive technology. But the developments of computers and improvements in information and communication technology have led to a rise in crimes committed online. These are the crimes that do need to be committed with the help of a physical weapon, and do not need a physical space to be committed or even the physical presence of the attacker. These are known as 'Cybercrimes'. Such crimes have the potential to cross borders and cause harm to the victims; without being traced. Cybercrime poses a larger risk to society not only because of its nature but also because of the havoc it may cause in a short period of time, as little as few minutes. For as long as it could be detected, the government and other social organizations could curb such crimes. The objectives is to understand the concept of the cybercrimes, to know the provisions of the Information Technology Act, 2000 dealing with cybercrimes and to analyze the statistical data of National Crime Records Bureau regarding cybercrimes from 2016 to 2021.The research methodology adopted for the paper is doctrinal and data collected from secondary sources. The secondary data collected from printed books, online legal research websites and information portals.For the purpose of the research paper, the statistics and reports published by National Crime Record Bureau (NCRB) is analyzed. Moreover, the legal statute, laws, and provisions available for dealing with cybercrimes in India are critically studied.

Keywords

Cyber crime, National Crime Record Bureau, Information Technology Act, 2000.

The Expression: An International Multidisciplinary e-Journal
(A Peer Reviewed and Indexed Journal with Impact Factor 3.9)
www.expressionjournal.comISSN: 2395-4132

LEGAL REGIME ON CYBER CRIME: AN ANALYSIS OF NCRB DATA

Ruchi Maurya, [LL.M. Qualified UGC NET & JRF]
Research Scholar, Department of Law, Central University of Punjab, Bathinda, India
Dr. Sukhwinder Kaur
Assistant Professor, Department of Law, Central University of Punjab, Bathinda, India
Mr. Sadanand Patel, [LL.M. Qualified UGC NET & JRF]
Research Scholar, Department of Law, Central University of Punjab, Bathinda, India

INTRODUCTION:

It is well known that the cybercrimes are committed by making use of computers either as a tool or as a target by making use of computer networks, but the crime is not committed by the computer itself. It is committed by humans and therefore it can be said the technology has helped humans to increase their capabilities of committing crime and vandalising information necessary for running daily activities to functioning of worldly affairs that are dependent on technology. Dependency on the technology and services availed through technology assisted sources have led to the exposure of the beneficiaries or the internet users to the vulnerabilities and threats posed by the same technology. As much as technology helps in connecting people and making daily transactions easier for them, it can cause inconveniences to the people who are not aware about the threats and losses it might cause when being used by criminals to exploit for illegal gains. The advancement of technology gave birth to cybercrimes of various kinds and presently the world is facing the issues and challenges to not only combat the alarming rise in the existing cybercrimes but also to combat the emerging forms of cybercrimes. Both the beneficiary and the ultimate victim of technology assisted crimes, happens to be the society. Cybercrimes have the tendency to affect the organisational functioning, government proceedings and most importantly and largely the citizens of a country.

OBJECTIVES:

- To understand the concept of the cybercrimes and to know the provisions of the information Technology Act, 2000 dealing with cybercrimes.
- To analyze the statistical data of National Crime Records Bureau regarding cybercrimes from 2016 to 2021.

RESEARCH METHODOLOGY:

The research methodology adopted for the paper is doctrinal and data collected from secondary sources. The secondary data collected from printed books, online legal research websites and information portals. The statistics and reports published by National Crime

Record Bureau (NCRB) are analyzed during documenting the research paper. Moreover, the legal statute, laws, and provisions available for dealing with cybercrimes in India are studied.

CYBER-CRIME: MEANING AND NATURE

There is no exhaustive definition of cybercrime; however, it can be defined as an offence that is committed on or with the help of computer or internet. The only weapon used by the cyber criminals in the commission of cybercrime is technology and its knowledge therefore, the persons who are technically skilled in the field of computer and internet mostly commit it. Crime is a threat to worlds socio-economic, political and security system.[1]

Cyber crime contains all criminal offences, which are committed with the aid of communication devices in a network. This can be for example the internet, the telephone line or the mobile network.[2]

According to Pavan Duggal, *"cybercrime is species and the conventional crime is genus, where the computer is either an object or a subject of the cyber-criminal activities".* Any criminal who uses computer in furtherance of crime as either a target or a means comes within the ambit of cybercrime.

As regard to the ideal definition of the term cybercrime the Information Technology Act, 2000 is silent. However, the general definition of cybercrime may be *"an unlawful act wherein the computer is either a tool or a target or both".*[3] Thus, any criminal activity carried out with the help of computer or internet to harm computer system or person or property or reputation or government or society falls within the ambit of cybercrime.

Prof. S.T. Vishwanath has defined cybercrime in three different ways:

"a) Any illegal action in which a computer is the tool or object of the crime i.e., any crime, the means or purpose of which is to influence the function of a computer,

b) Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made a gain,

c) *Computer abuse is considered as any illegal, unethical or unauthorized behavior relating to the automatic processing and transmission of data."*[4]

The U.N. Congress on Prevention of Cybercrime and Treatment of Offenders[5] defined Cybercrime as follows:

1. In narrow sense, cybercrime connotes a computer crime, which includes any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

2. In broader sense, cybercrime includes all computer related crimes and consists of any illegal behavior committed by means of or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[6]

In the Indian framework, cybercrime is a willful and voluntary act or omission that adversely affects a property or person or computer system, which is made punishable by the Information Technology Act, 2000.

---

[1]D. Thomas & B. D. Loader ed, *Cyber Crime Law Enforcement, Security and Surveillance in the Information Age* 3 (2000).

[2] http://wikipedia.org/wiki/cybercrime

[3]R. Nagpal – what is cybercrime?

[4]S.T. Viswanathan, The Indian Cyber Laws with Cyber Glossary 81 (2001).

[5]Tenth UN Congress on Prevention of Crime & Treatment of Offenders was held in Vienna onApril 10-17, 2000.

[6] Ibid

As regard to the precise definition of cybercrime, the learned authorities hold the opinion that it is a misnomer because there is no universally recognized statutory definition. According to them there is no major difference between conventional crime and cybercrime because both include conduct whether act or omission, which causes breach of law and leads to punishment.

Provisions of Information Technology Act, 2000 Dealing with Cyber Crimes and Analysis of the Statistical Data of National Crime Records Bureau

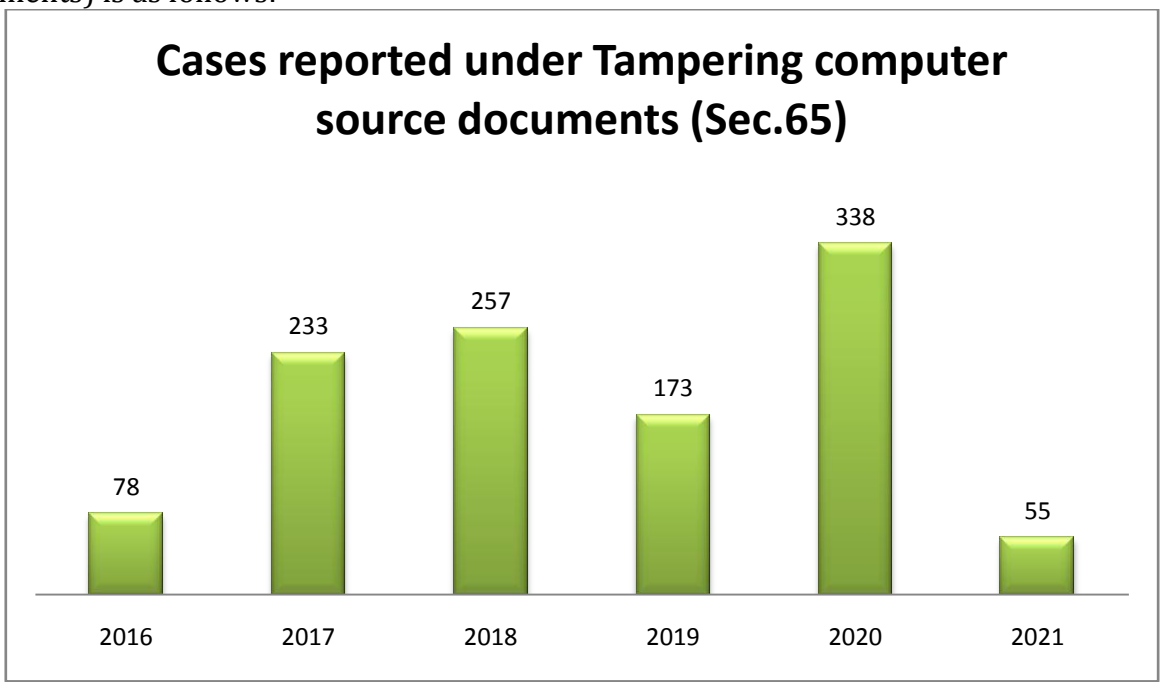
Chapter XI of the IT act, 2000 deals with offences. This part attempts to define various types of cyber-crimes in India and provide for punishment where computer may be a victim or is used as a tool or an object in the commission of a crime. Sections 65 to 78 provide for various offences that are committed by the accused against the individual, state and the society.

Certain offences are as follows:

- **Tampering with Computer Source Documents**

Section 65 states, "*if anyone through himself or through others, knowingly or intentionally, alters, destroys or conceals, computer source code, when it's required to be kept or maintained by law, which is used in computer, computer programme, computer system or computer network, shall be punishable with imprisonment of up to 3 years or with fine up to two lakh rupees or both.*"[7]

As per the NCRB data, the number of cases reported under Sec.65 (tampering computer source documents) is as follows:



Graph No.1: Cases reported under Section 65 from year 2016 to 2021

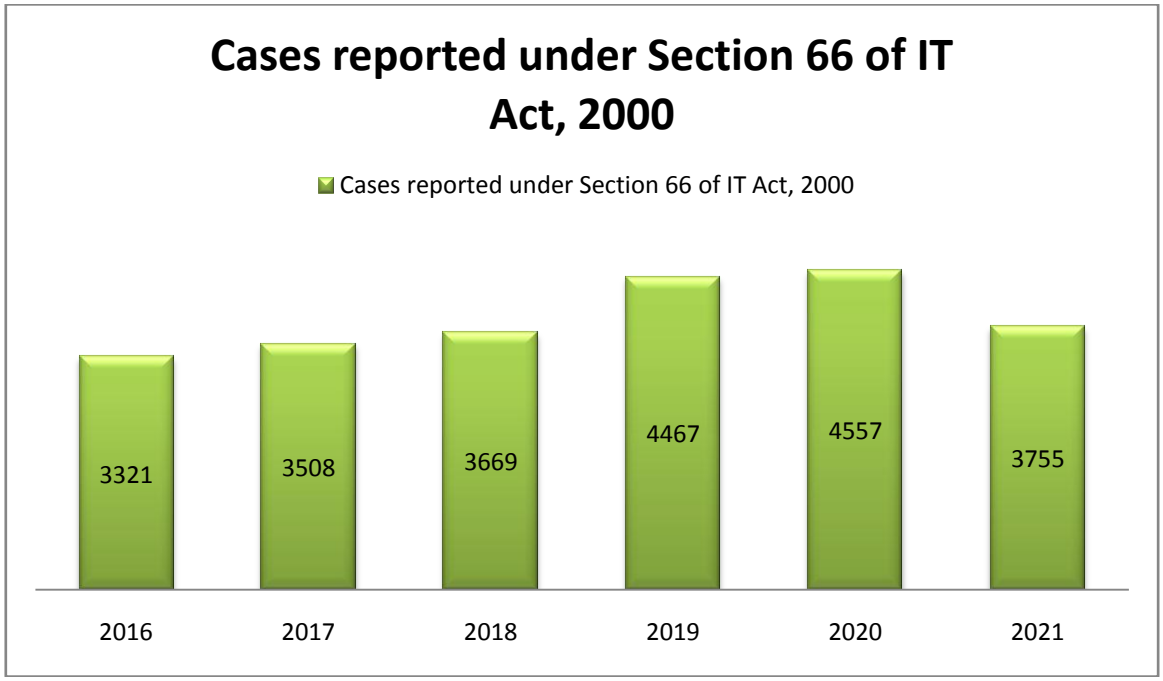
The above diagram shows that there has been a gradual growth from 2016 to 2018. However, there has been a decrease of around 32.68% of cases in the year 2019 as compared to 2018. But again in 2020, there has been an increase of about 95.37% of cases in the year of 2020 as compared to 2019. However, there has been decrease of around 83.72% of cases in the year of 2021 as compared to 2020.

- **Computer Related Offences**

[7] *Ibid*, Sec. 65

Section 66 states, "*if a person fraudulently and dishonestly does any of the acts stated under section 43, them he shall be punishable with imprisonment of up to 3 years or with fine up to five lakh rupees or both*."[8]

As per the NCRB data, the number of cases reported under Sec.66 (Computer Related Offences) is as follows:



Graph No.2: Cases reported under Section 66 from year 2016 to 2021

The above diagram shows that in the last five years there has been a gradual increase in cyber-crimes reported for computer related offences. But in 2021, there has been a decrease of around 17.59 % as compared to 2020.

- **Sending Offensive Messages through Communication Service**

It is to be noted that section 66A has been struck down by the Supreme Court of India, in the Shreya Singhal v. Union of India[9]case.

However, the provision as it stood before was as follows, that is, "*if any person sends information which is grossly offensive or has menacing character, or, where he knows that the information is false but to cause annoyance, inconvenience, danger, obstruction, insult, enmity, hatred, injury, ill will or criminal intimidation, uses computer resource or computer device; or where he sends electronic mail or a message through electronic mail, with the intent to cause annoyance or inconvenience, or to deceive or mislead as to its origin, to the addressee or recipient".*

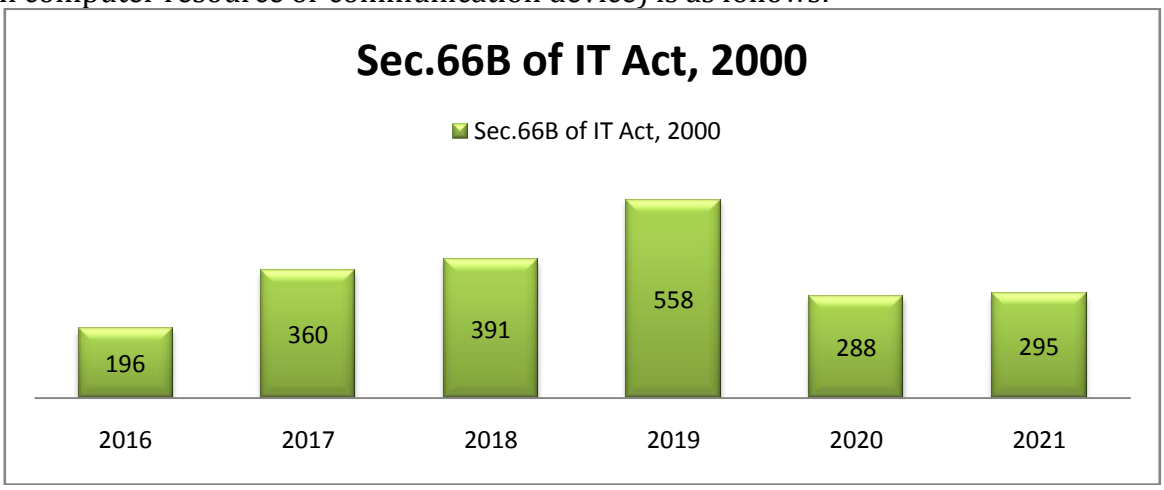
For these offences, the accused shall be punishable with imprisonment of up to 3 years and with fine.

- **Receiving Stolen Computer Resource or Communication Device**

Section 66B states, *"if anyone dishonestly receives or retains computer resource or communication device, knowingly or having reason to believe that its stolen, shall be punishable with imprisonment of up to 3 years or with fine up to rupees one lakh or with both."*[10]

[8]*Ibid*, § 66.
[9]Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[10]Information Technology Act, 2000,§66BNo. 21, Act of Parliament, 2000 (India).

As per the NCRB data, the number of cases reported under Sec.66B (dishonestly receiving stolen computer resource or communication device) is as follows:



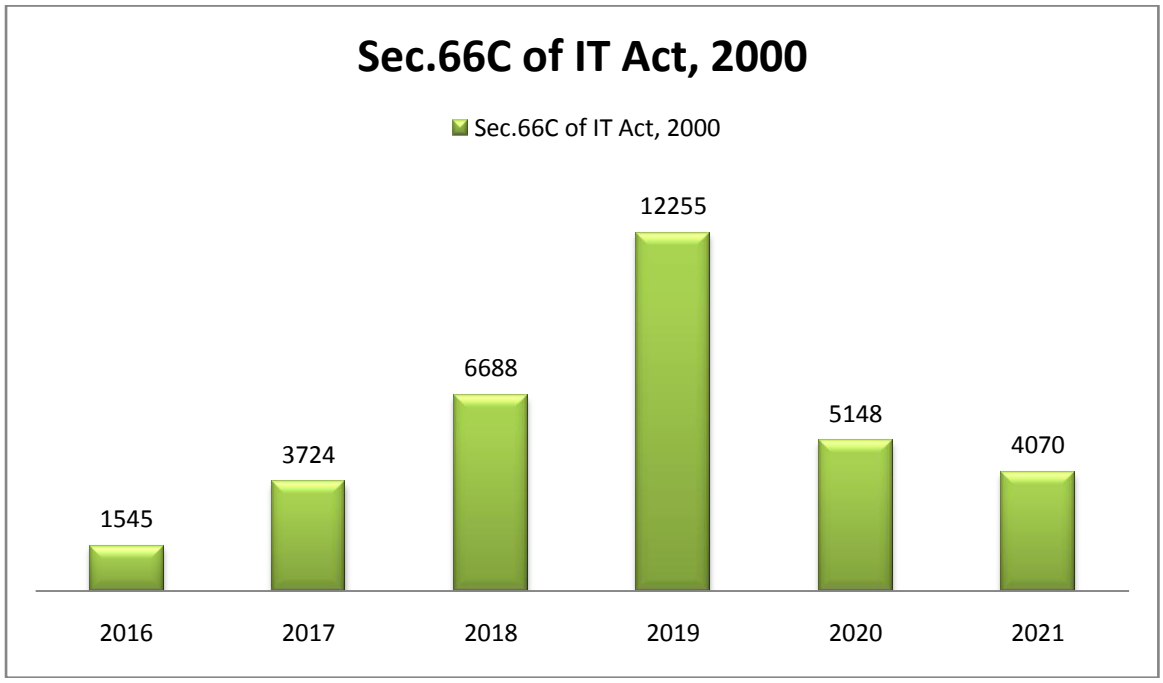
Graph No.3: Cases reported under Section 66B from year 2016 to 2021

The above diagram shows a gradual increase under section 66B. In the year 2019 there has been an increase of 43% of crimes being reported in India. It is to be also noted that there has been a gradual increase cases reported from 2016 to 2019. But in 2020, there is a decrease of 48.28% as compared to 2019. There has been a slight increase in the cases reported around 2.43% in 2021.

- **Identity Theft**

Section 66C states, "*whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, he shall be punishable with imprisonment of up to 3 years and with fine up to rupees one lakh*."[11]

As per the NCRB data, the number of cases reported under Sec.66C (Identity Theft) is as follows:

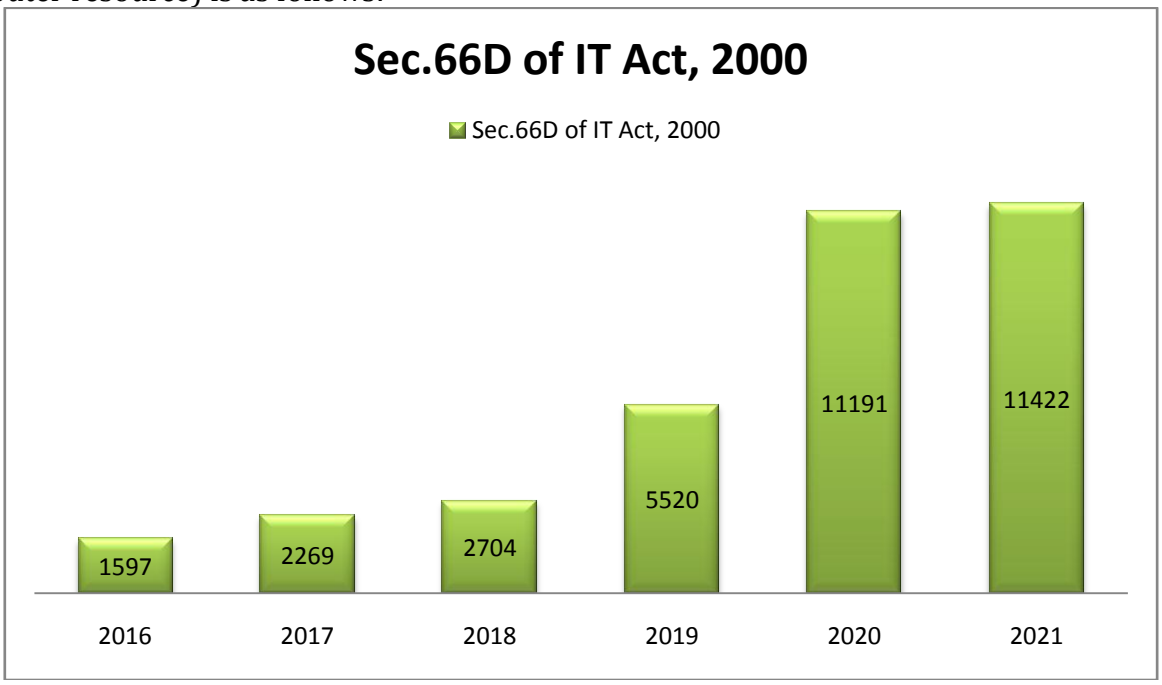


[11] *Ibid*, § 66C

Graph No.4: Cases reported under Section 66C from year 2016 to 2021
The above diagram shows that the highest number of cases got booked under section 66C for identity theft in India. Over the period of year, we see a very high rate of increase in number of crimes being reported, in the year 2017, there was a 141% increase, in 2018 there was 79.59% increase and in the year 2019 there was 83.23% increase. But in 2020 there is decrease of about 57.99% as compared to 2019. Again in 2021, there is decrease of about 20.94% as compared to 2020.

- **Cheating by Personation**

Section 66D states, "if any person by means of a computer resource or communication device, cheats by personation, he shall be punishable with imprisonment of up to 3 years and with fine up to rupees one lakh."[12]
As per the NCRB data, the number of cases reportedSec.66D (Cheating by personation by using computer resource) is as follows:



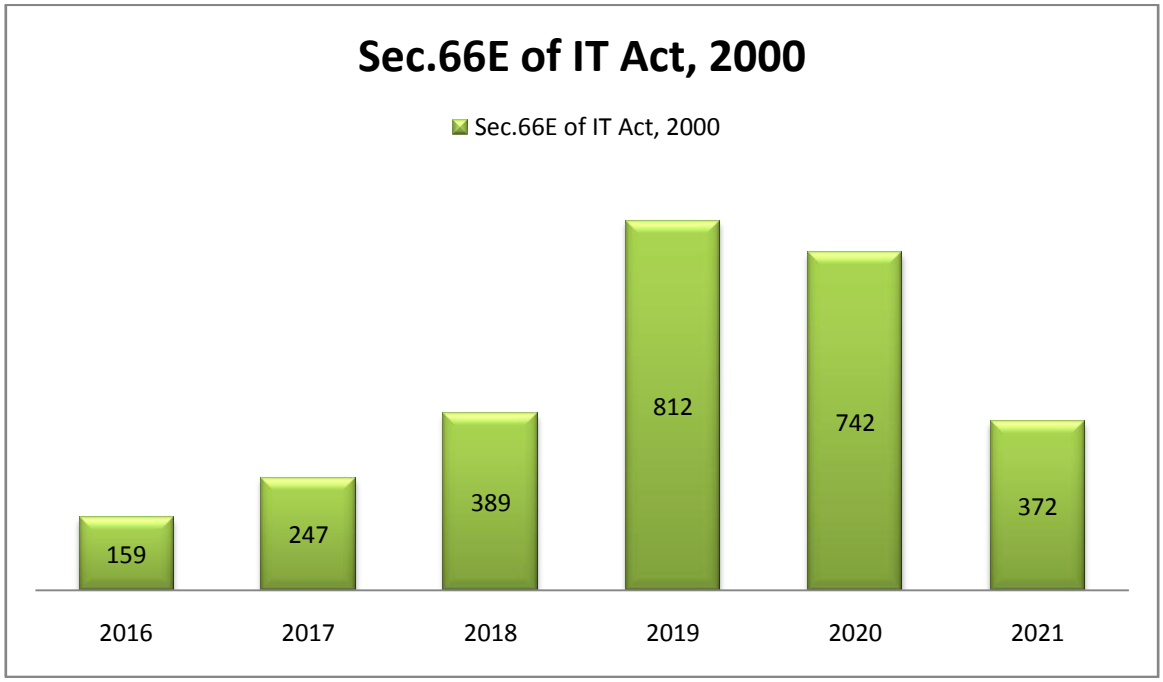
Graph No.5: Cases reported under Section 66D from year 2016 to 2021
The above diagram shows that for Cheating by personation by using computer resource under Section 66D. There was a gradual increase in crimes reported till 2018; however in the year 2019, there has been significant jump around 104%. In 2020 there is an increase of 50.67% as compared to 2019. There has been a slight increase about 2.06 % in 2021 as compared to 2020.This shows that cybercrimes with the intent to commit fraud has increased tremendously.

- **Violation of Privacy**

Section 66E states, "*whoever, knowingly or intentionally captures, publishes or transmits the image of a private area of any person without his or her consent, where such circumstances violate the privacy of that person, he shall be punishable with imprisonment of up to 3 years or with fine up to rupees two lakh or with both*."[13]

[12]*Ibid*, § 66D.
[13]*Ibid*, §66E.

As per the NCRB data, the number of cases reported under Sec.66E (violation of privacy) is as follows:



Graph No.6: Cases reported under Section 66E from year 2016 to 2021

For the violation of privacy, from 2016 to 2018, there was a gradual increase, however in the year 2019 we see a jump in cases reported under section 66E, with an increase of 108% over the cases reported in 2018. But there is a decrease of 8.62% as compared to 2019. Again in 2021, a decrease of 49.86% as compared to 2020.

- **Cyber Terrorism**

"*A person is said to have committed the offence of cyber terrorism under section66F if he performs the following acts:*

a) "With the intent to threaten the unity, integrity, security of sovereignty of India or to strike terror in the people or any section of the people does the following acts such as:

i. denying or cause the denial of access to a person who is authorised to access such computer resource; or

ii. attempts to penetrate or access a computer resource to which he has no authorisation or exceeding authorised access; or

iii. introducing or causing to introduce any computer contaminant, due to which it is likely to cause death or injuries to persons; or cause damage or destruction to the property, or disrupts or knowing does so to cause damage or disruption to supplies or services essential to the life of the community; or affect the critical information infrastructure stated under section 70";

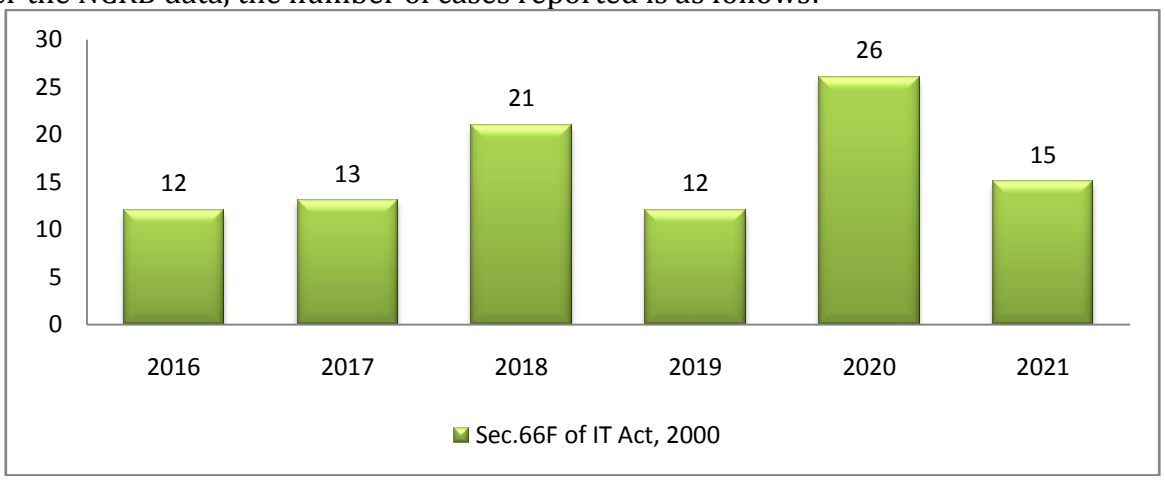
b) If

i. "knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons for the security of the State or foreign relations, or

ii. any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause of likely to cause injury to the interests of the sovereignty and integrity Of India, the security of the State, friendly

relations with foreign States, public order, decency or morality, or in relation to contempt of Court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise"; is said to have committed the offence of cyber terrorism and where he commits or conspires to commit such act, he shall be punishable with imprisonment up to life imprisonment."[14]

As per the NCRB data, the number of cases reported is as follows:



Graph No.7: Cases reported under Section 66F from year 2016 to 2021

Cyber terrorism is the worst form of crime that could be committed in the present times, using technology. The above diagram is not a good sign for any nation to book cases of cyber terrorism. In the last six years there has been on an average 17 cases reported, with the highest number of cases reported in the year 2020.

- **Publishing or Transmitting Obscene Material in Electronic Form**

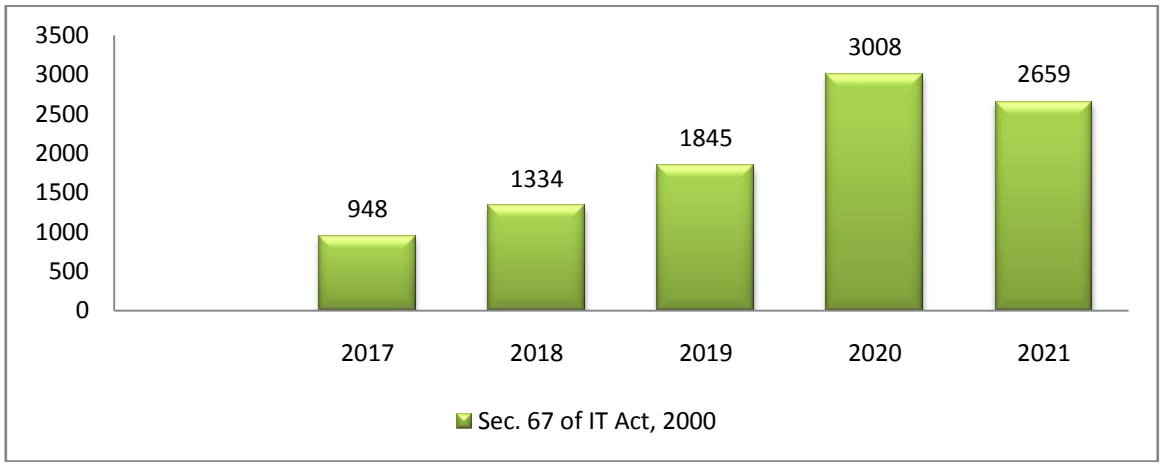
Section 67 states, "*if anyone publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it then; in case of the first conviction, he shall be punished with imprisonment up to three years and fine up to five lakh rupees. In case of second or subsequent conviction, he shall be punished with imprisonment up to five years and fine up to ten lakh rupees.*"[15]

The section is gender-neutral recognising that online harassment can victimise any gender. Nonetheless, Section 67 is the primary provision that is applied in maximum cases of cyber crimes against women along with Section 66 E which penalises violation of privacy. Now the sheer range and volume of cybercrimes targeting women have multiplied. In light of these facts, we shall determine whether the Section is adequate to cater to the evolving character of cybercrimes in the global era. We shall also discuss if its application is serving the originally intended purpose or has it gone awry.

As per the NCRB data, the number of cases reported under Sec. 67 (publishing or transmitting obscene material in electronic form) is as follows:

[14] *Ibid*, § 66F.

[15] *Ibid*, §67.



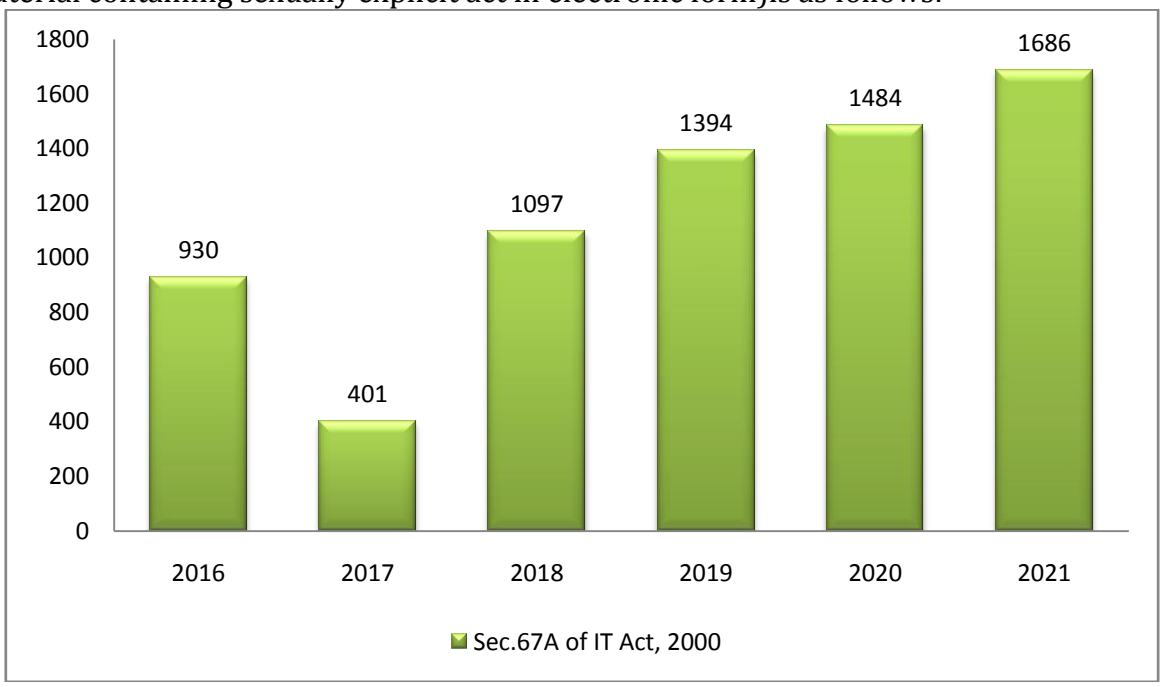
Graph No.8: Cases reported under Section 67 from year 2016 to 2021

The above diagram shows that for publishing or transmitting obscene material in Electronic Form, the cases reported have gradually increased. An increase of 63% has been seen in the year 2020 in cases reported. However, in 2021 we seen the decrease around 11.6% as compared to 2020.

- **Publishing or Transmitting of Material Containing Sexually Explicit Act, Etc. in Electronic Form**

Under section 67A for the said act, "*if anyone publishes or transmits materials which contain any sexually explicit act then the said person shall be punished; in case of the first conviction, he shall be punished with imprisonment up to five years and fine up to ten lakh rupees. In case of second or subsequent conviction, he shall be punished with imprisonment up to seven years and fine up to ten lakh rupees.*"[16]

As per the NCRB data, the number of cases reported under Sec.67A (publishing or transmitting of material containing sexually explicit act in electronic form)is as follows:

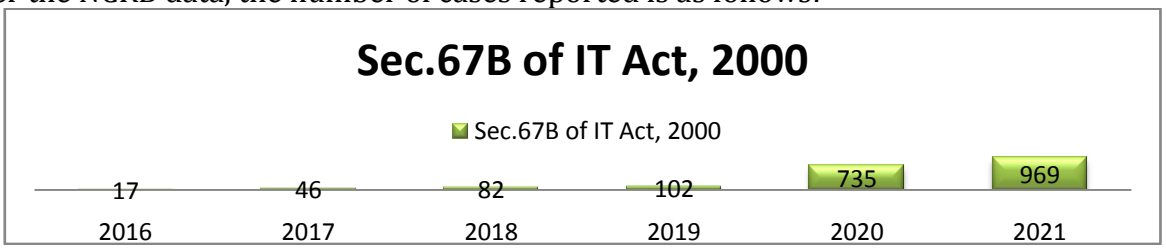


[16]*Ibid*, §67A

Graph No.9: Cases reported under Section 67A from year 2016 to 2021
The above diagram shows that under section 67A there has been increase in crimes reported in the last five year from 2016 to 2019. There has been an increase of 6.45% of cases reported in 2020 as compared to 2019 and 13.6% increase in 2021 as compared to 2020.

- **Publishing or Transmitting of Material Depicting Children in Sexually Explicit Act, Etc. in Electronic Form**

Section 67 B states that "*anyone who:*
a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or
b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or
c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
d) facilitates abusing children online, or
e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished; in case of the first conviction, he shall be punished with imprisonment up to five years and fine up to ten lakh rupees. In case of second or subsequent conviction, he shall be punished with imprisonment up to seven years and fine up to ten lakh rupees."[17]
As per the NCRB data, the number of cases reported is as follows:



Graph No.10 Cases reported under Section 67B from year 2016 to 2021
The above diagram shows that there has been a gradual increase in crimes reported under section 67B over the last five years. There is an increase of 620% in 2020 as compared to 2019 and 31.8% increase in 2021 as compared to 2020.

- **Preservation And Retention of Information by Intermediaries**

Section 67C states that "*the intermediaries are required to retain the information for such duration, manner and format as prescribed by the central government, and if they intentionally or knowingly contravene this provision, then it shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both.*"[18]

- **Directions of Controller**

Section 68 states, "*if certifying authority or by its employees, knowingly or intentionally, fails to follow the orders of the controller, in compliance of the provisions of the Act or rules or regulations, then it shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both.*"[19]

[17] *Ibid*, § 67B.
[18] *Ibid*, § 67C.
[19] *Ibid*, § 68.

- **Interception or Monitoring or Decryption of Any Information Through Any Computer Resource**

Section 69 states that "*the appropriate government can intercept monitor or decrypt any information generated, transmitted, received or stored in any computer resource.*
This can be done in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence. And in doing so the subscriber or intermediaries shall extend all facilities and technical assistance to the agency, failing to do so, they shall be punishable with imprisonment of up to seven years and liable for fine."[20]

- **Blocking for public Access of Any Information**

Section 69A states that "*the central government or its officers can direct the agency of government or intermediaries to: block the access to the public any information generated, transmitted, received, stored or hosted in any computer resource. This act would be necessary in the interest of the sovereignty or integrity of India, defence of India, and security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence. In case the intermediary fails to do so, they shall be punishable with imprisonment of up to seven years and liable for fine*."[21]

- **Monitor and Collect Traffic Data or Information**

Section 69B states that "*the central government in order to enhance cyber security and to identify, analyse and prevent the intrusion of or spread of computer contaminant in the country; Authorise the agency to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource; In such case the intermediary shall provide all the technical assistance and facilities, fails to do so intentionally or knowingly contravenes, they shall be punishable with imprisonment of up to three years and liable for fine.*"[22]

- **Protected System**

Section 70 provides that "*appropriate government may declare by notification, that the computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system. Thus, if any person gains or attempts to gain access to a protected system in contravention of this provision, they shall be punishable with imprisonment of up to ten years and liable for fine*."[23]

- **Misrepresentation**

Section 71 states that "*if anyone makes any misrepresentation or suppresses any fact to the controller or the certifying authority, in regard to licence or an electronic signature certificate, they shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both.*"[24]

- **Breach of Confidentiality and Privacy**

Section 72 states that "*if a person authorized under this act, secures access without the consent of the person concerned, and discloses any electronic record, book, register, correspondence, information, document or other material, such person shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both.*"[25]

---

[20]*Ibid*, § 69.
[21]*Ibid*, § 69A.
[22]*Ibid*, §69B.
[23]*Ibid*, §70.
[24]*Ibid*, §71.
[25]*Ibid*, §72.

- **Disclosure of Information in Breach of Lawful Contract**

Section 72A provides that "*if any person, including the intermediary when they are providing service under a contract, gain access to material containing personal information about another person, and without the consent of such person, discloses such information, with intent or knowingly, which would cause wrongful loss or gain, shall be punishable with imprisonment of up to three years or with fine up to rupees five lakh or with both*."[26]

- **Publishing Electronic Signature Certificate**

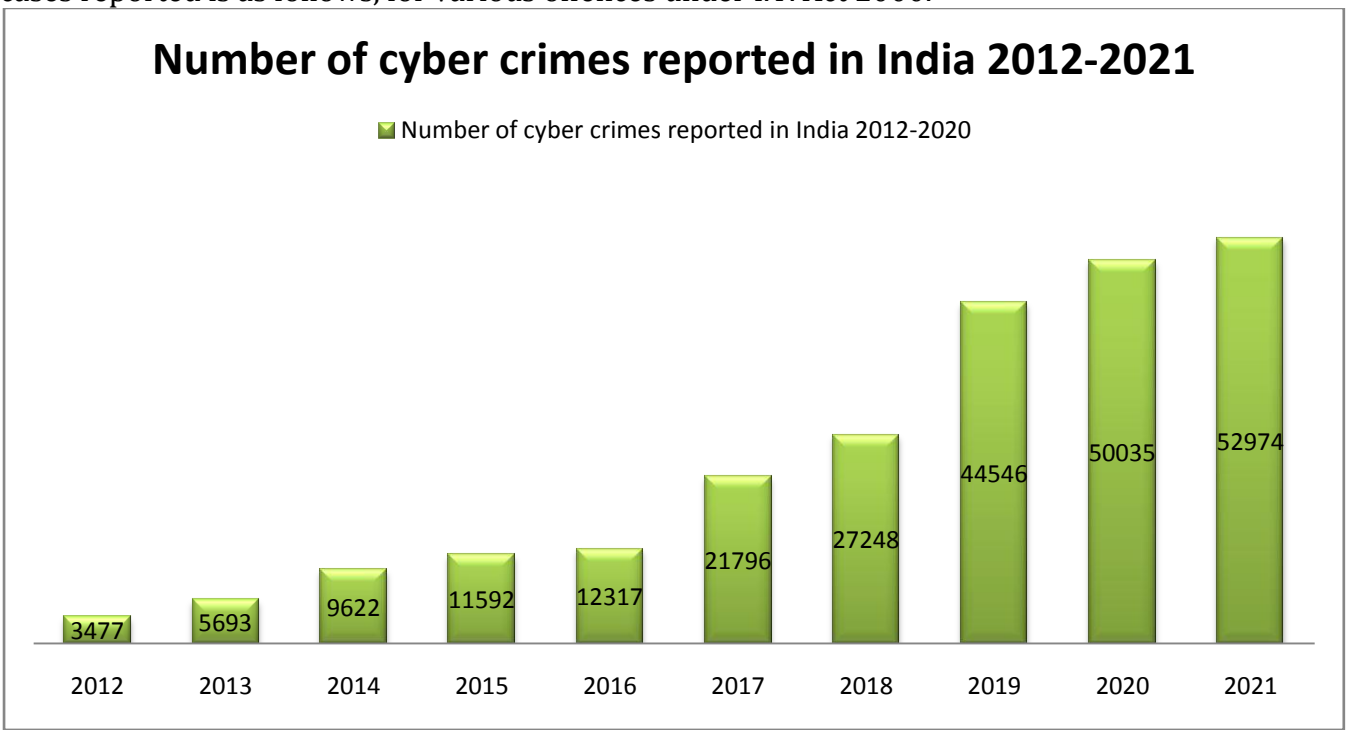
Under section 73, "*if a person publishes or makes available Electronic Signature Certificate to another person, when the certifying authority has not issued it; or the subscriber has not accepted it; or if it has been revoked or suspended; shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both*."[27]

- **Publication for Fraudulent Purpose**

Section 74 states that "*if anyone knowingly, for fraudulent or unlawful purpose, creates, publishes or makes an Electronic Signature Certificate available, shall be punishable with imprisonment of up to two years or with fine up to rupees one lakh or with both*."[28]

Total Number of Cyber Crimes Cases Reported in India from 2012-2021

The above stated provisions are seen as the main provisions to prevent and control different forms of cyber-crimes and the diagram below highlights that over the last few years there has been a steady increase in cyber-crimes in India. As per the NCRB data,[29] the total number of cases reported is as follows, for various offences under I.T. Act 2000.



Graph no.11 Total number of cybercrimes case reported in India from 2012-2021

In India, there was a drastic increase in registered cybercrimes in 2021 compared to the

[26]*Ibid*, § 72A.
[27]*Ibid*, § 73.
[28]*Ibid*, § 74
[29]Crime In India | National Crime Records Bureau, https://ncrb.gov.in/en/crime-india (last visited July 29, 2022).

previous year. 52,974 cybercrime cases were reported in that year, a considerable rise from the roughly 3477cases in 2012.

- With almost ten thousand incidents reported to the authorities, Telangana State had the highest number of recorded cybercrimes in 2021 compared to the rest of the States.
- Uttar Pradesh (8829), Karnataka (8136) and Maharashtra (5562) positioned second, third and fourth respectively in registered cybercrime cases.
- In Union Territory, Delhi has the highest number of cybercrime cases.
- The preponderance of these incidents was registered under the IT Act with the motive to fraud (32230) or sexual exploitation.
- The rate of total cybercrime rate in 2021 is 3.9.
- Telangana has the highest rate of cybercrime around 27% in 2021.

CONCLUSION

India, which has the second-largest internet user population in the world, was also a part of the expanding digital village. While increased web connectivity offers widespread advancement, it also exposes our digital societies to new threats. Cybercrimes are transnational and have developed at a rate equal to that of new technologies. Every year, a considerable increase is seen in the number of cybercrimes that are reported nationwide. The types of offences, however, ranged from minor online frauds to lottery scams and sexual harassment. However, the banking and financial industry appears to be the one that is most targeted. With the advent of the corona virus pandemic and the shift of most services online, there is a significant risk in other industries as well. Not only the law is for people but people also for the law. Prevention is better than cure. The lack of awareness of cyber hygiene has been one of the main obstacles to reducing cybercrime. First, we need to know our enemy without knowing the enemy we cannot combat it. Thus, people require to know and vigilant about the cyber space the crime related to it. It is also require that when crimes were reported to the police, the system and procedure should handle such cases effectively.

REFEERENCES

Manish Kumar Chaubey, *Cyber Crime and Legal Measures* (Regal Publications, New Delhi, 2013)
Justice Yatindra Singh, *Cyber Laws* (Universal Law Publications, New Delhi, 5th ed. 2012)
Harish Chander, *Cyber laws and IT Protection* (PHI Learning Private Limited, New Delhi, 2013)
R.P. Kataria, S.K.P., *Cyber Crimes Law Practice and Procedure* (Orient Publishing Company, Allahabad, 1st ed.)
D. Thomas & B. D. Loader, *Cyber Crime Law Enforcement, Security and Surveillance in the Information Age* (Routlege Tylor and Francis Group, London and Newyork, 1st ed. 2000).
R. Nagpal, *What is cybercrime?*
S.T. Viswanathan, *The Indian Cyber Laws with Cyber Glossary*: (Bharat Law House, New Delhi 2nd ed. 2001).
Tenth UN Congress on Prevention of Crime & Treatment of Offenders *available at,*https://digitallibrary.un.org/record/404748?ln=en(last visited on 25 November 2022)
http://wikipedia.org/wiki/cybercrime (last visited on 25 November 2022)
Information Technology Act, 2000
Reports of National Crime Records Bureau