Annals of Justice and Humanity (AJH)
Vol 1, No 1, 2021, 39-49 https://doi.org/10.35912/ajh.v1i1.1389

A study on issues and challenges of information technology act 2000 in India

Srinivasa Rao Dokku[1], Deenamma Kandula[2]
Siddhartha Institute of Technology, India[1], Velagapudi Durgamba Siddhartha Law College, India[2]
srinu_dokku@yahoo.co.in[1], kanduladeenamma@gmail.com[2]

Article History
Received on 13 December 2022
1st Revision on 3 January 2023
2nd Revision on 6 January 2023
3rd Revision on 9 January 2023
4th Revision on 11 January 2023
5th Revision on 12 January 2023
Accepted on 16 January 2023

Abstract
Purpose: This article focused on the jurisprudence of cyber law, how cybercrime is categorized in relation to regular crime, and the jurisdictional problems it raises. In India, the Information and Technology Act of 2000 primarily governs cybercrime. The Information and Technology Act of 2000's implementation problems and difficulties are also identified in this study.
Research Methodology: The study's objectives were to understand the many cybercrimes that occur in India as well as the problems and obstacles related to them. The study is based on secondary data, and it analyses and interprets data from the last three years. The primary information was gathered through press publications, crime bureaus of investigation, etc.
Results: In the past three years, the nation has reported over 16 lakh cybercrime incidences, and more than 32,000 FIRs have been filed in India since 2020. 8,829 instances were reported in Uttar Pradesh in 2021, down from 11,097 in 2020. Karnataka saw a decrease in instances from 10,741 in 2020 to 8,136 in 2021. 10,730 cybercrimes against women were reported in India in 2021. Out of this, the majority of instances were related to disseminating obscene sexual content or cyberpornography. 1,896 similar instances were reported in 2021.
Limitations: This study is based on secondary information only. The data was collected from only secondary sources and from the last three years only
Contribution: The policymakers, educators, and the general public will benefit from this study's explanation of cybercrimes in India. Additionally, it draws attention to the difficulties with the 2010 Indian Information Act.
Keywords: *Cyber crime, Cyber space, Jurisdiction, Issues, Challenges*
How to Cite: Dokku, S. R., & Kandula, D. (2021). A study on issues and challenges of information technology act 2000 in India. *Annals of Justice and Humanity*, 1(1), 39-49.

1. Introduction

India has one of the youngest populations in the world, with an average age of just 29 years. Ages 0 to 14 make up more than a quarter of the population (25.78%). Sixty-two. 5%, or nearly another third, are between the ages of 15 and 59. Although this helps India's economy thrive, the nation's big and young population is also vulnerable to digital influences.

Generation X and Millennials, who range in age from 39 to 54, are investigating the advantages and potential of the digital age. Thanks to the digital revolution, people, companies, and the government now have access to opportunities that were previously unthinkable (Das & Nayak, 2013). The need of educating "Generation Z" (7–22 years old) and future generations to prevent them from being vulnerable because they lack the maturity of Millennials and Gen X gets lost in this enthusiasm (Hudalil, 2022). The next concern is whether the elder generation as a whole is completely aware of the risks associated with the digital world and cyberspace (Poonia, 2014).

There is probably an urgent need to evaluate millennial and Generation X's knowledge of cyber awareness and safety. We, as cyber aficionados, need to take the initiative on this path. Finding "Influencers" and "Drivers of the Influencers" is crucial to this education (Amiri, Khademi, Khafri, Akbari, & Jangjoo, 2022). For instance, the government influences and motivates businesses (Sushanth, 2013). Corporations play a key role in influencing customers. The legal system is what motivates Indians to fight for their rights (Majesty, 2010).

Cybercrime could be defined broadly as "unlawful acts in which the computer is either a tool or a target, or both." In the context of cybercrime, a cybercriminal is someone who commits an illegal act with the intent to commit a crime (Hajgude & Deshmukh, 2020). Cybercriminals include motivated criminals, organized hackers, disgruntled employees, and cyber terrorists (Rosadi & Barus, 2022). Cybercrime can range from non-delivery of goods or services and computer intrusions (hacking) to infringements on intellectual property rights, economic espionage (theft of trade secrets), online extortion, international money laundering, identity theft, and a long list of other Internet-facilitated crimes (Swaathi & Kannappan, 2018). Furthermore, it is difficult to identify the crime method and answer questions such as where and when it was committed (A. F. Anoke, Onu, & Agagbo, 2022). The Internet's anonymity makes it an ideal channel and tool for many organized crime activities (F. Anoke, Ngozi, Uchechukwu, & Joyce, 2022).

2. Literature Review

Between January and June of this year, more than 6.7 lakh cyber security incidents in India were recorded. Ajay Kumar Mishra, a minister for the Union, briefed Parliament. All of this happened in spite of the government's continued efforts to improve the system for fighting cybercrime. In India, more than a million of these instances were reported between January 2019 and June 2022. The Department of Supervision at the RBI reports that 13,951 fraud instances totaling Rs 76.49 crore with a loss of Rs 25.77 crore were reported in 2021–22. While these three numbers only totaled 9,675, 57.06 crore, and 22.88 crore in 2020–21, respectively, there were 39,134 fraud instances the year before, resulting in losses totaling Rs 85.26 crore and Rs 31.27 crore. The state with the highest instances in 2021–2022 in Tamil Nadu (4,866), followed by Maharashtra (2,443) and Delhi (1,402) (Sarmah, Sarmah, & Baruah, 2017).

According to the most recent "Crime in India" report, there were 3477 cases of cybercrime reported in India in 2022, although 52,974 cases were reported in 2020. According to official data, the number of cybercrime events in India has been rapidly rising and increased by almost nine times between 2013 and 2020. According to the most recent "Crime in India" report, the number of cybercrimes registered in India climbed to 50,035 in 2020 from 5,693 in 2013. Additionally, according to CNN-analysis News18's statistics, the number of instances increased by nearly 85% between 2018 and 2020. India reported 27,248 cybercrime-related incidents in 2018. Additionally, there were 44,735 more instances reported in 2020 than there were in 2019 — a rise of about 12%. (table -1).

Over 60% (30,142 incidents) of the crimes reported in 2020 were committed with fraudulent intent, while just 7% were motivated by sexual exploitation and 5% by extortion. The statistics showed that while most states have reported an increase in cybercrimes in 2020, areas like Uttar Pradesh, Karnataka, Mizoram, Rajasthan, and Sikkim have seen a decrease in incidents compared to 2019. Sikkim is the only state in all of the states and union territories that had no cybercrime cases last year.

Table 1. Number of cybercrimes reported across India from 2012 to 2021

Year	Number of cyber crimes
2012	3,477
2013	5,693
2014	9,622
2015	11,592
2016	12,317

2017	21,796
2018	27,248
2019	44,546
2020	50,035
2021	52,974

Source: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

2.1. Reasons behind the Cybercrime

There are many reasons why cyber-criminals are doing cyber-crime (Kalra, 2017); chief among them are mentioned below:

a. For the sake of recognition.
b. For the sake of quick money.
c. To fight a cause one thinks he believes in.
d. The ow marginal cost of online activity due to global reach.
e. Catching by law and enforcement agencies is less effective and more expensive.
f. New opportunity to do legal acts using technical architecture.
g. Official investigation and criminal prosecution are rare.
h. No concrete regulatory measure.
i. Lack of reporting and standards
j. Difficulty in identification
k. Limited media coverage.
l. Corporate cyber crimes are done collectively and not by individual persons

2.2 Types of Cybercrime

As previously stated, cybercrime differs from traditional crime. Cybercrime, like traditional crime, comes in a variety of forms (Joshi & Singh, 2013). Figure 1 depicts some of the types of cybercrime that have evolved as a result of the invention of new techniques (Arya, 2019).

2.3 State-wise cybercrimes in India

The state of Uttar Pradesh reported 11,097 cybercrime cases in 2020, followed by the state of Karnataka with 10,741 incidents. The data showed that Telangana (5,024 cases) and Maharashtra (5,496 cases) were the following states. Arunachal Pradesh (from 7 to 30), Assam (2,231 to 3,530), Chhattisgarh (175 to 297), Goa (15 to 40), Gujarat (784 to 1,283), Manipur (4 to 79), and Telangana were the states that saw a significant increase in the number of cybercrimes between 2019 and 2020. (2,691 to 5,024).

Additionally, states, including Bihar, reported a sharp increase in cybercrimes in 2018 compared to 2017. Since 2018, the number of cybercrime cases has more than quadrupled in Bihar and Telangana, and grown by more than 75% in Uttar Pradesh. Since 2018, the number of cases has more than doubled in Odisha, West Bengal, Karnataka, and Chhattisgarh, while it has tripled in Tamil Nadu and Manipur (Singh, 2021).

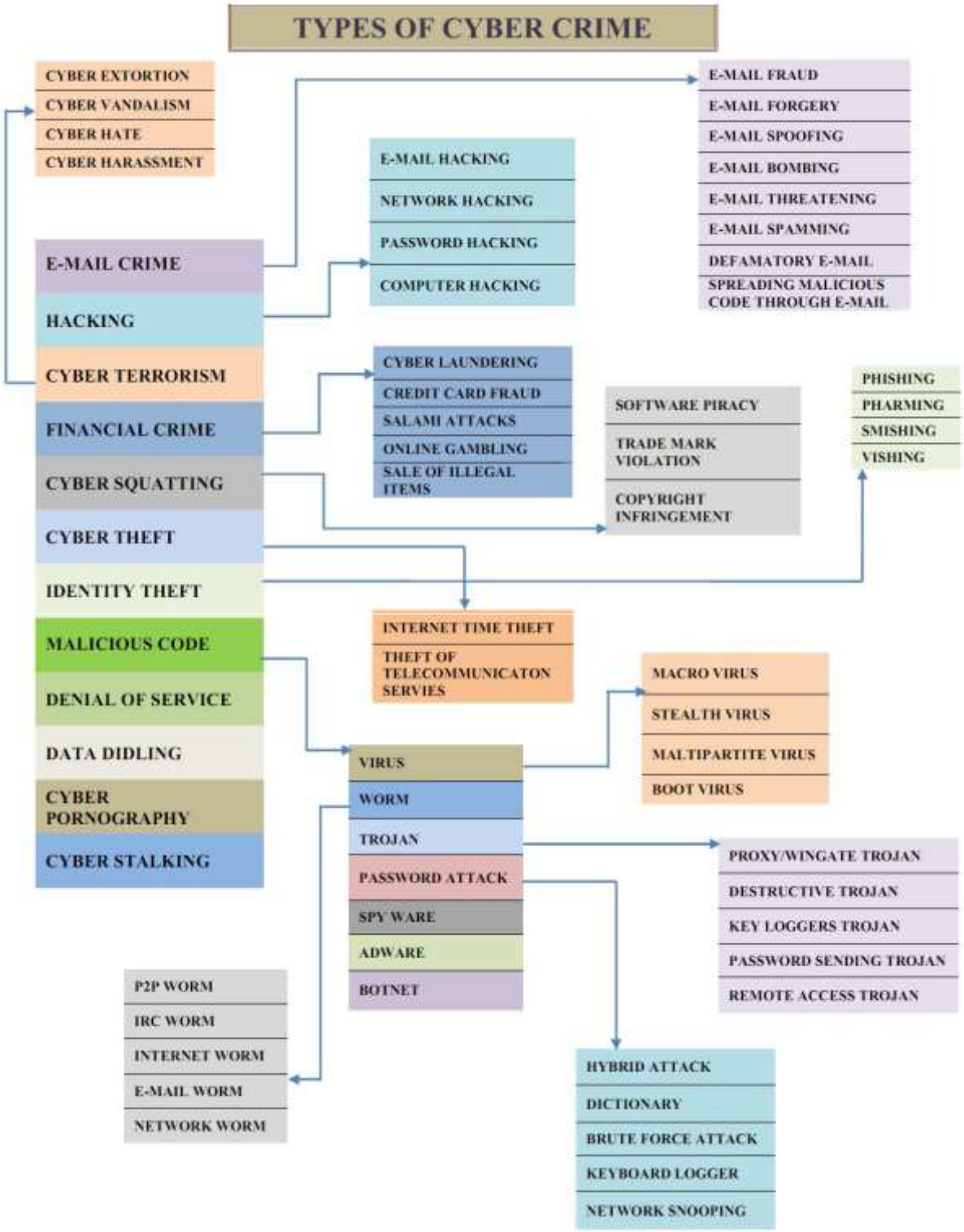

Figure 1. Types of Cybercrime

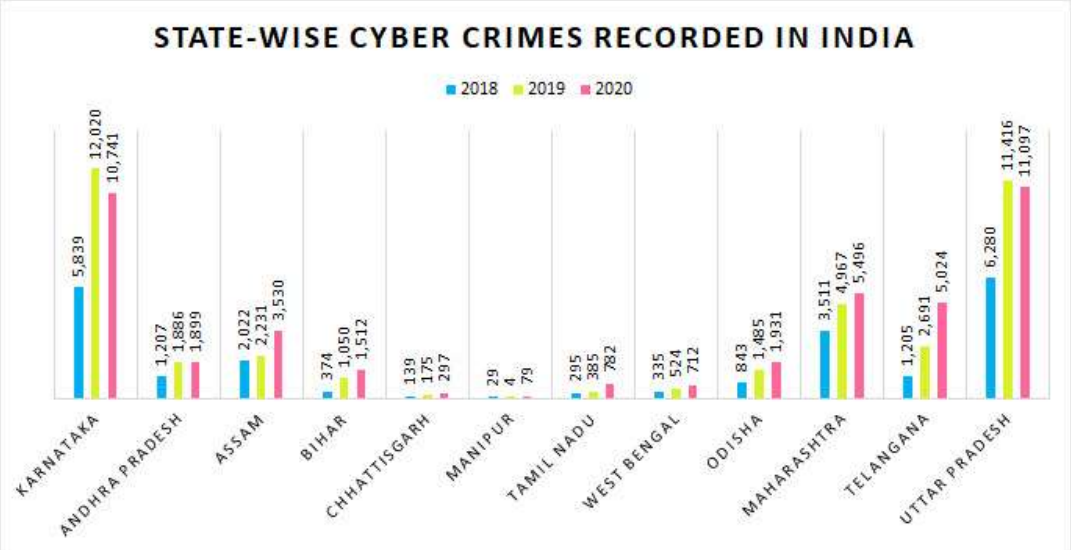

Figure 2. Cybercrimes recorded in India

In 2020, there would be 3.7 cybercrimes for every 1 lakh people, up from 3.3 in 2019. This is 0.9 for union territories and 3.8 for states. Karnataka (16.2), Telangana (13.4), Assam (10.1), Uttar Pradesh (4.8), Meghalaya (4.4), Maharashtra (4.4), and Odisha recorded the highest rates of cybercrime in 2020. (4.2).

2.4. Top Cities which record highest cybercrimes in India

The number in Hyderabad, which came in second on the list, increased from 2,553 in 2020 to 3,303 in 2021. The number of cases in Mumbai, the following city on the chart, increased to 2,833 in 2021 after declining the year prior. 2,433 such incidents were reported in Mumbai in 2020 and 2,527 in 2019. (Figure 3).

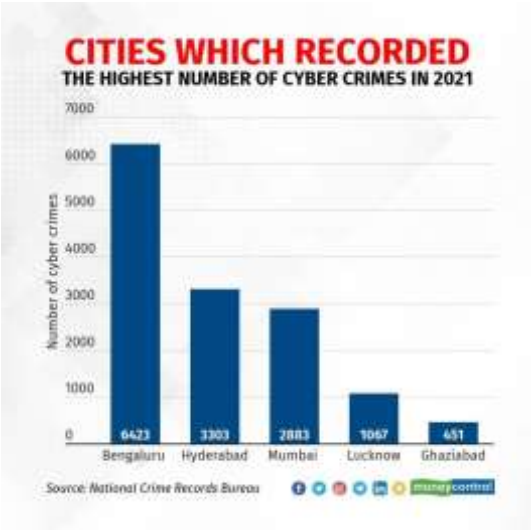

Figure 3. Cybercrime in India 2021

2.5. Motive for cybercrime in India

Nearly 61 percent of all cybercrime cases—32,230 cases—were committed with the intent to commit fraud (Poonia, 2014). Extortion, which was the third most frequent reason, was responsible for 5.4 percent (2,883 incidents), followed by sexual exploitation, which accounted for 8.6 percent (4,555 cases) (figure 3).

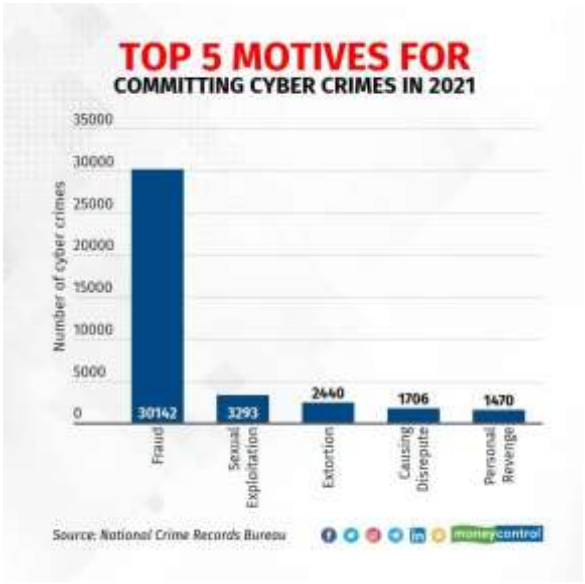

Figure 4. Top 5 motives for committing cybercrime

2.6. Cyber-crimes against women in India

10,730 cybercrimes against women were reported in India in 2021. Out of this, the majority of instances were related to disseminating obscene sexual content or cyberpornography. 1,896 similar instances were reported in 2021. With 2,243 incidents, Karnataka has the most instances of cybercrime against women. In 2021, the police pendency rate for cybercrime cases increased. At the end of 2020, 71.3 percent of all cases under investigation were still pending; in 2021, this percentage dropped to 56.4 percent.

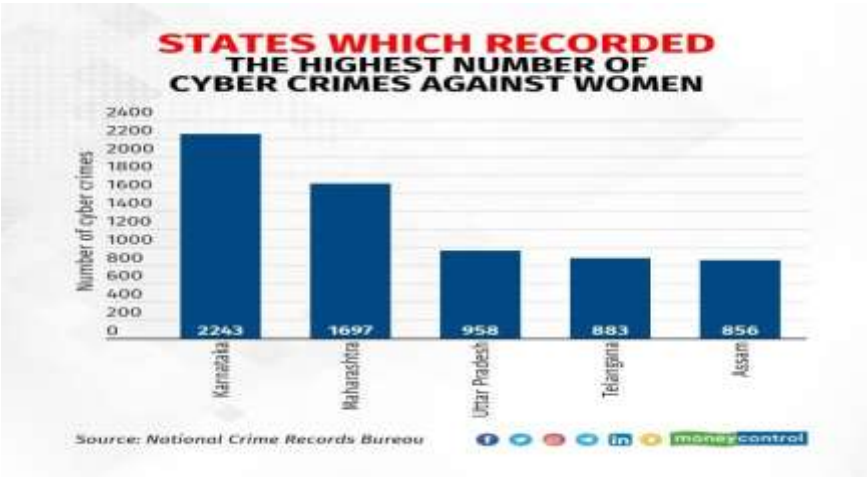

Figure 5. The highest number of cybercrimes against women

2.7 Current Indian legal framework against cyber-crime

The penal provisions against cyber-crimes in India are enumerated mainly within two statutes:

a. The Information Technology Act, 2000
b. Indian Penal Code of 1860.

The IT Act of 2000 provides protection against crimes such as email account hacking, credit card fraud, web defacement, virus introduction, phishing, email scams, source code theft, and theft of confidential information. Despite the fact that the IT Act does not specifically describe cyber crime, it does cover both cyber crime and cyber violations. The following are the main provisions relating to cyber crime and its penalties.

2.7.1 History of the IT Act in India

On October 17, 2000, the Information Technology Act of 2000 went into effect. This Act is applicable to all of India, and its provisions also apply to any violation or offense committed by any individual, regardless of nationality, even outside the Republic of India's territorial authority. Such an offense or contravention shall include a computer, computer system, or computer network located in India to be subject to the provisions of this Act. The extraterritorial applicability of the provisions of the IT Act 2000 is provided by Section 1(2) read in conjunction with Section 75. 90 Sections make up this Act.
The Information Technology Act of 2000 in India aims to incorporate legal ideas from earlier information technology laws passed in several other nations as well as various information technology law guidelines. The Act recognizes electronic signatures and grants legal legitimacy to electronic contracts. This is a current piece of legislation that makes crimes out of hacking, data theft, virus spreading, identity theft, defamation (sending abusive communications), child pornography, and cyberterrorism.

Rules for cyber cafés, electronic service delivery, data security, and website blocking are among the rules that supplement the Act. It also contains guidelines for the exercise of due care by internet service providers (ISPs), network service providers (NSPs), cyber cafés, etc. Any person impacted by data theft, hacking, or virus transmission may submit a criminal complaint as well as a claim for compensation with the Adjudicator appointed under Section 46. To the Cyber Appellate Tribunal is an appeal from the adjudicator.

2.7.2 Types of offenses and penalties under the IT Act 2000

1. Section 65 - Tampering with computer source documents: When the computer source code for a computer, computer program, computer system, or computer network is required to be stored or maintained by law for the time being in effect, it is unlawful for anyone to intentionally conceal, destroy, or alter it, or to cause someone to do so.
Penalty - Imprisonment up to three years, or/and with a fine up to RS 200,000.

2. Section 66 – Hacking with a computer system: Hacking occurs when someone destroys, deletes, modifies, reduces the value of, or otherwise negatively impacts information stored in a computer resource with the aim to cause or knowing that he is likely to cause unjustified loss or damage to the public.
Penalty - Imprisonment up to three years, or/and with a fine up to RS 500,000

3. Section 66B - Receiving stolen computer or communication device: A computer resource or communication device that is known to have been stolen or that the owner has cause to suspect has been stolen is received or kept by someone.
Penalty - Imprisonment up to three years, or/and with s fine up to RS 100,000

4. Section 66C – Using the password of another person: Someone who uses someone else's password, digital signature, or another kind of unique identification fraudulently.
Penalty - Imprisonment up to three years, or/and with a fine up to RS 100,000

5. Section 66D – Cheating using computer resources: If a person cheats on someone using a computer resource or communication.
Penalty - Imprisonment up to three years, or/and with a fine up to RS 100,000

6. Section 66E – Publishing private images of others: If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge.
Penalty - Imprisonment up to three years, or/and with s fine up to RS 200,000

7. Section 66F – Act of cyber terrorism: Cyberterrorism is the act of denying access to authorised individuals to computer resources, breaking into a secured system, or introducing a contaminant into a system with the goal to undermine India's unity, integrity, sovereignty, or security.

Penalty - Imprisonment up to life.

8. Section 67 - Publishing information which is obscene in e-form: If someone publishes, transmits, or arranges for the publication of any material that is lascivious, appeals to the prurient interest, or if its effect tends to deprave and corrupt people who are likely, given all the pertinent facts, to read, see, or hear the matter contained or embodied in it, then that person violates the law.
Penalty - Imprisonment up to five years, or/and with a fine up to RS 1,000,000

9. Section 67A - Publishing images containing sexual acts: If a person publishes or transmits images containing a sexually explicit act or conduct.
Penalty- Imprisonment up to seven years, or/and with a fine up to RS 1,000,000

10. Section 67B – Publishing child porn or predating children online: If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.
Penalty- Imprisonment up to five years, or/and with fine up to RS 1,000,000 on the first conviction. Imprisonment up to seven years, or/and with a fine up to RS 1,000,000 on a second conviction.

11. Section 67C - Failure to maintain records: Persons deemed as an intermediary (such as an ISP) must maintain required records for the stipulated time. Failure is an offense.
Penalty- Imprisonment up to three years, or/and with a fine.

12. Section 68 - Failure/refusal to comply with orders: If necessary to guarantee adherence to the terms of this Act, rules, or any regulations established thereunder, the Controller may, by order, direct a Certifying Authority or any employee of such Authority to take the specified actions or cease engaging in the specified activities. Any person who disobeys one of these orders is guilty of an offense.
Penalty- Imprisonment up to three years, or/and with a fine up to RS 200,000

13. Section 69 - Failure/refusal to decrypt data: If the Controller determines that doing so is necessary or advantageous for reasons that must be documented in writing, including the sovereignty or integrity of India, the State's security, friendly relations with foreign countries, or the maintenance of public order, he may direct any government agency to intercept information sent through any computer resource. When requested by any agency that has been instructed, the subscriber or anybody in charge of the computer resource must provide all facilities and technical support to decrypt the material. Anyone who refers an agency but does not help it is regarded to have committed a crime, even subscribers.
Penalty- Imprisonment up to seven years and possible fine.

14. Section 70 - Securing access to a protected system: Any computer, computer system, or computer network may be deemed a protected system by the competent government by publication in the Official Gazette. The individuals who are permitted to access protected systems may be approved by a written order from the competent government. A person is breaking the law if they acquire access to, or try to secure access to, a protected system.
Penalty- Imprisonment up to ten years, or/and with a fine.

15. Section 71 – Misrepresentation: If anyone makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate.
Penalty - Imprisonment up to three years, or/and with a fine up to RS 100,000

2.8 Challenges faced by Indian IT, 2011

1. **Digital Evidentiary Challenges**: The fundamental problem with computer crime is that almost all of the evidence is in digital form. Finding and preserving digital evidence has proven to be exceedingly challenging for investigators, and it has also proven challenging for judges and attorneys to speak in court. Problems with the sharing of evidence by Foreign Service Providers are

also brought on by S.65(B) of the Indian Evidence Act. The Indian legislative must take note of this issue and make the appropriate changes in the said provision in order to comply with the requirements of the digital era because international companies typically do not give certificates, which forces courts to reject the evidence.

2. **The traditional way of investigation which is failed in cybercrime**: ICT usage is growing, necessitating the deployment of new investigational tools. Therefore, particular technological expertise and understanding should be needed while conducting cybercrime investigations, prosecutions, and trials.

3. **Jurisdiction**: To choose The key area of difficulty for the judiciary when dealing with cybercrimes is jurisdiction. Cybercrime is essentially a global crime. The criminal justice system has a particularly difficult decision when deciding jurisdiction for a specific crime of this nature. The United Nations has also cited jurisdiction as a significant concern in cybercrime. Even the Indian government has acknowledged that one of the biggest challenges facing the judiciary is determining jurisdiction in cybercrimes. The government has been ordered by the Supreme Court to establish a common reporting system for cybercrime in this type of situation.

4. **No specific Legal Provision**: for the defence of personal freedoms online. Women who are online victims are generally protected under the IT Act of 2000. Although Indian legislators modified the IT Act 2000 in 2008, new types of cybercrime are still not covered. which also causes issues for the judiciary in cyber trials? When formulating national policy, criminal justice took this into consideration and instructed the Indian legislature to reclassify the preexisting cyber legislation.

5. **Operational challenges**: According to Section 78 of the IT Act of 2000, only police officers of the inspector rank conduct investigations into cybercrimes. This part has posed significant challenges on a practical level and has had an indirect impact on the judicial process. Court matters are taking longer and longer to resolve, which presents challenges for quick trials. In addition, because the government has not had authority over the Internet, service providers' lack of collaboration is another significant problem.

6. **The paucity of technical tools and skilled human resources**: Due to a lack of infrastructure, technical labor shortages, and technical instrument shortages, court proceedings are made more difficult for the judiciary. The Indian Parliament also proposed a nodal agency for cybercrime in 2017 and addressed the issue of training personnel who deal with it.

7. **The gap between Technology and Knowledge**: For the newly emerging cybercrime with the traditional criminal justice system, there is a gap between developing technology and traditional understanding. For dealing with the new types of cybercrimes, there are no established legal procedure norms, and there are no unique legal rules for each type of crime. Judges thus had several difficulties throughout the cyber trial when trying the case and handing down the verdict.

8. **Jurisdictional issues are a major hurdle:** Legal problems have been a significant roadblock in cybercrime prosecutions. The majority of crimes reported in Telangana are carried out by citizens of states like West Bengal, Bihar, and UP. There is no system in place to manage them locally. And going there to capture them is not so simple.

9. **Lack of awareness** – There is a lack of understanding at both the corporate and individual levels because there is no national regulatory policy in place for cyber security. Only in the presence of a regulated and overseen legislative framework can domestic internet users defend themselves and receive protection from cyberattacks.

10. **'Lack of urgency seen in cyber cases'**: There is always a link between the significant backlog of cybercrime cases and the improper production of incriminating electronic evidence in court. Furthermore, a lack of urgency in these matters always causes delays in the legal system.

Additionally, the prosecution finds it more challenging to present technological evidence in court as the trial drags on.

2.9 Suggestions for the success of the IT Act, 2000

(1) Educating and enlightening the average person about their online rights and responsibilities. Practically speaking, most people are unaware of the various types of cybercrimes, rules governing online, and venues for resolving disputes. To effectively combat cybercrimes and enforce cyber laws, it is essential that our law enforcement authorities, including the judiciary and police, receive the necessary legal and technical training (Karnikaseth, 2020).

(2) The police department's reporting and access points demand rapid attention. Every local police station on domestic territory should have a cybercrime cell that can efficiently look into cybercrime issues. One of the biggest barriers to swift justice delivery is accessibility.

(3) Additionally, Hyderabad, India is home to the sole government-recognized forensic laboratory in India that creates forensic reports for cybercrime cases. To effectively handle the growing number of cybercrime investigation cases, we need more labs like this. At the municipal, state, and international levels, trained and equipped law enforcement professionals can guarantee effective evidence gathering, proper investigation, mutual collaboration, and prosecution of cyber cases.

(4) In addition, there are no requirements for ISPs to keep logs for a reasonable amount of time to aid in tracing IP addresses in cybercrime cases under Section 79 of the IT Act, 2000. This requires immediate attention and action.

(5) Effective international cooperation regimes and procedures are needed for the investigation of cybercrimes, the prosecution of cybercriminals, and the execution of court orders. Although Section 1(2) read with Section 75 of the IT Act, 2000 gives India prescriptive jurisdiction to try suspects for offenses committed by anyone of any nationality outside India that involve a computer, computer system, or network located in India, on the enforcement front, the prosecution of such offenses and conviction is challenging in the absence of a duly signed extradition treaty or a multilateral cooperation agreement

3. Conclusion

In India, the judiciary is crucial to the defense, security, and rights of all online participants. The Information Technology Act of 2000 left some gaps, which the Indian judiciary has been attempting to fill. The judiciary has affirmed online stakeholder rights in various instances. However, in a dynamic environment, several new advances in cyberspace give rise to numerous undetected cybercrimes. India therefore, needed judges with such cyber-savvy who could handle and appropriately justify cybercrime. In addition, there has been relatively little societal progress or understanding of an individual's online rights, so it is important to increase this awareness in society. Therefore, all constitutional mechanisms must take all necessary steps to increase public knowledge of cybercrime and to implement measures to combat cybercrime.

References

Amiri, Y., Khademi, N., Khafri, F. Z., Akbari, Z., & Jangjoo, R. (2022). The Impact of Corona Outbreak on Virtual Education Policy in Iranian Universities. *Journal of Social, Humanity, and Education,* 3(1), 1-15.

Anoke, A. F., Onu, A. N., & Agagbo, O. C. (2022). Managerial Competencies and Growth of Small and Medium Enterprise (SMEs) in Abuja Metropolis, Nigeria. *International Journal of Financial, Accounting, and Management,* 4(3), 255-268.

Anoke, F., Ngozi, N. H., Uchechukwu, E. S., & Joyce, I. (2022). Entrepreneurial Marketing And SMEs Growth In Post Covid-19 Era In Awka, Anambra State, Nigeria. *International Journal of Financial, Accounting, and Management,* 4(2), 115-127.

Arya, N. (2019). Cyber Crime Scenario in India and Judicial Response. *International Journal of Trend in Scientific Research and Development,* 3, 1108-1112.

Das, S., & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International journal of engineering sciences & Emerging technologies*, 6(2), 142-153.

Hajgude, A., & Deshmukh, H. (2020). Cybercrime Scenario in India and Challenges to Indian Cyber Laws. *Parishodh Journal*.

Hudalil, A. (2022). Market Orientation Model in Indonesia Special Autonomy Regional Government. *International Journal of Financial, Accounting, and Management*, 4(3), 349-363.

Joshi, Y., & Singh, A. (2013). A study on cyber crime and security scenario in India. *International Journal of Engineering and Management Research*, 3(3), 13-18.

Kalra, K. (2017). Emergence Of Cyber Crimes: A Challenge For The New Millennium. *Bharati Law Review*.

Karnikaseth. (2020). IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers.

Majesty, H. (2010). Cyber Crime Strategy. *SoSftH Department, Editor*, 42.

Poonia, A. S. (2014). Cyber Crime: Challenges and its classification. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, 3(6), 119-121.

Rosadi, Y. M. R., & Barus, I. S. L. (2022). The Effect of Time Budget Pressure and Auditor's Competency on Audit Quality. *International Journal of Financial, Accounting, and Management*, 4(3), 241-254.

Sarmah, A., Sarmah, R., & Baruah, A. J. (2017). A brief study on Cyber Crime and Cyber Law's of India. *International Research Journal of Engineering and Technology (IRJET)*, 4(6), 1633-1640.

Singh, N. (2021). Cyber Crimes in India Spiked Nearly Nine Times Since 2013, UP Topped Chart in 2020: Data. *CNN-News18*.

Sushanth, S. S. (2013). Emerging Trends & Challenges in Cyber Law. *International Journal of Advances In Computer Science and Cloud Computing*, 1(1).

Swaathi, B., & Kannappan, M. (2018). Cyber Crime-An Indian Scenario. *International Journal of Pure and Applied Mathematics*, 119(17), 1053-1061.