Volume 1, Issue 1, January - June 2025, Pg. 44- 52

Journal of Asian Law College ISSN: 3107-3859 (Online)

7

"Changing Contours of Cyber Laws in Era of Digital India"

Ayushi Gupta,
Ph.D. Research scholar,
University of Lucknow

Keywords
Sedition, Bharatiya Nyaya Sanhita (BNS) 2023, Indian Penal Code, Sovereignty, National Security, Anti-national.

INTRODUCTION

With development and advancement in new technology and communications, the internet has now emerged as an essential part in our lives. Our lives are dependent on such new tools and technology and it has also made complexities of day today life much easier than before but, if these tools and technologies are used in malafide manner they can also prove to be extremely dangerous. Cyber law deals with the computer, computer resources, internet and legal issues related to them. It revolves around the legal, statutory and constitutional provisions which affect computers and computer network. It incorporates laws related to digital signature, cybercrimes, intellectual property, data privacy and data protection. UNCITRAL adopted Model Law on e-commerce in 1996 because of the growth in e-commerce and globalization. And in respect to this, the U.N. General Assembly passed a resolution that the States should take into consideration the Model Law. With introduction of Model Law, the Government of India enacted its first statute on cyber law, Information Technology Act, 2000. The IT Act, 2000 is a primary law which deals with e-commerce and cybercrime. Its enactment led to the amendment of other Acts like BNS, BSA, RBI Act, etc. for the effective application of the IT Act, 2000. Further, in 2008, major amendments were made to deal with offensive computer communications and cyber terrorism. If we talk about recent upheavals being made in Cyber Laws in India, we can undoubtedly cite the cases of Karmanya Singh Sareen v. Union of India1 and Justice K. S. Puttaswamy (Retd.) and anr. v. Union of India and ors2 where emphasis was laid on dataprivacy and protection of personal data. As a consequence of these cases, we witnessed the laying

1 233 (2016) DLT 436.

2 (2017) 10 SCC 1.

3 Sections 91, 92, 93, and 94 of the Information Technology Act, 2000 were omitted by the Information Technology (Amendment) Act, 2008, and Schedules III and IV were also omitted by the Information Technology (Amendment) Act, 2008.

down of the Personal Data Protection Bill in 2019 with a vision to effectively protect the personal data of the users which saw its ups and downs and was withdrawn in August 2022 to bring about more comprehensive law for the matter at hand. Subsequently, in 2021 the Government of India introduced Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 to regulate the digital content and online platforms like OTTs along with regulation of other intermediaries that deal with such digital content which adversely affect the young generation. The most important and recent developments in the cyber laws stands on the draft proposed on Digital Personal Data Protection Bill, 2022 to the Parliament after withdrawal of Personal Data Protection Bill, 2019 and it envisions the overall coverage of regulation of matters relating to personal data and privacy in changing societal needs to protect the informational privacy from misuse and abuse. Also, the proposed Digital India Act, 2023 which was recently presented on 9th March 2023 also offers comprehensive protection and regulation of Digital India in consonance of changing times and gives a framework that includes:

1. Rules under the Digital India Act
2. Digital Personal Data Protection Act, 2023
3. National Policy on Data Governance
4. Amendments in Criminal laws for combating Cyber Crimes

Thus, the paper seeks to study recent developments in the Acts or statutes governing the Cyber Law in India. The paper will dive into the reasons behind how the present laws are sufficient to regulate the Cyber Law in India with a critical analysis of Information Technology (Intermediary guidelines and digital media ethics code) Rules, 2021 with prospective amendments to the same. The major emphasis will be laid on an overview of how the Digital Personal Data Protection Bill, 2022 and the proposed Digital India Bill, 2023 can bring about revolutionary changes into the cyber law regime in new evolving dynamics of cyber security and related laws.

II.Contemporaneous Cyber Laws and Regulatory Landscape in India

The present Cyber Law regime revolves around the Information Technology Act, 2000 which came into force on October 17, 2000. Electronic records filing with the government, e-governance, and e-commerce are all intended to be officially recognised by the Act, which also aims to protect citizens from cybercrime and cyberterrorism. Following are the initial legislations covering the domain of cyber laws in India:

1.Information Technology Act, 2000
2.IT (Certifying Authority) Rules, 2000
3.IT (Certifying Authority) Regulations, 2001
4.IT (Security Procedure) Rules, 2004

A.Information Technology Act, 2000 and relevant amendments

B.The IT Act, 2000 is the overarching law that governs the use of computers, computer networks, and electronic data and information storage and retrieval. Laws concerning cybercrimes and the responsibility of service providers are also addressed in this body of law, among other things. The Act aims to provide legal recognition for the actions taken through the means of interchange of electronic data and other means of electronic communication, commonly referred to as "Electronic Commerce", that is, the use of methods other than paper for communicating and storing information and it further enables electronic filings of documents with the Government agencies for ensuring effective e- governance. The Preamble of the Act states the goal for promoting and regulating the growth of the IT sector, e-commerce, e-governance, and cybercrime prevention. The

4 Section 43, Information Technology Act, 2000 (Amended vide ITAA-2008)
5 Section 43A, Information Technology Act, 2000
6 Section 79, Information Technology Act, 2000

Information Technology Amendment Act, 2008 brought various amendments in the IT Act, 2000. The amendment Act was passed in the Lower House of Parliament on 22nd December, 2008 and on 23rd December, 2008 it was passed by the Upper House. It received the President's assent on 5th February, 2009 and came into effect from 27th October, 2009. This amendment was brought to cover and deal with those issues and challenges to further the development in IT sector and security concerns which was not covered in the original legislation. After the amendment the Act of 2000 contained 90 sections which was spread over 13 chapters.3 There are certain highlights of the Information Technology (Amendment) Act, 2008 which brought about much needed changes and updates to Cyber Laws in India and brought it in line to some extent to the global standards as per the need of time. For example, in order to make the Act more user-friendly for technology, several new definitions were added or changed. So, for example, "communication device" is now defined as "cell phones, any personal digital assistant or combination of both or any other device used to communicate, send or transmit any text, video, audio or image." "Cyber cafe" is defined as any establishment that provides internet access to the general public in the normal course of business. "Cyber security" is defined as the protection of information and electronic devices that handle and store data from unwanted access, modification, destruction, and disclosure. The following examples show how the IT Act, 2000 has expanded its reach due to the addition of additional provisions:

1.Enforcement of Digital Contracts- Section 10A was inserted to make sure that the e-contracts shall not be deemed to be unenforceable on the sole ground that it was made in electronic form and through electronic means.

2.Damages paid to affected persons- Section 43 of IT Act earlier provided penalty up to Rs. 1 Crore for an act of targeting and damaging computer, computer system or resource, etc. This section has been deleted and the certain parts of it have been replaced by the words, "…he shall be liable to pay damages by way of compensation to the person so affected"4.

3.Protection of Sensitive and Personal Data- Insertion of section 43A was made with purpose to protect possession and handling of personal and sensitive data or information stored in a computer system which is owned, controlled or operated by a commercial organization. In cases where there is no proper implementation and maintenance of reasonable protocols for securing personal and sensitive data by such organization, which ultimately results into causing wrongful loss or wrongful gain to any individual or organization, such negligent organization shall be liable to pay the compensation to the affected person.5

4.Punishment for Cyber Crime and Cyber Terrorism- The Amendment Act added Sections 66A to 66F to Section 66 that prescribes punishment for certain offenses such as electronic transmissions containing obscene material, cheating by impersonation of another with the use of computer devices, online identity theft, privacy violation and cyber terrorism.

5.Reduction in punishment for publishing and transmission of obscene material- The Amendment made in Section 67 deals with the term of imprisonment for publication or transmission of obscene and sexually explicit material in electronic form which has been reduced from five years to three years but has balanced the odds by increasing the amount of fine to Rs. 500,000 from Rs. 100,000. 6.Insertion of Sections 67A, 67B and 67C for regulating and

7 Information Technology (Amendment) Act, 2008

8Sections 118 and 119, Indian Penal Code, 1860.

9"Salient Features of the Information Technology (Amendment) Act, 2008." AdvocateKhoj. Available at: https://www.advocatekhoj.com/library/bareacts /informationtechnology/schedule1.php?Title=Information%20Techn ology%20Act&STitle=Amendments%20to%20the%20Indian%20Penal%20Code (last accessed on November 19, 2024).

penalizing sexually explicit material- a.Sections 67A and 67B provides for the penalty for offenses relating to publication or transmission of material having sexually explicit material and obscene acts including child pornography in e-format. b.a. The regulations pertaining to the intermediary's duty to preserve and retain sexually explicit information or material, including child pornography, as may be defined for the time, method, and format required by the central government are outlined in Section 67 C. 7.Empowering State against Cyber Terrorism-

1. Section 69 was revised to provide the authority to the state to command the interception or surveillance of any computer resource in order to decrypt any information, in light of the increasing possibilities and danger of terrorism. Sections 69A and 69B were subsequently introduced to the Act to accomplish this purpose. The purpose of these provisions was to give the state the authority to direct the restriction of public access to information through any cyber resource and to authorise the monitoring and collection of data or information through any cyber resource in order to guarantee cyber security. 8.Minimizing liability of Intermediary- By amendment made in Section 79 the intermediaries are minimized to the extent that the liability of an intermediary for any third party data, information, connection or link hosted by the intermediary is been exempted in the following specified conditions: - a.In cases where the responsibility of Intermediary is limited to facilitating the transmission, temporary storage, or hosting of the third party's information via a communication platform or system; b.Where the intermediary does not – i.starts transmission of data or information or ii.determine the receiver or iii.select or modify the data; c.Where the intermediary exercises due diligence while performing his duties.6

C. Amendments in IPC and Evidence Act

Indian Penal Code, 1860- In the Information Technology Act, 2000 the amendments related to IPC were mentioned under Section 91 and in the First Schedule of the Act. But the 2008 amendment7 deleted the provisions concerning the IPC and transferred to Part III of the Amendment Act, 2008. Sections related with records and documents like section 192, 201, 463, 464, 468, 470, 471, 474, 476 etc. under the IPC were amended with the introduction of the Information Technology Act, 2000 by inserting the word 'electronic'. To bring the electronic records and documents under the purview of all those provisions. Amendment was made under Section 4 of IPC, where a clause was inserted which states that if any person commits an offence outside India via targeting a computer resource situated in India, the IPC will be applicable in such circumstance. The explanation of 'Computer resource' which has the same meaning as mentioned under Section 2(1)(k) of the Information Technology Act, 2000 was inserted in the explanation of the provision for more clarity in the applicability of the Section 4. An explanation to the meaning of 'offence' was substituted that now states that every act which is committed outside territory of India using computer resource situated in India will be punishable under IPC. Further, Section 118 and 119 of IPC were also amended. In both the provisions the words "voluntarily conceals by any act or omission or by the use of encryption or any other information hiding tool, the existence of a design" was substituted by the words "voluntarily conceals, by any act or illegal omission, the existence of a design".8 In Section 464 the words "electronic signature" was substituted by the word "digital signature".9 These amendments made it clear that use of encryption and hiding tools employed for concealing an design of an offence are covered well in its purview. Therefore, Section 40 that defines

10 Information Technology (Amendment) Act, 2008
11 Ibid
12 Ibid
13 Ibid
14"National Policy on Information Technology, 2012." Ministry of Electronics and Information Technology, GovernmentofIndia.Available at:https: //www.meity.gov.in/writereaddata/files/National_20IT_20Policyt%20_20.pdf (last accessed on November 21, 2024).
15 Ibid
16 233 (2016) DLT 436

offence under IPC was amended by mention of Section 118, 119 and 120 under a clause of the Section. The meaning and purview of "offence" which holds the ground for penal laws thus stands amended by introduction of IT Act, 2000. Indian Evidence Act, 1872- Before the enactment of the Information Technology Act, 2000 the evidence admitted in the Court were generally in physical form. With the introduction of the IT Act, 2000 electronic record and documents were given evidentiary value in the court and were made admissible. After the 2008 amendment10 provisions related to electronic evidence were included under the Evidence Act. Inserted Section 65A and 65B which states the Admissibility of electronic records and documents as evidence. Section 65B states that the information which is taken from an electronic storage device or computer and produced in a court in electronic media or printout will be considered valid evidence under the Indian Evidence Act, if taken without any manipulation and signed by the person who is declaring it as correct records. Under Section 3 the interpretation clause in the Act, an amendment was made by inserting words "digital signature" and "Digital Signature Certificate" to bring it in tune with Information Technology Act, 2000. And later 2008 amendment11 these words were substituted with "Electronic signature" and "Electronic Signature Certificate", respectively. Section 47A was inserted by the IT Act, 2000 relating to relevancy of opinion as to digital signature. And the words, "Digital Signature" and "Digital Signature Certificate" were substituted with the words "Electronic signature" and "Electronic Signature Certificate" by the 2008 amendment12. Section 45A which talks about the Opinion of Examiner of Electronic Evidence states that when a court can admit an opinion on a matter related to information transmitted or stored in electronic form. Thus, the Opinion of the Examiner of Electronic Evidence mentioned in Section 79A of the Information Technology Act, 2000 is considered a relevant fact after insertion of 45A under Indian Evidence Act. Section 67A, 85A, 85B and 90A were also inserted by the IT Act, 2000 and later by the 2008 amendment13 words "digital signature" were substituted by "electronic signature".

D. National Policy on Information Technology, 2012

In September 2012, the Union Cabinet introduced the National Policy on Information Technology 2012. The Policy aims to strengthen Information & Communication Technology (ICT), to address and act towards country's economic and developmental issues.14 The Policy envisions, to strengthen and enhance India's position as the Global IT hub and to use IT and cyber space as an engine for rapid, inclusive and substantial growth in the national economy.15 The Policy is contemplated with the objective to increase revenue of IT industry and aims to expand exports in the sector by 2020, which has been achieved to an extent. It also envisages to create a cluster of supplementary skilled employment in the industry.

III.Karmanya Singh Sareen v. UOI16 (The Whatsapp Case)

This particular case needs an important mention as it is relating to dissemination of personal information stored in computer resource and its usage where the court talked about the concerns relating to misuse of the collected data. The brief facts of the case are that several privacy activists challenged the new terms of service of Whatsapp that allowed Whatsapp to share its user's data with Facebook. In 2010, when Whatsapp was launched, it has expressly promised that the users will get complete privacy protection and that their data would not be shared in any case and circumstances. But after the acquisition by Facebook, Whatsapp's privacy policy underwent a

17 Justice K.S. Puttaswamy v. Union of India (2017) 10 SCC 1

18 "Data Protection Committee Report." Ministry of Electronics and Information Technology, Government of India. Available at: https://www.meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last accessed on October 21, 2024).

19 Barik, Soumyarendra. "Government Withdraws Data Protection Bill to Bring Revamped, Refreshed Regulation." The Indian Express. Available at: https://indianexpress.com/article/india/government-withdraws-data-protection-bill- 8068257/ (last accessed on December 19, 2024).

drastic change. The Petitioners claimed that this action of revising the terms of service and taking away the privacy protection of users contradicts the most valuable and essential basic feature of Whatsapp that was complete security and protection of users' privacy. In the claims regarding revision of its terms of services, it contended that Whatsapp had provided advance notice to its users and only the individuals who have accepted and consented to continue are being bound by the revised terms. The petitioners, however, countered the argument saying that the changes made in the privacy policy are contrary to the principles of estoppels and is against the users' right to privacy. The court ruled that the users cannot compel Whatsapp to continue with its original terms of service as the original terms of service empowered Whatsapp to unilaterally change its privacy policy and stipulated the continued use of the Whatsapp's service to be considered as a deemed to be consented towards the terms of the revised policy post amendment of the privacy policy. Further, the court said that there cannot be grant of any relief under the Constitution as the legal position regarding the right to privacy was not yet decided. (As it was pre-K.S Puttaswamy17 Judgment). The Court directed that- (i)WhatsApp has to completely delete information of those users who chose to delete their WhatsApp account and (ii) As the individuals, who have opted to continue with the use of WhatsApp service, are concerned, it restrained WhatsApp from disclosing their information which was collected under the original terms of service, to Facebook or any one of its group companies. This case highlights a lack of critical and conceptual understanding of data protection in the Indian scenario, particularly with regard to the context of "consent" by the Courts in regard to use of collected data by the companies. While consent may be the requirement for processing data under the Data Protection Rules, but it does not indicate that the consenting people must throw open their privacy and surrender their rights. This lack of clarity in the proper definition of what constitutes "consent" under the existing laws highlights the need for a stronger regulatory framework to govern data collection and processing, and not mere self-regulation, to meet the challenges and risks of big data.

IV. Recent Developments in Cyber Law Regime in India

Landmark judgments on privacy and personal data made India's legislature to observe the need for a new regulatory framework to protect the users' privacy and personal data. So, the Personal Data Protection Bill 2019 was released on 10th December 2019. The Bill proposed to establish an independent authority that is Data Protection Authority of India, to look after the enforcement of the Bill. The Bill also proposed certain rights for data principal and liability of data collectors. And majorly addressing the right to access and confirmation, right to be forgotten, etc. As the introduction of the Data Protection Bill was the first effort of its kind, it needs detailed analysis and contemplation. It should be kept in mind that the new Bill i.e. Digital Personal Data Protection Act, 2022 which was introduced in November 2022 takes its foundation on the reasons for which the PDP Bill of 2019 was withdrawn.

A.Introduction and Withdrawal of Personal Data Protection Bill, 2019

In 2018, in order to create a "comprehensive legal framework" for policing the online world, the government withdrew the Personal Data Protection Bill from Parliament. Separate regulation on internet ecosystem as a whole, cyber security, telecom rules, data privacy and the use of non- personal data to promote innovation in the country are all included in this framework. This comes after the Bill was in development for almost four years, during which time it underwent numerous revisions, was subjected to assessment of Joint Parliamentary Committee and encountered opposition from

20"Intermediary Guidelines and Digital Media Ethics Code Rules, 2021." Ministry of Electronics and Information Technology,GovernmentofIndia.Availablea t : https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules- 2021.pdf (last accessed on December 29, 2024).

21 Rule 4(1) (b), Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021.

various parties, including technology giants and campaigners for protection of privacy. The government intended to introduce the new legislation during the winter session of Parliament, according to sources of the Ministry of Electronics and Information Technology (MeitY)18. Following the JCP's suggestions for a stronger data protection framework, the updated Bill will be prepared, considering the landmark 2017 Supreme Court decision in Justice K. S. Puttaswamy (Retd.) and anr. vs. Union of India and ors., which established the Right to Privacy as a basic right under Article 21 of the Indian Constitution. The official stressed the need of carefully revising and preparing the legislative outline in light of the many revision proposals received from the JCP. The Data Protection Bill has been in the works since 2018, after the creation of a draft by a committee headed by the former Supreme Court Judge, Justice B. N. Srikrishna. After that, a Joint Committee of Parliament (JCP) looked into it and then, in November 2021, they gave their recommendations and a Bill draft. Union Minister Ashwini Vaishnav explained the bill's withdrawal in a letter she issued to all members of parliament. The Joint Committee of Parliament thoroughly examined the Personal Data Protection Bill, 2019, he stated. Twelve recommendations and eighty-one edits went into the JCP report, which is now the basis for a comprehensive legal framework. It is advised that "The Personal Data Protection Bill, 2019" be withdrawn and replaced with a new Bill that follows all the rules given the present situation. The minister of state for information technology, Mr. Rajeev Chandrasekhar, recently said that new regulations will soon be introduced in Parliament. After initial preparation in 2018 and several revisions by JCP in 2021, the government withdrew the Personal Data Protection Bill.19

B. Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021

Nowadays, social media has evolved from just being a medium of entertainment to a platform for trade and commercial activities as well. The increase in usage of social media has also led to an increase in various kinds of abuse and infringement of privacy. And the lack of Grievance redressal mechanism for such social media platforms and OTT platforms made the victims helpless. To tackle these types of problems, on 25th February, 2021 the Ministry of Information enacted the Information Technology (Intermediary Guidelines and Digital Media Ethics) Rules, 2021 (Hereinafter, 2012 Rules).20

Following are the key points that illustrates the functioning of the 2021 Rules-

1.Publishing Privacy Policy and Directions for use of Personal Data- Rule 4(1)(a) of the 2021 Rules makes it mandatory for the intermediary to publish their privacy policy and guidelines for usage of personal data of the users on their websites or mobile application or both. It also states that privacy policy and user agreement are to be drafted in a certain way that makes the users not to host, display, publish, transmit, store or share such information which is against the society, misleading the public or harms the dignity of a person.21 2.Termination of account- Further, the Rule 4(1) (c) of 2021 Rules put an obligation on the intermediary to specifically notify the users in the cases where unethical information has been transmitted that such transmission would lead to termination of account or removal of the information. 3.Removal of unethical information- Rule 4(1)(d) of 2021 Rules states that if there is transmission of any unethical information on a platform, the intermediary has to remove that information as soon as it comes to their knowledge as specified under Section 79(3) of the

22 Ayanso, Anteneh, and Tejaswini Herath. "Law and Technology at Crossroads in Cyberspace." In Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practice, edited by Alfreda Dudley, James Braman, and Giovanni Vincenti, 57-76. United States of America: Information Science Reference (IGI Global), 2012.

Information Technology Rules, 2000. Further, that information has to be stored by the intermediary for 180 days for investigation. 4.Publicize details of Grievance Redress Mechanism- The intermediary has to publish the details of the Grievance Officers and the mechanism which it will be going to follow. In case when there is a violation of Rule 4 or other misuses, the officer has to register the complaint within three working days and has to resolve it within one month from the date of complaint. 5. Identification of First Originator of Information- The crucial element of the Rules is to the intermediary's obligation to ascertain the initial source of the information as directed by the Court or the responsible authority specified in Section 69 of the Information Technology Act, 2000. 6.T h e distinction of Age groups -OTT platforms have to classify the contents on the platform into 5 categories grouped as U, U/A- 7+, U/A -13+, U/A -16+ and A. Therefore, the 2021 Rules has successfully given a regulatory framework to the OTT keeping in mind their growing popularity among students and young population in majority. However, being objective in nature it does not cover other major concerns like data protection and data privacy

V.Towards Secure Digital India

As it is said that one should change with changing times, the same is applicable for the law and the society. With the advancement in the area of Information Technology, it becomes pertinent to change the law of the Country to step up in consonance with the cyber world. International efforts have been made in different countries for protection of their citizens from various threats of Data breach, Data Theft, Protection of Personal Data, Cyber Crimes and various other aspects. This is why in November 2022, India introduced the Digital Personal Data Protection Bill,2022, which is now being considered for passage in the House of Parliament. It lays out a comprehensive framework for the protection of personal data and covers the essentials of the Personal Data Protection Bill of 2019. In this bill, the processing of digital personal data, whether gathered online or offline and then digitalized, is discussed in relation to its applicability inside India. If the processing is done outside of India with the purpose of providing goods or services or profiling persons in India, it will also be subject to this law. The protection of personal data is another feature of the bill. It states that personal data may only be used for authorised reasons and with the owner's agreement. The concept of Implied Consent might be used in certain contexts. In addition, the bill seeks to designate individuals as data custodians, who are then obligated to ensure that data is accurate, safe, and deleted after its purpose has been fulfilled—an action that indicates the recognition of the Right to be Forgotten. The right to access one's own data, request its deletion or correction, and have one's grievances heard are all rights guaranteed to citizens under the bill. It also lays out the authorities of the federal government, which allow it to exclude some government agencies from the Bill's requirements in order to address matters of state security, public order, and crime prevention, among other things. Additionally, the bill offers a well- organized framework for data protection and states that the Central Government must create the Data Protection Board of India to decide on cases involving non-compliance with the bill's requirements. The Indian government faced a wide range of cyber threats, including privacy and data protection on the internet. In response, the cyber-legal community eagerly anticipated the proposal of the Digital India Act, 2023, which would address all the gaps in our current cyber law framework. While the final text of the bill has not yet been submitted, the idea was made public at the Digital India Dialogues in Bengaluru, Karnataka, on March 9, 2023, by the Ministry of Electronics and Information Technology (MeitY).

The presentation of proposal covered Digital India Goals, 2026 along with the need for Global Standard Cyber Laws and the vision of Digital India that states: 1.$1 trillion digital economy by 2025-26: empowering Atmanirbhar Bharat 2.G l o b a l innovation and entrepreneurship system 3.I n d i a shaping the future of technologies 4.India to become a significant and trusted player in the global chain for Digital Products, Devices, Platforms and Solutions to enhance the economy by utilizing cyber resources Along with the vision, it illustrates the structure of Digital India Act that addresses the tenets of Open Internet, Online Safety and Trust, Accountability and Quality of Service with a dedicated and specified Adjudicatory System for civil and criminal offences with the ease of access, fast and timely delivery of remedies, resolution of cyber disputes, developing a unified cyber jurisprudence and that ensures enforcement of the rule of law online.

VI.Conclusion/ Suggestions

As we delve into the current cyber laws and regulations, we discover a significant void in the current regulatory system when it comes to establishing the parameters for citizens' safe and stress- free online presence. This void must be filled with a robust adjudicatory and regulatory framework that is both promising and significantly more stringent in the digital age. The Information Technology Act, 2000 and its subsequent revisions and ancillary rules and regulations fall short of the current state of cyber law. The Digital India Act, 2023 proposal highlights these shortcomings: inadequate protections for users' rights, trust, and privacy; inadequate identification of threats and new types of cybercrime; no system in place to raise public awareness of the issue; and no clear framework for regulating unlawful and harmful content and information found on the i There is a lack of a unified, coordinated, and harmonised institutional regulatory body; there is also a lack of a specialised and effective system for investigating cyber incidents; and lastly, there is no system in place to respond to cyber incidents in a coordinated manner. Therefore, the world as it seems has been changing at a rapid rate and to be in consonance of changing dimensions of the society, it is imperative to have a complete cyber regulatory mechanism in India. As India has now become a forerunner in internet usage and there are several ways to deal with computer crime using technologies. Legal fraternity should not be hesitant and needs to consider the appropriate technologies that should be in place to support the successful implementation of security policies. With the security technologies in place and the policies and procedures for acceptable use should be integrated components of any regulatory strategy by the framers of new legislations. The most commonly used protection measures while using technological resources which can be efficiently used for their enhanced performance are as follows:

● Authentication and Authorization: for providing a system of tracking access to network resources. ● Enhanced Firewall technology: which acts as a security gateway in the form of hardware and/or software placed between internal and external networks to prevent outsiders from invading private networks which has a double check at the time of entering the private information. ● Intrusion Detection System (IDS): an application designed to detect network-based attacks, such as Denial of Service (DoS) attacks. ● Intrusion Prevention System (IPS): an application designed to prevent network-based attacks, such as Denial of Service (DoS) attacks. ● Authenticating Encryption based module: which runs to provide a encoding of information before its transmission into the network, then decoding them at the receiving end so that recipients can read or hear them.22

Thus, with the need of revamping Information Technology Laws in lines of era of Digital India it can be concluded that rigorous study and research is still needed to bring the idea behind Digital India Act to its reality as it promises to meet the global standards of regulatory and adjudicatory mechanisms which can be achieved by catering to the technological advancement and using strategic mechanism.