Cyber Laws Governing Online World in India

Bhavana
Regional Institute of Education, Ajmer, Rajasthan
Email: bbhavana1289@gmail.com

Abstract- *Society includes institutions like family, school, religious organisations, polity. Polity makes rules and takes decisions for whole society. These laws create order in the society. Similarly, to regulate cyberspace, the online world and the related crimes, cyber laws are made. Covid 19 pandemic made us more connected and dependent to that online world. When the usage increased it also increased cybercrimes like hacking, cyber stalking, phishing, identity theft, cyber bullying, cyber terrorism, voyeurism. Data today is considered new oil. Government, private sector and individuals store lots of data virtually of the financial, personal and intellectual property nature and the one having access to it rules. Just like oil is a driver for any economy this position is now slowly taken by data. Hence the awareness about cyber laws and cyber security become much more crucial. Information technology act 2000 is a landmark statute that regulates cybercrimes also. Amendments to Indian penal code that defines crimes in India were made under the information technology act to include cybercrimes in that list. A subordinate legislation to this act has also been passed namely information technology rules 2021 to frame ethical code for social media platforms, digital media and OTT platforms. It is important that our population also have civic education and awareness regarding these legislative measures. Therefore, this paper aims to study cyber laws, cyber ethics and statues in place to prevent cybercrimes and build cyber security in India. It uses secondary sources for arriving at study results.*

Keywords**:** cyber laws, cybercrimes, information technology act, cyber ethics

Introduction

Laws bring order in society and these are the standards that people follow to bring uniformity in their social behaviour. The definition of law here includes all the sources of law including custom, religion, scientific commentaries,adjudication, equity,natural justice,legislation. As society is dynamic and it keeps on unfolding its new dimensions hence the constitutions around the world have made provision for amendment in order to match footsteps with the society. For example, to make education accessible and inclusive article 21A was added to the constitution of India as a fundamental right just after article 21, Right to life and personal liberty. It was realised the now mere existence of life is not sufficient, need is of a dignified life and education plays a very prominent role here. Human when part of society is able to grow in every realm, educational, professional, political, cultural, religious and spiritual, environmental collectively. State was created with the aim of solving all the conflicts and disorderliness while achieving all

of these aims. With the development of technology and the creation of cyber space, a whole new area of responsibility has been added in the domain of state. Now the state not only will be guarding the problems in the physical world but also this virtual and cyber realm.

India is witnessing the rise of new age technology with the industrial revolution 4.0 like artificial intelligence, machine learning, internet of things, Virtual reality, Augmented reality, 5G technology etc. As an invention is a gift in the hands of a scientist, the same invention becomes a source of destruction when in the hands of a criminal. The same thing applies to this cyber space also that has provided a whole new area for the criminals, where the risk of executing the crime in the anonymity of the cyber world has become lesser and lesser as compared to the physical world. With the newer definition of property and our identity online for example, the intellectual property, cryptocurrency etc., criminal has got the opportunity to impact people`s lives through cybercrimes like hacking, identity theft, social media frauds, online banking frauds, copyright infringement, online hate speech, phishing, snooping, online stalking, bullying and even cyber terrorism.

Objectives

This paper aims to study the significance of the cyber laws in today`s changing realm. It explores the laws in place ranging from parliamentary legislations, amendments, subordinate legislations, judicial pronouncements in this domain.

The study is also trying to emphasise that cyber technology has linked government and private sphere. Hence there is need of coordination between public and private domain to solve the issues in the cyber space.

As the internet has linked the world beyond territorial boundaries, so there is also the need of contribution internationally as holistic approach, in order to deal with the crimes like cyber terrorism and cyberattacks impacting countries across the nation equally.

Methodology

Secondary researchhas been adopted involving summarising and synthesising existing work. Data from official documents from government of India like Information technology act 2000 and its subsequent amendments, Indian Penal code 1860, The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 etc. have been analysed. Official websites of the concerned departments and ministries, newspaper editorials, published academic papers have also been taken into consideration. For understanding some of political and legal concepts, textbooks have also been referred. Studied previous researches and applied the learning for establishing statutory and jurisprudential analysis of cyber laws in India.

Need of Cyber Laws in India

As there are changes in the definition of society, state, laws, similarly there are changes in the definition of government. As there used to be a strict difference in the public and private arena. Nowadays public and private arena is intermixing with the coming of cyber world and hence the

cybercrimes. The internet is very international and anonymous making it difficult to decide jurisdiction in cybercrime. Even the definition of war is changing, it is no more the conventional one fought with arms, ammunitions and missiles, it a hybrid warfare now, conventional warfare aided by new age threats to the state like cyber warfare and information warfare as was seen during Russia-Ukraine war recently. It can lead to disorder even in normal situations by meddling with our democratic processes like elections, formation of public opinions, campaigning as we saw during Cambridge Analytica, fake news cases, online hate speech cases etc. That impact the process of our political socialisation, political culture and the voting behaviour of our electorate.

Cyber Laws in Place

In India, the information technology act 2000 is the fundamental statute in this regard. This document gives definition of cybercrimes and also specifies their punishments. The cybercrimes defined in the information technology act 2000 and suggested punishment and penalties are:

- Tampering with computer source documents.
- Sending offensive messages through text, image, audio and video.
- Dishonestly receiving stolen computer resource.
- Fraudulently making use of the password or any other unique identification feature of any other person called identity theft.
- Cheating by personation by using computer resource
- Violation of privacy

This act further amended some other legislations like Indian penal code 1860, Indian evidence act 1891, banker`s books evidence Act 1891 and RBI act 1934 in order to align them with the cyber space domain.

Internet has helped to connect people across boundaries and made communication, storage, banking, education, business and entertainment, accessible and inclusive. It also had its dark side. The criminal realm was also making use of the internet as a disruptive technique to destabilise a country`s functioning through video terrorismand it became necessary to redefine what terrorism means. Similarly, as the government itself was adopting e-governance as measures to regulate and manage affairs ofthe state, hence the threat of breaching the security of a military computer for example was also impacting the public realm. IT Act was then amended in 2008 in order to address issues likecyber terrorism, sending offensive messages, child pornography, leakage of data by intermediaries and voyeurism. Offenses defined after the amendment were:

- Cyber terrorism
- Punishment for publishing or transmitting obscene material in electronic form
- Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form

- Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form

Cyber terrorism has been defined in the act as whoever, with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people by–(*i*) denying access to any person authorised to access computer resource; or (*ii*) attempting to access a computer resource without authorisation (*iii*) introducing any computer contaminant, and by means of such conduct causes death to persons or damage to property or disrupts supplies essential to the life of the community or adversely affect the critical information infrastructure, commits cyber terrorism. This provision came in order to control the use of computer networking and internet connectivity by the terrorist for committing their organised crime and also to stop propaganda activities adopted by them to spread ideologies and to terrorise the population.

Results and Discussion

Success of these laws is visible when justice is provided to people under the provision of this act. These Supreme Court cases in this regard are worth noting.

- Syed Asif Uddin and Ors. vs The State Of Andhra Pradesh [2005] A case involving section 65 of the IT Act and was ruled that a phone handset also comes under the category of computer, accused was found guilty of tempering with the computer source (section 65).
- Bhim Sen Garg Vs State of Rajasthan and Others. [2006] Libellous content was shown against the person by tempering with the computer source (a CD), provided justice through section 65 of IT Act.
- Shankar Vs State Rep. [2010], A case of unauthorised access to a protected system and was charged under section 66, 70 and 72 of the IT Act [computer related offences (section 66), protected system (section70), disclosure of information in breach of lawful content(section 72).]

Government of India while dealing with cybercrimes and maintaining cyber security infrastructure has the provisions of the IT Act to its aid. According to this act the government both at centre and the state has the power:

- To issue directions for monitoring or decryption of any information through any computer resource.
- To issue directions for blocking the public access of any information through anycomputer resource.
- To authorise, monitor and collect traffic data or information through any computer resource for cyber security
- The appropriate government may declare any computer resource whichaffects the facility of critical information infrastructure, to be a protected system.

According to the provisions of Information and Technology Act section 70B, the IndianComputer Emergency Response Team (CERT-In) was formed in 2004 by the government of India under the ministry of communications and information technology (Now, Ministry of electronics and information technology). These following functions are performed by it, in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents;
- Alerts and emergency measures for handling cyber security incidents;
- Coordination of cyber incidents response activities;
- Issue guidelines, advisories and carrying out research relating to information security practices, procedures,response and reporting of cyber incidents;
- Give direction to the service providers, intermediaries, data centres, body corporate and any other person.

CERT-In in its regular vulnerability notes issue directions, advisories, recommendations for the users of applications/browsers like WhatsApp, Facebook, Twitter, zoom app, Microsoft edge, Google chrome, Zoho software to name some, in order to make users update them from newer vulnerabilities that have crept in. This is the government Nodal agency for solving cyber issues.

In today`s realm when the world has faced and is facing the cyberattacks like Wanna Cry ransomware, Petya, Stuxnet that doesn't differentiate between territorial boundaries of the states and as the internet is big and international, connecting people from across the globe. So is the case for cyber laws. In order to cater to this internationality of cyber space and to provide justice the IT Act says that provisions of this act shall apply also to any offence committed outside India by any person irrespective of his nationality. Similarly, to deal with cyber security issues for example collaborative efforts from Government department, Police, Academia, Industry, International organisation has been initiated in the name of cyberdome project by Kerala police.

This law also has some guidelines for the intermediaries. According to the said act itself an "intermediary" with respect to any particular electronic record, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. It includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cybercafé. This act has provided guidelines for them to function. For example, Section 67C of the IT Act gives powers to the intermediaries to preserve and retain information, as the central government may prescribe.

Recently WhatsApp`s new privacy policy came under sharp criticism and was accused of violating Right to privacy of the users, sharing of the user`s personal data with a third party, violating data localisation norm, not specifying what type of information will be collected and if users disagree, then they will not be allowed to access the app. Later WhatsApp allowed the

users even if they don't agree with new privacy policy and added another layer of protection to the communication app called end to end encryption service.

With the coming of new age platforms like over the top media (OTT) and their associated threats like adult content, lack of censorship, obscenity, using abusive language, associating vulgarity with the traditional culture etc, the need was felt to regulate this unregulated media also. So, the information technology (intermediary guidelines and digital media ethics code) rules, 2021 creates a framework to regulate their content and requires them to formulate a grievance redressal platform for the users to address their issues. Recently Central Government has notified amendment to these rules including addressing people`s concerns in their regional language and allowing users to appeal the intermediary`s action on their complaint to Grievance appellate committee.

Conclusion

Technological development is the need of the hour, internet is here to stay, grow and develop in the light of fourth industrial revolution and artificial intelligence. Similarly, laws should also continue to develop to match the pace of technology. Just like amendments, judicial pronouncements, executive orders keep the orderliness of the physical world in pace with the changing society, similarly all the sources of laws legislation, adjudication and amendments etc have to develop accordingly in case of cyber laws also. For example, some of the provisions of the Information technology act have been held invalid by the supreme court of India considering its contravention with the fundamental rights as are mentioned in constitution of India. Shreya Singhal vs union of India is the case in point where section 66A of this IT Act was repealed by Supreme court of India as it violated article 19 (1) (a) freedom of speech and expression. Regulation of cyber world in necessary as Rule of law principle applies in the cyber space too.

References

Information Technology Act 2000 (amended 2008), available at:https://www.meity.gov.in/content/information-technology-act-2000

Information technology (intermediary guidelines and digital media ethics code), Rules, 2021 available at: https://www.india.gov.in/information-technology-intermediary

For government notifications referred this:Press Information Bureau (pib.gov.in)

Indian computer emergency response team, official website, available at:cert-in.org.in

O.P. Gauba: An introduction to political theory (National Paperbacks, 2019).

Cyber Security Awareness Booklet for Citizens.pdf (cybercrime.gov.in)

For landmark judgements : Shreya Singhal v U.O.I (legalservicesindia.com)