21st century is a witness to the deep penetration of internet technology. The need to connect people across the world and bring them closer has been the driving force of the new age inventions. No sector of today’s life is devoid of internet, ranging from its employment in businesses, banking, finances to government administration. The depth of internet diffusion has moved beyond the social confines of individuals’ lives and has become a decisive means influencing every waking moment around the world.

As the principle of Yin and Yang dictates, the good and bad remain inseparable so has been the case with the invention of the internet. The same internet which aims at connecting people has become the driving force to lodge a wedge among the people, creating feelings of fear and resentment among the masses. The rapid interconnectivity offered by the internet has become a major channel to spread disinformation and fake news, conduct online theft and security breaches, stifle freedom of expression. During such times, it becomes imperative for the state to step in and take up the charge of positive regulation of this ever-expansive medium called the internet.

States across the world are still coming to terms with the internet phenomenon as they reap the benefits out of it and battle its negatives. A number of legislations have come into existence to control the surge of crimes witnessed with the increased infiltration of the internet. For example, America has enacted Cyber Intelligence Sharing and Protection Act to address various cyber-crimes as well as enacted the Children’s Online Privacy Protection Act, being considered the country’s first privacy act written with regard to the internet. Even the European Union has enacted the GDPR (General Data Protection Regulations) in its effort to ensure data privacy of its citizens from public and private organizations. Also, it caters to the dimension of data portability i.e. people having the right to demand a return/transfer of their data from a particular entity. The institution of National Data Protection Authorities across the EU member states to investigate matters of data breach forms an important part of GDPR.
Back home, India introduced cyber legislation as early as 2000 with the ITA (Information Technology Act) and its amendment, the IT Amendment Act of 2008. These legislations emerged with the electronic communication occupying a centre spot, amidst the growing tide of globalisation, international trade and e-commerce in the early ‘90s. Paperbacked records began to be replaced with electronic data and systems of communication. Model Law on E-commerce passed by UNCITRAL (United Nations Commission on International Trade Law) in 1996 provided recognition to electronic communication and records, as an equal to paper-based records and communication. This prompted other countries including India to make subsequent additions to their Constitutions.

The ITA 2000 gave legal recognition to electronic documents and digital signatures, as well as instituted systems to deal with various offences, contraventions and cyber-crimes. However, the increased reliance on IPC (Indian Penal Code) for cyber-related crimes and criticisms of the ITA 2000, arose the need for a number of amendments within the Act. This resulted in the introduction of the consolidated Information Technology Amendment Act 2008. Some of the positive changes in the form of emphasis on data privacy and information security were added. At the same time, it addressed concerns regarding child pornography and cyber-terrorism. It redefined the role of intermediaries and the Indian Computer Emergency Response Team (CERT-In) in maintaining cybersecurity. The 2008 Amendment, also, issued directions for the corporates regarding their internet security practices.

However, a number of events in the digital realm are questioning the effectiveness of the available cyber legislation in the country. From the abrupt blocking of internet services in
the state of Jammu and Kashmir last year to its restoration at only 2G speed. Also, monitoring and taking down social media posts and accounts condemning government actions after the announcement of the Citizenship Amendment Act (CAA) are some of the examples of overt state control. Simultaneously, the inability of the government to manage the extensive use of social media to incite communal disharmony in the form of riots, lynching in the society. And its further exacerbation with terrorist organizations employing the online platforms for radicalization, propagation of their cause and committing cyber-crimes

The implementation of law regarding the censorship and content regulation has been skewed on a number of occasions in the country. This is evident from the Shreya Singhal v. Union of India 2015 case. Herein, the Supreme Court invalidated Section 66A of the ITA 2000. The Court stated that “prohibition against the dissemination of information by means of a computer resource or a communication device intended to cause annoyance, inconvenience or insult” is beyond the scope of reasonable and valid exceptions as mentioned under the right to freedom of speech and expression [Article 19(2)]. The judgement comes after the arrest of two women who posted on Facebook questioning the shutdown in Mumbai city after the death of a popular political leader. The police arrested them under Section 66A of the ITA 2000 for their supposedly offensive and objectionable online statements. Section 66A details into the punishment of individuals involved in spreading of offensive/false information through online medium, for the purpose of causing “annoyance, inconvenience, danger, insult, injury, hatred or ill will”. The women were later released, however, went ahead and filed a petition seeking redressal for the violation of their fundamental right to freedom of speech and expression, challenging the constitutional validity of Section 66A.

Section 66A was termed as vague with no specificity by the Court, thus, infringing on the right to freedom of expression. However, according to the 2018 study of Internet Freedom Foundation, the Section was still employed to register approximately 70 cases in the lower courts. The Supreme Court was moved again in 2019 regarding the dissemination of its judgement, challenging the “post-decisional oversight and implementation”.

This imposing surveillance of the state has been extended to international actors as well in the digital space. The recent geopolitical and border tensions between India and China has sparked a digital ban on various Chinese applications operating in the country. Section 69A of the ITA 2000 along with relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009 (the Blocking
Rules) have been invoked. The ban has been imposed under Rule 9 of the Information Technology Rules, 2009 which calls for an emergency situation. The government in its statement defending its actions has stated that these apps are “stealing and surreptitiously transmitting users’ data in an unauthorized manner to servers which have locations outside India”. This poses a dangerous and serious threat to the sovereignty, integrity and security of the country, thus, resulting in the government’s immediate ban.

The contentious decision to block the access to these Chinese apps has been detrimental for the Indian public as a large part of the population are avid users of these apps. TikTok itself has 100 million active users in India and the WeChat application has been a useful communication link to Tibetan refugees as well as Indian students in Chinese universities.

This very notion of the ban is interfering with people’s exercise of their fundamental rights as enshrined in Article 19(1). Judgements in cases like Faheema Shirin v. State of Kerala and Anuradha Bhasin v. Union of India confirm the same. It explains how blocking of internet services is tantamount to violation of an individual’s privacy and counts as ‘abuse of power’.

The imposition of restrictions on fundamental rights citing valid reasons under Article 19(2)
need to be just, reasonable as well as fair under Article 14, which is applicable to both citizens and non-citizens. This brings under the scrutiny the very object of seeking a ban against the Chinese apps, as numerous American and European apps like Facebook, Amazon, too, have been penalised internationally for their questionable personal data collection methods. Also, the spread of disinformation, through apps like TikTok form a major part of the concern as it interrupts with the democratic processes in the country. However, these concerns extend beyond Chinese apps and have reared their ugly head on every other internet application. This raises the question regarding the effectiveness of the ban. And emphasizes the dissimilar treatment met out to Chinese app developers. Thus, a number of Chinese companies have moved the Court against the decision, citing it as discriminatory and unfair under Article 14.

Such a differential treatment towards Chinese apps results in a subsequent selective block on access to users of these apps as well, invoking the provisions of Article 14. “A restriction on access to the internet also has to be fair, just and reasonable and not arbitrary at the very least.” This affects the rights of internet users as their right to expression through a certain medium stands restricted. The intrusive nature of the ban has infringed with their fundamental notion of civil liberties. However, the constitutionality of Section 69A along with Information Technology (Procedures and Safeguards for Blocking for Access of Information by Public) Rules, 2009 has been validated by the Supreme Court in Anuradha Bhasin as well as Shreya Singhal cases. Accordingly, the government do possess within their right to block access to selective internet services.

Chinese laws such as Articles 7 and 15 of National Intelligence Law (2017) require corporations to share users’ data upon request. Also, apps like Helo, Shareit gain access to users’ phone location, camera and microphone increasing the risks associated with Chinese apps. At the same time, India lacks a proper, defined data protection system framework owing to the privacy concerns as raised in the Justice Puttaswamy I (Retd.) v. Union of India case (2017).

The actions of the state in blocking the fundamental rights must be proportionate to the intended legitimate goal. The provisions by which such proportion can be scrutinized are laid down in Modern Dental College v. the State of MP by the Supreme Court. The state must adopt one of the least restrictive measures to achieve the aim, such as ensuring the application creators are following the required security procedures, imposing fines and issuing directions in case of any breach, in this particular case.

Indian cyber environment, in recent years, has become vulnerable to the spread of online terrorist propaganda. The expanding nature of social media has provided the terrorists,
particularly ISIS, fertile grounds to reach out to the youngsters to further their program of radicalization. The former ISIS recruiter in India, Mohammad Shafi Armar, who was killed in a drone attack in Syria, was involved in the formation of ISIS units in every state. Apart from 30 recruits from India, he was in contact with 600-700 potential recruits via online platforms of WhatsApp, Facebook, Telegram. ISIS has been employing the use of regional languages such as Hindi, Urdu, Gujarati and Tamil to reach out, especially to the Muslim youth in India.

Videos, blogs, chats are the various forms of online communication initiated by ISIS recruiters in India and the Gulf region. The youth have become susceptible to the pro-ISIS agenda through the mechanism of ‘fighting for a cause’ combined with videos akin to Hollywood action films, showcasing video-game effects. Their social media reach expanding up to 30,000 Twitter handles (as of 2015) also has been responsible for communal clashes in the country, owing to constant hate mongering on the social media platforms inciting the public, leading to law and order problems. Simultaneously, ISIS methods have sparked competition among rival terror groups vying for similar social media tactics, such as the widespread online popularity enjoyed by late Kashmiri militant Burhan Wani.

Bothered by these concerns and the 2015 Paris attacks conducted by ISIS through its foreign fighters, the Ministry of Home Affairs started monitoring online activities sympathetic to the ISIS cause. For the same, a multi-agency 24/7 social media analysis centre as an effective measure of counter-terrorism was considered as early as 2015. But due to the evolving nature of cyber terrorism, ITA 2000 falls short of curbing the online terrorist activities as well as addressing the various legal, policy, regulatory concerns associated with the internet. Thus, the laws need to be in tandem with the new developments in communication technology. This should be in complement to the existing counter-cyber security initiatives such as National Informatics Centre (NIC), Indian Computer Emergency Response Team (Cert-In), National Information Security Assurance Programme (NISAP), and Indo-US Cyber Security Forum (IUSCSF).
India needs an institutionalized counter-response to online terrorism. Surveillance, monitoring needs to be supported by de-radicalization programmes. Simultaneously, it is significant to encourage a healthy online discussion regarding terrorist propaganda for spreading awareness. However, care should be taken to avoid the online dialogue regressing into a propaganda bandwagon.

**Conclusion**

The misuse of legal provisions such as Section 66A of the ITA 2000 has created the image of a ‘big brother’ government, wherein people are targeted for expression of their political opinions. The very revocation of this Section has been perceived as an attempt to uphold the democratic ideals as prescribed in the Constitution.

With increasing concerns regarding data privacy and internet monitoring, it has become imperative for law to distinguish between personal and public data information. Also, the retrieval and use of such data by security and law enforcement agencies has come under the
Cyber Legislation In India: The Road So Far

limelight. The present provisions under the IT (Reasonable Security Practices and Procedures & Sensitive Personal Data and Information) Rules 2011 as well as the proposed Privacy Bill 2014 state that “any information that is freely available or accessible in the public domain or to be furnished under the Right to Information Act, 2005, or any other law for the time being in force shall not be regarded as sensitive personal data for the purposes of this Act”.

In 2018, the Personal Data Protection Bill was submitted to the Parliament catering to the privacy of personal data as well as the formation of Data Protection Authority of India. The Bill has come under criticism for including provisions giving the government unlimited access to users’ data.

Concerns regarding arbitrary blocking of internet services under Section 69 and 69(a) need to be addressed as well. As witnessed in the form of shutting down of internet services in various parts of the country during the 2019 CAA (Citizenship Amendment Act) protests. It is important to “inform(ing) censored groups/individuals reasons for the block and allowing them to contest it and seek redressal from the relevant authority, as also informing the public about the reasons of the block after the emergency has been dealt with, to encourage openness”.

The overarching powers assigned to the intermediaries under Section 79 of the ITA 2000 can very well be misused. As the internet service providers may act beyond the requirements of the government, the nature of the content posted online should be the responsibility of the users and the companies. Multiple internet applications and platforms comply with the cyber laws of their home country, even in their local operations in the host nation. This results in clashes, as the Indian government expects these companies to comply with the local laws of the land, especially dealing with sensitive issues of blocking online content/services. Thus, it is important for the Indian government to resolve the legal dilemma regarding the precedence of laws in the cyber world.

The above mentioned are few of the multiple challenges faced by the Indian legal system in its management of the internet. To resolve and overcome these obstacles, it is imperative to view the internet as a medium and update the ITA 2000 which was formulated primarily to cater to e-commerce. Presently, the Indian legal mechanism is incapable of dealing with the dynamic nature of the internet. Transparency, accountability, autonomous, proactive legal provisions are the basic requirements for the formulation of a new and improved internet-centred legislation.
Cyber Legislation In India: The Road So Far

Sources

https://globalfreedomofexpression.columbia.edu/cases/shreya-singhal-v-union-of-india/

https://thewire.in/tech/india-ban-chinese-apps-tiktok-legal

http://sbi.hnlu.ac.in/rising-against-cyber-terrorism-indian-perspective/

https://thediplomat.com/2016/05/isis-in-india-the-writing-on-the-facebook-wall/


https://idsa.in/system/files/monograph/monograph55.pdf

The views and opinions expressed in this article are those of the author and do not necessarily reflect the views of The Kootneeti Team

Facebook Comments