INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

SECURING CYBER SPACE: A CRITICAL ANALYSIS OF IT ACT, S. 69A

AUHTORED BY - AKSHAY PRAMODH & GOWRI DEV

INTRODUCTION

In June 2020, netizens woke up to the news of the Indian Government banning some of the most used platforms and application including TikTok. Colloquially the 'TikTok ban', the Union Government's move of total ban of 59 Chinese apps came in the midst of the India-China stand-off at Galwan. The Government notification blocking access to the apps describing them as prejudicial to sovereignty, integrity and national security. In addition to it, the Government also blocked access to nearly 40 pro-Khalistan websites. The saga of ban continued with the Government blocking 118 apps including the video game giant PUBG stating similar reasons. While the security threats that such apps pose cannot be entirely dismissed, the possibility of it being a catalyst for unreasonable trespass over internet freedom lurks behind. Till January 2023, the Union Government has banned around 300 apps citing the reasons of national security.

The power of the Central Government to block content, block access to websites and applications comes from:

a) Section 69A of the IT Act

Section 69A grants wider powers to the Government to block or to affect the blocking of any information on six main grounds:

a) sovereignty and integrity
b) defence
c) security of the state
d) friendly relations with foreign states
e) public order
f) and preventing incitement of any cognisable offence related to the above.

It grants the power to block content to the IT Ministry if at least one of the grounds are present.

b) Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public (sic)) Rules, 2009 ("Blocking Rules").

ISSN: 2582-6433

The Blocking Rules have been enacted under Section 87 of the Information Technology Act, 2000 which empowers the Government to formulate rules of procedure. Under Section 69A, the Government is empowered to issue directions for blocking public access to information stored in a computer resource. The Rules lays down the procedures and safeguards with respect to blocking content. It outlines 16 rules which deals exclusively with the procedural aspects to be followed in blocking contents online.

c) Intermediary Guidelines

Section 2(1)(w) of the Information Technology Act 2000 defines an intermediary as

"any person who on behalf of another person receives, stores or transmits an electronic record or provides any service with respect to that record and 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 cyber cafes".

This broad definition covers social media companies, e-commerce sites, search engines etc, making it an exhaustive provision.

The Central Government notified the Information Technology (Intermediaries Guidelines) Rules, 2011 ("Intermediary Guidelines, 2011") bringing about certain obligations on intermediaries including publication of privacy policy, and user agreements. The 2011 Rules were superseded by the 2021 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Guidelines"). The 2021 Guidelines have classified the intermediaries and has also introduced the provision for Indian Computer Emergency Response Team.

UNCOVERING THE INEFFICIENCIES

The Information Technology Act is the de facto legislation governing all information technology related aspects. The Act along with the rules form its legislative framework. This framework is not short of criticisms. There are several problems and challenges related to the Information Technology (IT) Act in India, some of which are:

Lack of Clarity: The IT Act has been criticized for its lack of clarity in defining key terms, such as "obscene content," "hate speech," and "offensive material." This has led to confusion among law enforcement agencies and resulted in arbitrary actions against individuals and companies.

ISSN: 2582-6433

Violation of Privacy: The IT Act has been criticized for its provisions that allow for the interception, monitoring, and decryption of electronic communications without due process. This has raised concerns about the violation of privacy and civil liberties.

Censorship: The IT Act provides the government with the power to block access to online content in the interest of national security, public order, and other reasons. However, this has led to concerns about censorship and the violation of freedom of expression.

Inadequate Cybersecurity: The IT Act has been criticized for not adequately addressing cybersecurity issues, such as cybercrime and data protection. This has led to a rise in cybercrime and incidents of data breaches, which have resulted in financial losses and damage to reputation.

Enforcement Challenges: The IT Act has faced challenges in enforcement due to the rapidly evolving nature of technology and the internet. The lack of resources and expertise among law enforcement agencies has made it difficult to investigate and prosecute cybercrimes.

Section 69A of the Information Technology (IT) Act, 2000 in India empowers the government to block access to any information or content that it deems necessary in the interest of the sovereignty and integrity of India, defence of India, security of the state, friendly relations with foreign states, or public order.

According to this section, the government can direct any agency or intermediary to block access to any website or online content if it is found to be involved in activities that are deemed unlawful or pose a threat to national security. The government can also order the interception, monitoring, or decryption of any information transmitted through any computer resource if it is considered necessary for national security.

Under Section 69A, the government is required to follow a due process of law before taking any action. The government must provide a reasoned order to the intermediary or agency, stating the reasons for the blocking or interception of information. The intermediary or agency has the right to appeal against the order within a specified time period.

Section 69A has been controversial in India, with concerns raised about the potential for abuse of

ISSN: 2582-6433

power and violation of freedom of expression. However, the government has defended the section as necessary to safeguard national security and maintain public order.

On the constitutional Implications

The Supreme Court decision in the landmark case, Shreya Singhal v. UOI expanded freedom of speech and expression through the restrictive interpretation of constitutionally recognized grounds of restriction of free speech in the country. The Court narrowed down the unfettered application of public interest as a ground for effectively prohibiting free speech in a democratic society. While the judgment can be hailed for its exhaustive view on free speech with respect to Section 66A of the Information Technology Act 2000, the court has failed in extending the same principles to the interpretation of Section 69A. The power of the Central Government to block access to contents was upheld by the Supreme Court on the ground that it follows the constitutional standards of reasonable restrictions. The court highlighted that the fact that a website could be blocked on grounds of security and defense at par with the constitutionally recognized reasonable restrictions. According to the SC, Section 69A restricted expression on constitutional grounds of free speech. The SC decision upholding Section 69A thus allowed any kind of ban on websites as long as it is in the "interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order". The court collated the grounds under Section 69A with that of Article 19 (2) to conclude that Section 69A was based on the constitutional standards. Further, the court opined that the blocking rules 2009, ensured sufficient procedural safeguards against the Government. The court analysed that since the blocking order had to be in writing, it is subject to writ jurisdiction under Article 226.

"111. Merely because certain additional safeguards such as those found in Section 95 and 96 CrPC are not available does not make the Rules constitutionally infirm. We are of the view that the Rules are not constitutionally infirm in any manner."[1]

The Supreme Court's view of upholding the power of the executive to regulate and restrict speech, if at par with the constitutional standards is flawed. The fact that statutory language can be very broad, granting wider powers to the executive in restricting constitutionally protected rights. Constitutional safeguards act as the standards on which a statute is tested. The Court to test a

[1] *Shreya Singhal* v. *Union of India*, AIR 2015 SC 1523.

ISSN: 2582-6433

statute for its unconstitutionality shall specifically scrutinise its constitutionality based on the limits set by the constitution. Characterising unfettered power of the Executive at par with constitutional standards on the ground that the statute has incorporated constitutional safeguards through the statutory language is extremely dangerous. Even if a statute is prima facie constitutional, the power given to the Executive to interpret it, may involve encroachment into the fundamental rights of people. Article 19(2) allows reasonable restrictions to be placed through 'law'. A statute is passed after deliberation in the Parliament. But when a statute specifies powers to the Executive, such powers have to be weighed on a different scale. In this particular situation, the Executive's power to interpret the terms 'sovereignty, national security' etc, indirectly giving them the power to determine the extent of a person's freedom of speech. A direction passed by the Executive under Section 69A is partisan, it isn't made public nor debated upon. The Supreme Court decision upholding the constitutional validity of Section 69A has thus led to the culmination of the series of blocking information on the internet citing reasons of national security.

This SC judgment in 2014 therefore, heralded the passing of the 2021 Intermediary Rules which granted similar powers to Ministry of Information and Broadcasting to block websites or apps.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, colloquially called the IT Rules 2021, was notified in the Official Gazette on 25th February 2021, replacing the Information Technology (Intermediary Guidelines) Rules 2011. These Rules, in addition to the Blocking Rules 2009, grants the power to block, modify or delete any information to the Ministry of Broadcasting and Information. The IT Rules 2021 is the culmination of about three year-long deliberations. The Rules are made in lieu of the Supreme Court order in Re Prajwala Letter, wherein the Supreme Court directed Government of India to draft guidelines to eliminate child pornography and such other sexual violence videos or content and to block websites that hosted such content. Since its passing in 2021, the IT Rules have been a subject of contentious debate, quite similar to its predecessors, the IT Act and the Blocking Rules.

A recent report by Software Freedom Law Centre of India, has revealed that India has blocked 55607 websites between 2019 and 2022, 47.6% of it being blocked under Section 69A.[2] A major

[2] 'Finding 404: A Report on Website Blocking in India • Software Freedom Law Centre, India' (*Software Freedom Law Centre, India • Defender of Your Digital Freedom*, 12 January 2023) <https://sflc.in/finding-404-report-website-blocking-india> accessed 5 April 2023

ISSN: 2582-6433

part of it has been issued by the Ministry of Electronics and Communications under the Blocking Rules and the rest, around 94 of them, mostly YouTube hyperlinks have been blocked under the IT Rules 2021.

Dissecting the legality or rather the constitutionality of the saga of blocking websites, it is evident that Rules under Section 69A are constitutionally flawed. It was in Maneka Gandhi v. Union of India[3] that the apex Court laid down the golden triangle rule; any law that violates the personal liberty under Article 21 shall satisfy Articles 14, 19 and 21. The Blocking Rules 2009, do not provide an appeal process. Additionally, the opportunity of being heard is eliminated in emergency situations. Perhaps the most controversial or the most problematic aspect of the Blocking Rules is Rule 16, which guarantees secrecy or confidentiality to the entire complaints mechanism. A website, if blocked under the Rule, the reason for it removal or the complaint upon which it has been blocked shall not be made available publicly. Essentially, nobody beyond the intermediary will know about the block.

As has been held in *State of UP* v. *Raj Narain*[4], there can only be a few secrets in a Government of responsibility. Every person must have access to know about the public acts done by public authorities. The confidentiality rule thus implicates the right of general public their right to information. The SC reasoned it's decision on confidentiality by stating that when the order of the Executive blocking websites is a written and reasoned one, it is subject under Article 226. Unfortunately what the court has overlooked is the fact that an order can be challenged only if it is accessible. Even if it can be implied from the judgement that an order must be in writing that it shall be made available to the public, there is no clarity to this position till date.

Later, in the landmark judgment of *Retd. Jus. K. S. Puttaswamy* v. *UOI*[5], the Supreme Court recognised right to privacy including right to informational privacy as a part of Article 21. Justice D. Y. Chandrachud in his majority opinion argued that privacy is the right of an individual to exercise control over their personality. Referring John Locke's 'Second Treatise of Government', he echoed that lives, liberties and estates are a private preserve. Right to privacy was recognised, giving due recognition to the subset rights including informational privacy and the privacy of

[3] Maneka Gandhi v. Union of India, AIR 1978 SC 597; (1978) 1 SCC 248.
[4] AIR 1975 SC 865.
[5] AIR 2017 SC 4161.

ISSN: 2582-6433

choice.

The Court opined,

"The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the internet."[6]

The IT Rules grants social media intermediaries to decode the end-to-end encryption of information to trace the originator of it. While the Rules do not right out limit end-to-end technology, by virtue of Rule 4(2)[7], significant social media intermediaries need to trace the originator of messages. This, in effect, dilutes end-to-end encryption. End-to-end encryption prevents any kind of unauthorised access to your data, even if it is intercepted. Thus a dilution in end-to-end technology will quite possibly result in the internet being ineffective in the long run. End-to-end encryption ensures informational privacy, which has been recognised as a subset to right to privacy in the Puttaswamy judgment. The IT Rules authorising intermediaries to decode personal information of its users is especially ill-timed in this current scenario. With numerous suits filed across the world, alleging unauthorised access to data and even sale of personal data for ulterior purposes. A perfect example for this is the string of allegations against Facebook starting from 2007. In 2018, a Belgian court had ordered Facebook to stop tracking Belgian user data illegally.[8] After the 2019 data theft scandal, the Federal Trade Commission charged an hefty fine of $5 billion on Facebook. When the government decision to ban numerous applications and block websites came in the light of alleged unauthorised interference and use of data against the sovereignty of India, the provision enabling decoding information is like granting free license to misuse it. In fact, Section 84A, IT Act empowers the Central Government to develop encryption standards and methods to electronic communications.

The fact that the Rules grant discretionary power on the Secretary of Ministry of Information and Broadcasting to block information without the provision of being heard to the publisher is in direct violation of the natural justice principles. Arbitrary exercise of power goes against the fabric of

[6] ibid.
[7] Information Technology (Intermediary Rules and Digital Ethics Code) Rules, 2021 r4(2).
[8] Newcomb A, 'A Timeline of Facebook's Privacy Issues — and Its Responses' (*NBC News*, 24 March 2018) <https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651> accessed 4 April 2023.

ISSN: 2582-6433

the Constitution; arbitrariness is violative of Article 14.[9] A power granted to the Executive by virtue of a statute which is disproportionate to the purpose to be achieved is invalid in the absence of any guidelines on its exercise.[10] The test whether state action violates privacy[11] is dependent on three factors: legality, need and proportionality. The latest rules by virtue of its ambiguity allows the government overreach over people's freedoms. Article 14 of the Constitution of India guarantees reasonability and fairness.[12] It protects individuals from unfettered discretion of the government. Reading the IT Rules, there have been no limits set by the framework on the 'regulation' of digital media.

CONCLUSION

"As guardians of the Constitution, it is our duty to ensure that the exercise of power by the state is not arbitrary or oppressive but is guided by the principles of rule of law and due process. The internet has become a crucial tool for the exercise of fundamental rights, including the right to free speech and the right to privacy. Any regulation of the internet must be guided by the principles of proportionality, necessity, and legality, and must not become a tool for censorship or abuse of power." - Justice D Y Chandrachud, Indian Supreme Court.

Fundamental rights of a person are those inherent rights which enables them to express their individuality to live freely on their terms while acting as a bulwark against tyrannism and authoritarianism. Regulating the rights of a person is justifiable as long as it is for the protection of a greater good. What constitutes 'greater good' is rather subjective, and ever-changing with time. In this current era, where everything is digital, traditional outlook on fundamental rights have drastically changed. Lawmakers around the globe has realised how the traditional legislative frameworks are impotent in regulating human conduct on the internet while also balancing the safeguards over fundamental rights.

The Internet needs to be regulated, as anything else. The extent of such regulations is what determines democracy and freedom on the internet. Striking the balance between regulation and encroachment is absolutely the most crucial part of ensuring good governance. The Constitution

[9] *Maneka Gandhi* v. *Union of India,* AIR 1978 SC 597; (1978) 1 SCC 248.
[10] *District registrar* v. *canara bank* (2005) 1 SCC 496
[11] ibid (n 5).
[12] *State Of Punjab* v. *Shri Amar Singh, General* (1998) 119 PLR 498.

ISSN: 2582-6433

of India safeguards its citizens from arbitrary state-action. It scrutinises government actions to protect and promote the fundamental rights of its citizens.

The current legal framework on digital media in India which comprises of the IT Act 2000 and the two rules under it are nothing short of flawed. The broad language used and the potential for overreach by intermediaries in their implementation raise concerns about the rule of law and due process. Furthermore, the lack of transparency and accountability in its implementation has been a cause for concern. As such, the constitutionality of these regulations has been challenged in court, and the outcome of these cases will have significant implications for the future of free speech and digital rights in India.

Moving forward, there is a need for a balanced approach that considers the protection of national security while also safeguarding the fundamental rights of citizens. A transparent and accountable framework for the implementation of these regulations is crucial to ensure that they do not become tools for censorship or abuse of power.