X. INFORMATION TECHNOLOGY RULES 2021: ARE WE HEADING TOWARDS A DRACONIAN RULE?

- Shipra Tiwari and Kerti Sharma[*]

ABSTRACT

"If liberty means anything at all it means the right to tell people what they do not want to hear."

-George Orwell

Ever since the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, were passed by the government of India, they have been a topic of discussion and have faced serious criticism for being violative of fundamental rights. While, with the increase in the overall internet accessibility and increase in cybercrimes, it is without a doubt true that the digital space does need to be regulated, the regulations need to be drafted in a manner that strikes a balance between the duty of the State to protect the citizens by way of drafting laws for the purpose, and the fundamental rights of the citizens. This paper provides an overview of the provisions of the IT Rules and analyses them on the touchstone of the constitutional provisions to test their validity. The authors aim to provide an alternate perspective, by comparing the Rules with international instruments and legislations regarding the control of media and user privacy, like the Cyber Security Law of People's Republic of China, and the General Data Protection Regulation of the European Union, in order to highlight the shortcomings of the Indian framework, and suggest how the authorities could oversee digital communications and content and protect the morality and security of the nation and its people, without overstepping the constitutional boundaries or violating the rights of the citizens.

[*] The authors are fourth-year B.A. LL.B. students at National University of Study and Research in Law, Ranchi. Views stated in this paper are personal.

I. INTRODUCTION

Article 19(1)(a) of the Indian Constitution provides to all citizens the freedom of speech and expression, subject to reasonable restrictions stated under Article 19(2). The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (**"IT Intermediary Rules"** or **"Rules"**) impose additional hassles on the affected parties in terms of the restrictions. The Rules, supposedly lack teeth,[1] are unconstitutional, and are violative of Articles 19(1)(a) and 21 of the Indian Constitution, among other such constitutional irregularities. The Rules are formed to protect the interest of the parties affected by viewing or circulation of content on online platforms. Since their publication, these Rules have been the subject of condemnation by publishers and content producers. This article discusses these rules in light of their legal and constitutional validity. The

[1] Samanwaya Rautray, *Centre promises to tighten new digital media rules after Supreme Court says they lack teeth*, THE ECONOMIC TIMES (2021), https://economictimes.indiatimes.com/news/economy/policy/centre-promises-to-tighten-new-digital-media-rules-after-supreme-court-says-they-lack-teeth/articleshow/81359441.cms?from=mdr (last visited Mar 30, 2021).

recent incidents including the *boys' locker room*,[2] the *toolkit* case,[3] the abetment of suicide by an Instagram post,[4] the increased cases of obscene content, and many more such incidents highlighted the need for regulation on the online platforms circulating and publishing such objectionable information freely. The Central Government informed the Supreme Court that these rules are formed after various reported complaints and requests from the general public and politicians.[5]

II. BIRD'S EYE VIEW OF THE IT INTERMEDIARY RULES

A. Background

Owing to the increased reports of sexual harassment cases on the internet, the Apex Court in 2018, In *Re: Prajwala Letter*[6] stated in the order that the Central Government may frame necessary guidelines/Standard Operating Procedures and implement them within two weeks to eliminate child pornography, rape, and gang rape imagery, videos, sites, content hosting platforms, and other applications. Previously in 2015, pursuant to the

---

[2] Sidharth Ravi, *Bois Locker Room, a reflection of an existing mindset,* THE HINDU (2021), https://www.thehindu.com/news/cities/Delhi/bois-locker-room-a-reflectionof-an-existing-mindset/article31638044.ece (last visited Mar 30, 2021).

[3] *What is toolkit case and how it is related to farmers protest,* THE TIMES OF INDIA (2021), https://timesofindia.indiatimes.com/india/explained-what-is-toolkit-controversy-and-how-it-is-related-to-farmers-protests/articleshow/81046302.cms (last visited Mar 30, 2021).

[4] Chirali Sharma, *Girl Bizarrely Accused Of Abetment To Suicide In Bois Locker Room Case Over Instagram Post,* ED TIMES (2021), https://edtimes.in/girl-bizarrely-accused-of-abetment-to-suicide-in-bois-locker-room-case-over-instagram-post/ (last visited Mar 30, 2021).

[5] Debayan Roy, *Enacted IT Rules 2021 after receiving several complaints regarding content on OTT platforms: Centre's reply in plea for regulatory body,* BAR & BENCH (MARCH 23, 2021, 11:17 AM), https://www.barandbench.com/news/litigation/enacted-it-rules-2021-complaints-content-ott-platforms-centre

[6] In Re Prajwala Letter (Videos of Sexual Violence and Recommendations), (2018) 17 SCC 79.

directives given by the Apex Court, the government banned around 857 porn sites, particularly including child pornography.[7] The move was highly criticized on the ground of the lack of legislation to do so.[8] The Uttarakhand High Court, recently, reaffirmed the 2015 notification[9] and after giving directions, asked to ban child pornography.[10]

Further, in the *Tahseen S. Poonawalla case,*[11] the Apex Court highlighted the need for a regulation for the irresponsible and explosive messages circulated on social media platforms which lead to hatred and harming public peace.

Furthermore, the Ad-hoc committee report of Rajya Sabha about pornography on social media and its effect suggested the amendment of the Information Technology Act, 2000 (**"IT Act"**), and the Information Technology (Intermediaries guidelines) Rules, 2011 (**"2011 Intermediary Rules"**) to reduce and control the circulation of obscene content.[12]

---

[7] Karthikeyan Hemalatha, *Porn ban: People will soon learn to circumvent ISPs and govt orders, expert says*, TIMES OF INDIA, (August 03,2015), https://m.timesofindia.com/tech-news/porn-ban-people-will-soon-learn-to-circumvent-isps-and-govt-orders-expert-says/articleshow/48320914.cms

[8] PTI, *857 porn sites banned in India; Govt plans ombudsman for Net content*, FINANCIAL EXPRESS, (January 28, 2020), https://www.financialexpress.com/industry/technology/porn-ban-in-india-sparks-censorship-debate/113070/

[9] *Supra* note 7.

[10] In Re, In the matter of, Incidence of Gange Rape in a Boarding School, situated in Bhauwala, District Dehradun v State of Uttrakhand, WP No. 158/2018.

[11] Tehseen S. Poonawalla v. Union of India, (2018) 9 SCC 501.

[12] *Report of The Adhoc Committee of The Rajya Sabha To Study The Alarming Issue Of Pornography On Social Media And Its Effect On Children And Society As A Whole*, PARLIAMENT OF INDIA (January 25, 2020), https://rajyasabha.nic.in/rsnew/Committee_site/Committee_File/ReportFile/71/140/0_2020_2_16.pdf.

These are a few instances among others, that lead to the implementation of the IT Intermediary Rules for the regulation of the online platforms including OTT, intermediary, etc.

B. IT INTERMEDIARY RULES

The new IT Intermediary Rules which amended the 2011 Intermediary Rules are discussed briefly, formed under Sections 69A, 79, and 89:

I. Due Diligence by the Intermediary

Rules 4-6 implement a duty on the intermediaries to implement due diligence in their functioning. These duties are:

The rules and regulations, privacy policy, and user agreement should explain to the user not to publish, modify, upload, display any information which comes under the heads mentioned under Section 4(1)(b). The intermediary may be asked to remove any information which comes under any of the said restrictions and may be asked to provide information about the disputed content by government order. The information of the identification of the first publisher shall be given by the social media intermediary, providing messaging services like WhatsApp, to the judicial officer on the order received under Section 69 of the Act. They are required to use technology-based measures which will help in disseminating the information promoting restricted information.

A Chief Compliance Officer, a Nodal Officer, and a Resident Grievance Officer shall be appointed within three months of the publication of such rules to ensure due diligence and publish a compliance report every six months. The cyber incidents are to be reported by them to the Indian

Computer Emergency Response Team following the policies and procedures as prescribed in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.

II. Code Of Ethics and Procedure and Safeguards about Digital/Online Media

As per Section 2(w) of the IT Act, 2000, the intermediaries are simply persons who facilitate the use of the internet. It includes cyber cafes, interactive websites like WordPress, blogs, web hosts, search engines like Google, Opera, etc. The functions of intermediaries are hosting content, collecting information, evaluating scattered information, facilitating communication and information exchange, aggregating information, providing access to the internet, etc.

The Rules state that when asked by the government order, they (intermediaries) must disclose the identity of the first originator of the information on their platform. The due diligence to be followed by the intermediaries to control the content has put a significant amount of obligation on them, but at the same time has infringed the privacy of the originator and freedom of expression of the publisher.

Publishers, as per Part III of the Rules, include: (i) news and current affairs content providers, and (ii) online curated content providers, such as the Leaflet, Livelaw, etc. Therefore, publishers mean all such publishers who operate in the territory of India or conduct the systematic business activity of making their content available in India. A Publisher shall be deemed to operate in the territory of India where such publisher has a physical presence in the

territory of India.[13] The Rules cover individual content producers like bloggers as well. In response to a plea filed in the Delhi High Court on May 31, the Court issued notice to a microblogging site for non-complying with the IT Intermediary Rules.[14]

Following is the structure for grievance mechanism for the said entities:

- Level I - Self-regulation by the applicable entity;
- Level II - Self-regulation by the self-regulating bodies of the applicable entities;
- Level III - Oversight mechanism by the Central Government.

Inter-Departmental Committee and an authorized officer as the Chairperson shall be appointed by the Ministry. The authorized officer will give notice to the applicable entity of the disputed content for the reply and the content will be subsequently reviewed by the inter-departmental committee.

Also, the authorized officer is required to submit the recommendation of the Committee along with the information available to the Secretary in the

[13] Obhan & Associates, *India tightens the noose on intermediaries and social media platforms*, LEXOLOGY, (March 1 2021), https://www.lexology.com/library/detail.aspx?g=3737118d-e2bf-4377-ada2-39c7d8a36f7b.

[14] Rahul Srivastava, *On new IT rules, Twitter says it will strive to comply with applicable law in India*, INDIA TODAY, (May 27, 2021) https://www.indiatoday.in/technology/news/story/on-new-it-rules-twitter-says-it-will-strive-to-comply-with-applicable-law-in-india-1807716-2021-05-27.

Ministry of Information and Broadcasting (**"MIB"**), Government of India, and on his approval shall continue as per the directions.

III. Significant publisher and disclosure:

The significant publisher of the news and current affairs is required to notify the *broadcast seva* about the functioning and broadcasting in the territory of India for proper coordination and communication.

III. THE CONTROVERSY

The IT Intermediary Rules, essentially change the internet experience in India. They have the effect of bringing about governmental control, rather than regulation of social media, digital news platforms, and OTT platforms. Several of these rules are unconstitutional and violate the freedom of speech and the right to privacy of the users of these services.

A. Data Preservation and Traceability

Rule 3(1)(h) requires social media intermediaries to preserve data for 180 days. This information has to be preserved even after the user has deleted their account, for investigative purposes. Further, significant social media intermediaries are also required to allow their users to 'voluntarily' verify their accounts with appropriate mechanisms including their mobile numbers. The accounts so verified shall be indicated by a mark indicating such verification.[15]

[15] Rule 4(7), The Information Technology (Intermediary Guidelines and Digital Media Ethics Code), Rules, 2021, PART II—Section 3—Sub-section (i), THE GAZETTE OF INDIA, GOVT. OF INDIA, available at https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf [Hereinafter *Intermediary Guidelines and Digital Media Ethics Code 2021*].

Instances of such 'voluntary' requirements becoming practically mandatory are not unknown to India. (For instance, although initially, *Aadhar* Cards were introduced as voluntary ID proof, yet activities like banking transactions, getting a sim card, etc, were linked to it in such a way that it was difficult to proceed in normal life without an *Aadhar* Card, thus, making it mandatory in effect.) This shall also enable the social media intermediaries to collect individual data via their respective government IDs. Therefore, these requirements, in the absence of data protection laws and oversight mechanisms regarding the working of surveillance in India, shall have severe implications on the privacy and anonymity of the social media users, where just recently, the Supreme Court had stated privacy to be a fundamental right.[16]

Rule 4(2) requires significant social media intermediaries to enable the tracing of the originator of information if required by a Court of competent jurisdiction or competent authority under Section 69 of the IT Act, thus putting an end to the system of end-to-end encryption if required.

End-to-end encryption (**"E2EE"**) is a technique employed by messaging apps where only the communicating parties have access to the messages exchanged between them. It prevents the internet service providers and other third parties from snooping into the information shared by the users. Social media platforms like WhatsApp use the system of end-to-end encryption, which allows the users to keep the integrity of their messages intact, while they communicate via the internet, which is otherwise considered an insecure public channel. Although the rules provide that such order shall only be passed for prevention, detection, investigation, prosecution, or

[16] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 641.

punishment of certain offenses that are specifically stated, the category of 'public order' is relatively broad and can be used to exercise arbitrary and whimsical actions. No doubt, this provision shall help in reducing the cases, and identifying the culprits of serious cyber offenses, but, at the same time, can be used to identify political dissenters and may be a threat to freedom of speech and right to dissent. This is contrary to the opinion of Delhi High Court, expressed in *Maqbool Fida Husain* v. *Rajkumar Pandey*[17] as,

> In a real democracy, the dissenter must feel at home and ought not to be nervously looking over his shoulder fearing captivity or bodily harm or economic and social sanctions for his unconventional or critical views. There should be freedom for the thought we hate. Freedom of speech has no meaning if there is no freedom after speech. The reality of democracy is to be measured by the extent of freedom and accommodation it extends.

B. 'Self-Regulation' and Content Blocking

The IT Intermediary Rules also regulate digital news media and OTT platforms, which before this, in the 2011 Intermediary Rules, were left out. The digital news media and OTT platforms are required to adhere to a Code of Conduct, provided in the Appendix to these rules. To ensure compliance with this code of conduct, the three-tier system discussed above includes a grievance redressal and appeal mechanism. This consists of a Grievance Officer at the first tier, the self-regulating body at the second tier, and an Inter-Departmental Committee constituted by the Ministry at the third tier. Under this mechanism, if the grievance officer is unable to provide the complainant

[17] Maqbool Fida Husain v. Rajkumar Pandey, 2008 SCC OnLine Del 562.

with a sufficient response, the complainant may appeal to the self-regulating body at tier II.

Now, as per Rule 11, this self-regulating body is supposed to be an independent body, headed by a retired judge of the Supreme Court or of a High Court, who shall be appointed from a panel prepared by the Ministry, and have other, not more than six members, from the field of media, broadcasting, technology, and entertainment. In case the applicable entity fails to comply with the guidance and advisory of the self-regulatory body within the stipulated time, the body may refer the matter to the Oversight Mechanism constituted under Rule 12. This Oversight Mechanism is the Inter-Departmental Committee, consisting of representatives from various ministries under the government and other organizations, including domain experts, that it may decide to include in the Committee, with an 'Authorized Officer' who shall be a member of the Ministry, designated by the Ministry, as its Chairperson. Therefore, while on the face of it, this mechanism may appear to be quite 'self-regulatory' with minimal government interference, on a deeper look, it is much more than that, keeping in mind the degree of control that the Ministry has over appointments in the 'self-regulating body'.

Furthermore, the action that can be taken by this Committee includes censoring the platform, asking the platform to reclassify ratings, and action under Section 69A(1) of the IT Act, on the mere ground that the Authorised Officer, on the recommendation of the committee, is satisfied that there is need for taking such action. Such action may be blocking concerning the content, subject to Section 69A(2), for reasons to be recorded in writing. Section 69A(2) provides that the procedure of such blocking, and the safeguards available against it, maybe as prescribed. This procedure has been prescribed

under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**"2009 Rules"**).

The Apex Court, in the case of *Shreya Singhal v. Union of India*,[18] not only declared Section 66A of the Act as unconstitutional but also upheld the constitutional validity of Section 69A, which was also challenged in the case. The reason provided by the Court for its decision was twofold. The Hon'ble Court noted that firstly, Section 69A is narrowly drawn, and contains several safeguards, unlike Section 66A, and secondly, the necessity envisaged in the section is on the grounds that are same as those envisaged under Article 19(2) of the Constitution of India, i.e. 'in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order, or preventing incitement to the commission of any cognizable offence'. However, what the Hon'ble court might have overlooked, was the fact that while Article 19(2) of the Constitution lays down grounds on the basis of which the Parliament and the State Legislature are allowed to pass laws that restrict the freedom of speech and expression of the citizens, what Section 69A allows on the similar grounds is for the government, or an officer authorised by the government to interpret the grounds such as security of the State, etc, as per their own understanding, and direct blocking of content. The reasonable restrictions provided under the Constitution are quite subjective. The difference between the passing of a law in the Parliament, and the issuance of directions by an officer is that while a bill is heavily debated in the Parliament before it becomes a law, a

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

governmental guideline may be based solely on the whims and fancies of the authority.

Another anomaly in the blocking procedure is found under the 2009 Rules. Framed under Section 69A(2) of the IT Act, these rules provide the procedures and safeguards concerning blocking. According to the 2009 Rules, every request for blocking is supposed to be reviewed by the review committee before action is taken, the review committee comprises of designated officers and representatives from the Ministry of Law and Justice, Information and Broadcasting, Home Affairs, and the Indian Computer Emergency Response Team.[19] The rules also provide the stakeholders with the opportunity of hearing, and for deliberations by a reviewing committee, before any decision for blocking is made, as a safeguard against unwarranted blocking. However, under Rule 9, the competent authority can direct the intermediary to block access by the public to any information for forty-eight hours, before the notice is deliberated upon by the review committee, in 'emergency cases'. What constitutes an emergency is not defined and is left to be interpreted as per the wisdom of the relevant authorities. The rules also provide for the Department to record in writing the reasons for the issue of the direction of blocking of content, which may, as noted in the *Shreya Singhal* case, 'be assailed in a writ petition under Article 226 of the Constitution'.[20] Although this provision is supposed to be a safeguard against whimsical actions, the forty-eight hours of

[19] Rule 7, The Information Technology (Procedure and safeguards for Blocking for access of Information by Public) Rules, 2009, PART II—Section 3—Sub-section (i), THE GAZETTE OF INDIA, GOVT. OF INDIA, available at https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28%20Procedure%20and%20safeguards%20for%20blocking%20for%20access%20of%20information%20by%20public%29%20Rules%2C%202009.pdf.

[20] *Supra* note 18.

unreviewed blocking, and the time taken to dispose of a writ petition, are enough to curb the voices of political dissenters or social movements that do not suit the government's interests. It is for these reasons that the constitutional validity of Section 69A and the action taken under the 2009 Rules, seem questionable.

This provision, and the misuse that may ensue thereof, becomes relevant in light of the Supreme Court judgment in *Indibly Creative (P) Ltd. v. the State of W.B.,*[21] wherein the Court stated that,

> The views of the writer of a play, the meter of a poet, or the sketches of a cartoonist may not be palatable to those who are criticized. Those who disagree have a simple expedient: of not watching a film, not turning the pages of the book, or not hearing what is not music to their ears. The Constitution does not permit those in authority who disagree to crush the freedom of others to believe, think and express.

At the point in time when India is not only a consumer but an active creator of original digital content released via OTT platforms, the opportunity could be used to monetize the growing OTT trend across the globe. In light of the South Korean model, where the government systematically works to realize the full potential of the *Hallyu* export market, building on USD 13.4 billion in export sales throughout the world in 2018-19, the increasing restrictions on the Indian content on these OTT platforms are not only a blow to the artistic freedom of content creators, and freedom of speech, but also a lost economic opportunity.[22]

---

[21] Indibly Creative (P) Ltd. v. State of West Bengal, (2020) 12 SCC 436.

[22] *Korean Film Industry Generated USD 18.45 Billion in 2018*, MOTION PICTURE ASSOCIATION (December 12, 2019), https://www.mpa-apac.org/press/korean-film-industry-generated-usd-18-45-billion-in-2018/.

C. Constitutionality of the Rules

In addition to the above, the concern is that the rules have no legislative backing in regulating said media, this is exercising powers beyond the scope of the parent legislation. It has been held by the Supreme Court in the *State of Karnataka and Another v. Ganesh Kamath & Ors*[23] that, "It is a well-settled principle of interpretation of statutes that conferment of rulemaking power by an Act does not enable the rule making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent therewith or repugnant thereto." A combined reading of Section 79(2) read with Section 89(2)(zg) makes it clear that the power of the Central Government is limited to prescribing guidelines related to the due diligence to be observed by the intermediaries while discharging its duties under the IT Act. However, the IT Intermediary Rules have imposed additional requirements and widened the ambit of requirements to be fulfilled by the intermediary.

Thus, the Rules extend the scope of the responsibilities of the intermediary and are ultra vires as an intermediary can act only after receiving an order from the court or a notification from the appropriate government or its agency. The intermediary is not required to exercise its discretion regarding the material which is to be removed or disabled.

Also, as per the Rules, the intermediaries are liable to follow the due diligence provisions which are similar to the provisions of due diligence attached in the 2011 Intermediary Rules. These principles under Rule 3(4) of the 2011 Intermediary Rules, were read down in *Shreya Singhal v. Union of*

[23] State of Karnataka and Another v. Ganesh Kamath & Ors., (1983 SCR (2) 665.

India,[24] to the extent that an intermediary would only be required to disable information that would be relatable to Article 19(2) of the Constitution.

Similarly, the IT Act does not provide any classification of intermediaries. Section 2(1)(w) of the Act defines an intermediary as "any person who on behalf of another person receives, stores or transmits that 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." Thus, all intermediaries are treated as a single undifferentiated entity that are subject to the same responsibilities and obligations. However, the new Rules have set up different categories of intermediaries like social media intermediaries,[25] and significant social media intermediaries.[26] This classification, in turn, subjects social media intermediaries with an extra set of obligations, and the scope of significant social media intermediaries' responsibilities also stands expanded. These new responsibilities find no basis in the parent act that does not classify intermediaries into different types.

Section 87(1) and Section 87(2)(z) and (zg), under which the Rules have been prescribed, do not give the Central Government the power to amend the definition of intermediaries as stated in the IT Act, or create any such classifications as the Rules have already done. Therefore, once again, it can be evidently seen that the Rules have gone beyond the parent legislation.

[24] *Supra* note 18.
[25] Rule(2)(1)(w), Intermediary Guidelines and Digital Media Ethics Code 2021
[26] Rule(2)(1)(v), Intermediary Guidelines and Digital Media Ethics Code, 2021.

Secondly, Section 79 of the Act provides that subject to clauses (2) and (3) the intermediary shall not be liable to any content of the third-party hosted or published by it. Thus, providing a clear safeguard to the intermediary. Further, Section 79(2) of the Act states the grounds under which the said safeguard will be availed to the intermediary and Section 79(3) mentions the grounds when the intermediary may be held liable if the content is not taken down when they have the knowledge of its unlawfulness.

In *Shreya Singhal v. Union of India*,[27] the Supreme Court read down Section 79(3)(b) to mean that an "intermediary upon receiving actual knowledge from a court order or on being notified by the appropriate government or its agency that unlawful acts relatable to Article 19 (2) are going to be committed, fails to expeditiously remove or disable access to such material."

Thus, requiring the intermediary to apply their own mind in the regulation of data goes against the Court's interpretation in the *Shreya Singhal* judgment.

Also, as per the Rules, the responsibility of administering Part II of the Rules lies with the Ministry of Electronics and Information Technology. As per the Allocation of Business Rules, 1961, Digital Media is under the purview of the Ministry of Information and Broadcasting, while the entry 'Matters relating to Cyber Laws, administration of Information Technology Act 2000 (21 of 2000) and other IT related laws', which would include IT Act, 2000 and framing of rules under the said Act, would fall under the MeitY. While it may be argued that Digital Media, concerning the processing of content on digital

[27] *Supra* note 18.

media by publishers can be covered as an aspect of the wide scope of 'cyber crimes', digital media still falls under the ambit of Information and Broadcasting and any legislation or delegated legislation in the form of rules, under this legislation, can be enacted by the MIB. Therefore, the MeitY cannot legislate upon digital media as a delegate or otherwise, since it is the job of the MIB. Neither can the MIB, under the IT Act, act as a delegate and administer a part of it, since it is an accepted principle of law that what cannot be done directly, cannot be done indirectly. To regulate digital media, the MeitY would have to pass a law in the Parliament, under which it may require the MIB to consult the MeitY and other ministries, but the enacting body would still be the MIB. Not passing the law amounts to an abdication of the Parliament's legislative duties.

The Supreme Court, in various cases, has stated that if a rule goes beyond the rule-making powers conferred by the statute, and hence, the rule should be declared ultra vires. The basic test is to determine and consider the source of the power conferred upon the rule.[28] For a rule to have the effect of a statutory provision, two requirements should be fulfilled. Firstly, the rule must conform to the provision of the statute under which it is framed, and secondly, it must also come into the scope and purview of the rule-making power of the authority making the rule. If any one of the above two conditions is not fulfilled, the rule shall remain void.[29] The conferment of rule-making power by an Act does not enable the rule-making authority to make a rule which travels beyond the scope of the enabling Act or which is inconsistent therewith or repugnant thereto.[30] Hence, it is clear that the rules are beyond

[28] Union of India and Ors. v. S. Srinivasan, (2012) 7 SCC 683.
[29] General Officer Commanding-in-Chief v. Dr. Subhash Chandra Yadav, (1988) 2 SCC 351.
[30] State of Karnataka and Anr. v. S Ganesh Kamath and Ors., (1983) 2 SCC 402.

the scope of the purview of the IT Act and are ultra vires the parent act, therefore, are liable to be challenged in court on this ground.

IV. NON-COMPLIANCE OF THE RULES: THE OUTCOME

The tussle between Twitter India and the Indian government over the compliance of the Rules was all over the news in recent times, with speculations of Twitter facing a potential ban in the country and the platform's eventual loss of intermediary status.[31] The implication of losing the status of an intermediary can be understood by an analysis of the provisions of the IT Act, and Rule 7 of the IT Intermediary Rules.

The IT Act provides a safe harbor to the intermediaries in the form of Section 79. The section states that an intermediary shall not be made liable legally or otherwise, in the context of any third party communication, information, or data hosted on its platform, provided that the function of the intermediary is limited to providing access to a communication system over which such third party information is transmitted or temporarily stored or hosted; that the intermediary does not initiate the transmission or select the receiver or select or modify the information contained in such transmission; and that the intermediary follows due diligence in the discharge of its duties under the Act. Further, an intermediary is exempted from the protection of the safe harbour provision if it has, in any way, conspired, abetted, aided, or induced the commission of the unlawful act; or if upon the knowledge or upon

[31] ANI, *Twitter loses intermediary status over non-compliance with new Rules: RPT*, BUSINESS STANDARD (June 16, 2021), https://www.business-standard.com/article/news-ani/twitter-loses-its-status-as-intermediary-platform-in-india-due-to-non-compliance-with-new-it-rules-121061600199_1.html.

being notified by the government that any data being hosted on the platform that the intermediary controls, is being used to perform the unlawful act, the intermediary fails to remove or block access to said material. The Act also provides that protection shall not be available to an intermediary in case it fails to observe any guidelines prescribed by the Central Government in this and 9(3), which adhere the digital news media and online publishers to adhere to a code of ethics prescribed by the Rules, being violative of Article 19(1)(a) of the Constitution. The Court noted that the Rules are 'manifestly unreasonable' and against the right to free speech of the citizens.[32]

V. INTERNET FREEDOM IN CHINA: TREADING A DANGEROUS PATH?

China, unlike democracies that try to advance the freedom and equality granted to its citizens, does not provide the same extent of freedom to its citizens. Deeply concerned with the protection of the monopoly of power, the Chinese Communist Party believes that giving the citizens as much freedom as in the democratic nations would threaten this monopoly. Specifically, over the past year, the country has been subject to a lot of criticism, both domestically and on an international level, after its endeavors to restrict the internet coverage of the coronavirus outbreak. Although these restrictions are a lot stricter and extensive in China, a comparative analysis of the recent incidents in China and India shows concerning similarities.

[32] Sharmeen Hakeem, *IT Rules Manifestly Unreasonable; Bring Chilling Effect on Free Speech: Bombay High Court Stays Digital Media Code of Ethics Enforcement*, LIVELAW (August 14, 2021), https://www.livelaw.in/top-stories/it-rules-2021-manifestly-unreasonablebring-chilling-effect-on-free-speech-bombay-high-court-179590

For instance, in 2019, the 30th anniversary of the Tiananmen massacre, the Hong Kong protests, and an ongoing trade war with the United States of America were among the most heavily censored topics, taking information control on the internet to unprecedented levels in China. This resulted in large-scale content removal, website closures, and social media account deletions of people who spoke up on these topics online.[33] This brings to mind the withholding of around two hundred fifty Twitter accounts in India, including accounts of persons tweeting and retweeting about the ongoing farmers' protests in the country, on the request of the MeitY under Section 69A of the IT Act.

Further, it has been alleged that Chinese technology companies actively aid government surveillance over the citizens by developing mandatory and semi-mandatory propaganda and public health mobile applications that were found to be collecting user data and passing it on to the government authorities.[34] In India, during the coronavirus outbreak, the government made the installation of the *Aarogya Setu* mobile application mandatory, to trace and track the virus. However, concerns were raised over the issue of breach of users' privacy. In a review of twenty-five virus tracing apps, the Massachusetts Institute of Technology stated that the *Aarogya Setu* App "collects far more data than it needs". Although the government claims that the data collected by the application would not be viewed by anyone, other than those who are necessary, privacy preachers state that what is done with

[33] Sarah Cook & Mai Truong, *China's Internet Freedom Hit a New Low in 2019 and The World Could Follow*, THE DIPLOMAT (November 19, 2019), https://thediplomat.com/2019/11/chinas-internet-freedom-hit-a-new-low-in-2019-and-the-world-could-follow/.

[34] China Freedom on the Net 2020, FREEDOM HOUSE, https://freedomhouse.org/country/china/freedom-net/2020, (last visited March 28, 2021).

the collected data is not known. Even the provisions of the new Rules make enough room for privacy violations and increased surveillance over the citizens. For instance, the provision for enabling the tracing of the originator of a message and the preservation of data for 180 days along with verification of user's social media accounts, under Rules 4 and 3 respectively. Along with allowing the government to peek into user communications on messaging applications, they also give the authorities access to the locations from which the messages are sent. Such rules not only pose a serious concern over the protection of the user's privacy but also enable unwarranted surveillance over them, which would be a violation of the Fundamental Rights guaranteed by the constitution.

The instances of the Chinese government shutting down internet services are not few. One of the longest such shutdowns was back in 2009, when authorities imposed a ten-month-long internet shutdown in Xinjiang, after ethnic violence in the capital Urumqi.[35] Similar instances of internet shutdown are not uncommon in India as well. For instance, the frequent internet blackouts in Jammu and Kashmir after the killing of Burhan Wani, and after the abrogation of the provisions of Article 370 of the Indian Constitution. A more recent example includes the internet shutdown in Haryana in the wake of the protest against the agriculture reforms- all this after the Supreme Court held in *Anuradha Bhasin and Ors. v. Union of India,*[36] that the freedom of speech and expression through the medium of the internet is an

[35] Chris Hogg, *China restores Xinjiang Internet,* BBC NEWS (May 14, 2010), http://news.bbc.co.uk/2/hi/asia-pacific/8682145.stm.
[36] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637.

integral part of Article 19(1)(a) and any restriction imposed thereof should be following Article 19(2) of the Constitution of India.

Chinese authorities, specifically after the Cybersecurity Law of 2017, pressure internet companies to actively censor content according to existing regulations or risk suspension, backlisting, closure, fines, or even prosecution of relevant personnel.[37] The country also made it mandatory for telecommunication companies to obtain facial scans of new internet or mobile phone users as part of the verification process a requirement that can also be found in the IT Intermediary Rules.[38]

Although the restrictions and regulations on the internet are admittedly more strict and extensive in China, the abovementioned recent incidents in India, along with the imposition of the new rules, are enough to instill a justified fear in the citizens of India, that the democracy is following up the path set by the Chinese government by increasingly curtailing freedom of speech and expression and privacy breaches through increased regulation of and interference with social media, OTT platforms, digital news media, and the internet in general.[39]

It is here that the new Rules come into the picture. The IT Intermediary Rules, under Rule 7, state that in instances where an intermediary fails to comply with the rules, the protection granted under Section 79 shall not be

---

[37] Cybersecurity Law of the People's Republic of China, 2017, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[38] AFP, *China Introduces Mandatory Face Scans for Phone Users*, THE HINDU (December 1, 2019), https://www.thehindu.com/news/international/china-introduces-mandatory-face-scans-for-phone-users/article30131810.ece.

[39] The Information technology Act, 2000, No. 21, Acts of Parliament, 2000 (lndia), § 79(2)(c).

applicable to them, and said intermediary would be liable under any law in force, including the IT Act and the Indian Penal Code, 1860.

Thus, the loss of intermediary status, which is resultant of non-compliance with the Rules, leads to the loss of protection granted to intermediaries under Section 79 of the Act. This leads to the intermediary being considered the publisher of all content on the platform and imposes upon it the liability for all content posted on its platform if such content is deemed unlawful.

VI. CHALLENGES TO THE RULES

Considering all the above, it is only understandable and expected that the Rules have been challenged in Courts by various platforms that it claims to cover, to settle the applicability and remove the ambiguity in them. Google, for example, appealed the Delhi High Court against an order of a single judge bench on the ground that it is classified as a social media intermediary and is required to comply with the Rules, whereas being a search engine, it considers itself not a subject to such compliances.[40]

Petitions have also been filed by the Wire,[41] the Quint,[42] etc., challenging the provisions of the Rules regulating digital news media and OTT

[40] Staff Reporter, *New IT Rules Don't Apply to Us, Google Tells Delhi High Court,* THE HINDU (July 2, 2021), https://www.thehindu.com/news/national/google-tells-hc-new-it-rules-not-applicable-to-its-search-engine/article34704908.ece.
[41] Livelaw News Network, *The Wire and Others move Delhi HC Challenging IT(Intermediary Guidelines and Digital Media Ethics Code), Rules, 2021*, LIVELAW (March 8, 2021), https://www.livelaw.in/top-stories/the-wire-moves-delhi-hc-challenging-itintermediary-guidelines-digital-media-ethics-coderules-2021-170905.
[42] Karan Tripathi, *Chilling Effect on Media': The Quint Challenges New IT Rules*, THE QUINT (March 19,2021), https://www.thequint.com/news/law/the-quint-challenges-new-it-rules-before-delhi-hc.

platforms, claiming that the rules impose upon them unreasonable restrictions that violate their freedom of speech and expression. A similar challenge has been made by the Press Trust of India as well.[43]

Even WhatsApp moved to the Delhi High Court against the traceability clause that requires it to break the end-to-end encryption that secures user communications, on the ground of it being violative of the people's right to privacy.[44]

Here, it becomes pertinent to note that the Bombay High Court, in a plea filed by AGIJ Promotion of Ninteenonea Media Pvt. Ltd., the company that runs the legal news portal the Leaflet, stayed the application of Rule 9(1) of the IT Intermediary Rules.

With the rapid pace of technological development and the internet becoming an indispensable part of the lives of people everywhere, the issue of the protection of user information and privacy, as well as the freedom of speech online has been a concern all around the world, and legislations regulating said aspects of the internet experience have been passed. Poland, for instance, proposed a law that criminalizes self-regulation by intermediaries. The country believes that the removal of content and regulation of free speech on social media platforms is not a function that the intermediaries should exercise, thus advocating for a 'free and transparent'

---

[43] Sparsh Upadhyay, *Press Trust of India Moves Delhi High Court Challenging IT Rules 2021, Notice Issued*, LIVELAW (July 8, 2021), https://www.livelaw.in/news-updates/press-trust-of-india-delhi-high-court-challenging-it-rules-2021-notice-issued-177053.

[44] *Delhi Court Adjourn to August 27 WhatsApp's Plea Challenging Traceability Clause under New IT Rules as Violative of Right to Privacy*, LIVELAW (July 30, 2021), https://www.livelaw.in/news-updates/delhi-high-court-adjourns-whatsapps-plea-against-traceability-clause-under-new-it-rules-178461.

internet policy. Failure to restore deleted content and accounts could cost the intermediaries up to $13.4 million by way of fines.[45]

While India is enabling government-sanctioned privacy breaches by requiring intermediaries like WhatsApp to break their end to end encryption, the European Union's General Data Protection Regulations (**"GDPR"**) requires the Information Commissioner-an independent regulator, to make sure that the personal data of the citizens are protected and their privacy is maintained under transactions that occur between the member states, by way of granting the Information Commissioner various responsibilities[46] and powers[47] like ordering the data controller or processor to inform the data subject about personal data breach, carrying out data protection audits, warning the controller that the intended data processing is likely to breach the provisions of GDPR, etc. The same has also been reiterated in the UK Data Protection Act, 2018.[48] Further, the GDPR provides that where personal data of users is stored, it must be done so in a way that allows the identification of data subjects for a period no longer than is necessary for accomplishing the purpose for which the data was so processed.[49] The only case in which personal data can be stored for a longer period is in instances where it relates to the public interest, or scientific or historical research purposes, or statistical purposes, subject to technical and organizational measures as prescribed by national laws. The European Union Regulation also provides the data subjects

[45] Adam Easton, *Poland proposes social media Free Speech Law*, BBC NEWS (January 15, 2021), https://www.bbc.com/news/technology-55678502.
[46] Article 57, L119, 4 May 2016, General Data Protection Regulation, 2016.
[47] Article 58, L119, 4 May 2016, General Data Protection Regulation, 2016.
[48] Article 115, UK Data Protection Act, 2018, available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.
[49] Article 5, L119, 4 May 2016, General Data Protection Regulation, 2016.

the right to object to the processing of personal information.[50] Processing includes collection, recording, storage, etc.[51] Under Article 21 of GDPR, the data subject can object to such processing at any stage, and the controller shall no longer proceed with the processing unless they demonstrate such 'compelling legitimate grounds' under which the processing overrides the interests, freedoms, and rights of the data subject, except when the processing is for direct marketing purposes, the controller shall, in no case, proceed with such purposes. In this light, the storage of user information for a period of one hundred and eighty days, irrespective of the purpose for which the information was collected under the IT Intermediary Rules, seems excessive. GDPR also emphasizes the lawfulness of data processing. It states that the purpose of such processing should be explicitly informed to the user, and be determined at the time of collection of the data.[52] It also categorically lays down the purposes for which processing would be considered lawful.[53] Although the Indian legislation does require the consent of the user to be taken before any processing, it does not, unlike the GDPR, define what consent means.

It must be kept in mind that while foreign legislations like GDPR state the right to protection of personal data as one of its objectives, the IT Act, and the Rules were not drafted for this purpose.[54] All this further strengthens the argument for the need for a data protection law in India.

VII. CONCLUSION

[50] Article 21, L119, 4 May 2016, General Data Protection Regulation, 2016.
[51] Article 4(2), L119, 4 May 2016, General Data Protection Regulation, 2016.
[52] Recital 39, L119, 4 May 2016, General Data Protection Regulation, 2016.
[53] Article 6, L119, 4 May 2016, General Data Protection Regulation, 2016.
[54] Article 1, L119, 4 May 2016, General Data Protection Regulation, 2016.

India is the world's largest democracy and in a time where democracies around the world are aiming to expand the scope of their citizen's freedoms and rights, the IT Intermediary Rules, are on the receiving end of large-scale outrage in the nation. It is clear from the provisions of these rules that the government has missed out on an opportunity for further betterment of the democratic rights of internet users. With the jurisprudence of rights of individuals on the internet evolving rapidly, the introduction of these intermediary rules, with their immoderate regulations and government interference, is like taking two steps back in catching up with this development.

Admittedly, the rise of internet coverage in the country has led to increased cases of illegal activities through the internet, including sexual harassment, pornography, and the spread of messages and content igniting communal violence. But in the absence of regulatory mechanisms, and due to the excessive interference on OTT platforms, we are of the view that these rules have far-reaching negative implications on the right to privacy, freedom of speech and expression, and access to information, alongside the above-mentioned constitutional irregularities.

While we agree that there is an urgent requirement for better regulation of these aspects of cyberspace, how these rules have been brought about, as well as their substance, beg urgent judicial review. What is required is the introduction of revised rules as the bill for deliberations in the Parliament and its subsequent enforcement as a law. The need for a data protection law becomes more highlighted in these circumstances. The formation of a regulatory body, to make sure that the data collected in compliance with such rules are used only for such verification purposes as mandated by the law, to

prevent an unwarranted breach of citizen's privacy is also vital. The authorities should be held accountable for the content takedowns or website blocks made at the request of the government, making the overall legislation more transparent, and ensuring that unwarranted and arbitrary actions are not taken to promote the government's propaganda and suppress any difference in opinion. Since time is of the essence in the spread of any political movement, cutting public access to any information or opinion of a political nature even for a few days could act as a tool to curb fair criticism or opposition of the government's policies. Inspiration could also be taken from international legislation like the European Union's GDPR, to ensure better protection of personal data and the fundamental right to privacy. The government could also set up a body specifically for monitoring and reporting misinformation trends and hate comments online. This would not only reduce the burden on the intermediaries but would also not require them to apply their minds in self-regulating the content posted on their platform.