REGULATING THE DIGITAL PUBLIC SQUARE: A CRITICAL ANALYSIS OF THE INFORMATION TECHNOLOGY RULES, 2021 AND INTERMEDIARY ACCOUNTABILITY IN INDIA

Anannay Singh Dhankhar, Dr. B.R. Ambedkar National Law University, Sonepat

ABSTRACT

With the increasing adoption of internet access in India, it has resulted in significant transformations in terms of how people communicate, conduct businesses, and consume the media. However, it has posed some critical challenges in the form of cyberbullying, non-consensual private image postings, and propagation of misinformation on the internet. As a means of regulating these challenges, the Central Government has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 through the exercise of its powers under Section 87 of the Information Technology Act, 2000.

In this research paper, the statutory legal shield provided by Section 79 of the Information Technology Act, 2000, termed as the Safe Harbour provision, will be considered in relation to its design and practical implications of the Information Technology Rules, 2021. It also provides a detailed analysis of changes brought to the 2021 Rules by subsequent amendments of 2022 and 2023. The paper examines the classification of large social media intermediaries, their obligations under these Rules, legal and technical complexities of determining the originating person of encrypted communications under Rule 4(2),The law and its implications for digital news sites and video streaming websites such as Netflix and Amazon Prime is analyzed.

This research also analyses the governmental appellate system in the form of Grievance Appellate Committee and the constitutional issues related to the State-owned Fact Check Unit, which was rejected by the Bombay High Court in the case of Kunal Kamra. This study analyses how this law affects the safety online, personal privacy under Article 21 and freedom of speech under Article 19(1)(a).

1. Introduction

For the first two decades of the existence of the internet in India, web enterprises operated under the concept of neutrality. Internet service providers, web hosting providers, search engines, and early social networks declared that they were merely technical conduits. Since they just delivered data packets between individuals without making any decision about whom to deliver the packets to or modifying their content, they did not have any liability for user-generated content.[1]

In order to ensure the development of the immature industry without being destroyed by legal actions, Parliament included Section 79 of the Information Technology Act of 2000.[2] In accordance with this provision, a platform or website could be protected against both criminal prosecutions and civil lawsuits for any user-uploaded or shared third-party content, provided that the platform met the basic requirements imposed by the state.[3]

With technological progress, the nature of the internet changed significantly. No longer were platforms just technical pipelines; they began implementing algorithms to track the users' activity and to push them content that would engage them for as long as possible.[4] Although this approach accelerated the interaction and content dissemination process, it also introduced significant dangers to the everyday life:

- Theft of personal photographs, non-consensual images, and deep fakes (fake videos created using computer algorithms) have been uploaded without the consent of the person;[5]
- False information was rapidly disseminated, resulting in real-life riots and physical assaults;[6]
- Child pornography and other illegal content was circulated on open networks;[7] and

[1] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1, 14–18 (India).
[2] Information Technology Act, 2000, § 79, No. 21, Acts of Parliament, 2000 (India).
[3] Information Technology (Intermediaries Guidelines) Rules, 2011, Gazette of India, pt. II sec. 3(i), G.S.R. 314(E) (Apr. 11, 2011).
[4] Tarunabh Khaitan & Farrah Ahmed, The Architecture of Platform Governance and Freedom of Speech, 42 Melb. U. L. Rev. 891, 897–903 (2019).
[5] Parliamentary Standing Committee on Information Technology, *Review of Mechanisms to Curb Fake News and Misuse of Social Media Platforms*, Fifty-Second Report, Seventeenth Lok Sabha, Lok Sabha Secretariat, New Delhi (2020).
[6] Vidhi Centre for Legal Policy, *Regulating Intermediaries: Designing a Robust Liability Framework for India*, Report for the Ministry of Electronics and Information Technology, at 23–29 (2019).
[7] In re: Prajwala, (2018) 18 S.C.C. 544, 549–552 (India).

- Social media organizations have started blocking the account and removing posts of the users without providing any form of hearing to the person.[8]

In Shreya Singhal v. Union of India case, a landmark judgment was pronounced by the Supreme Court of India in 2015 to deal with bad content on the platforms.[9] The judgment was given that internet platform is obligated to remove such content only when there is a court order or an order issued by a government officer in charge.[10]

Even though this judgment aimed to prevent corporations from curtailing speech in a hurry, there wasn't an easy means for common people to take recourse. In case, common people found themselves victims of leaking of manipulated photos and personal data, they often found themselves in a fix owing to lack of funds and legal assistance to approach courts for an interim injunction.[11]

Meanwhile, publishing of news and entertainment content shifted to digital platform. Press Council of India was responsible for regulating print media and cable television channels came under the purview of Programme Code under Cable Television Networks (Regulation) Act, 1995. However, there was no proper regulatory mechanism for digital media platforms such as Netflix, Hotstar and Amazon Prime Video.[12]

Thus, to address both these issues, the Ministry of Electronics and Information Technology (MeitY) along with the Ministry of Information and Broadcasting (MIB) issued Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on February 25, 2021 superseding earlier guidelines of 2011.[13]

The 2021 Rules established a dual structure as follows:

- **Part II (Rules 3 to 7)**, under the jurisdiction of MeitY, determines the regulatory requirements for social media intermediaries and messaging intermediaries. It demands

[8] Chinmayi Arun, Gatekeeper Governance: The Human Rights Responsibilities of Digital Platforms, 32 Harv. Hum. Rts. J. 245, 252–257 (2019)
[9] Information Technology Act, 2000, § 79(3)(b).
[10] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1, 84–89.
[11] Rishab Bailey et al., *Intermediary Liability in India: A Need for Fresh Thinking*, National Institute of Public Finance and Policy, Working Paper No. 301, at 14–18 (2020).
[12] Press Council Act, 1978, No. 37, Acts of Parliament, 1978 (India); Cable Television Networks (Regulation) Act, 1995, No. 7, Acts of Parliament, 1995 (India).
[13] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(i), G.S.R. 139(E) (Feb. 25, 2021)

that platforms appoint local officers in India, develop grievance redressal mechanisms, file periodic reports on content removal, and provide a traceability mechanism for messages.[14]

- **Part III (Rules 8 to 19)**, under the jurisdiction of the MIB, introduces an ethical code for digital news websites, an age-rating scheme for video streaming services, and a three-tier complaints mechanism for readers and viewers.[15]

The government amended the regulations twice again. In October 2022, the government created Grievance Appellate Committees consisting of government appointees to allow users to contest their account bans.[16] The government also amended the 2021 Rules in April 2023 to include online real-money gaming platforms and establish a government Fact-Check Unit to report misinformation regarding the Central Government.[17]

As a result of all the above-listed measures, the 2021 Rules have become one of the most controversial government orders in Indian legal history.

2. Research Problem

The primary problem addressed in this research paper is the direct contradiction between the attempt to make internet corporations comply with the laws of India and the need for protection of the constitutional rights of its citizens.

The IT Rules, 2021 was a necessary solution to the real problem – large international technology companies did not pay attention to the citizens' complaints about internet harassment and could not protect their rights in any way. To address that problem, the government linked the immunity of the platform under section 79 with the compliance with all of the strict rules.

Such regulatory framework gives rise to three major legal issues:

First, it puts private corporations in the position of online judges. In case of the possibility of

[14] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3–7.
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 8–19.
[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022, Gazette of India, pt. II sec. 3(i), G.S.R. 794(E) (Oct. 28, 2022).
[17] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, Gazette of India, pt. II sec. 3(i), G.S.R. 275(E) (Apr. 6, 2023).

losing total legal immunity for not removing content in a timely manner, corporations will obviously choose to remove the post immediately without going to court. As a result, private censorship occurs, during which all honest journalism and political criticism get deleted.[18]

Secondly, the rules vest the power of decision-making regarding the content that can be published and communicated in Governmental committees. The creation of Grievance Appellate Committees in 2022 and Fact-Check Unit in 2023 have vested the powers of resolving disputes about speech in executive officers. In doing so, these provisions violate the fundamental principle of the law that no one is to be judge in their own case. This is because the government bodies decide about the truthfulness of the criticism addressed at the state.[19]

Thirdly, Rule 4(2) requires messaging companies to trace the identity of the original sender of any unlawful communication. The contemporary messaging applications utilize end-to-end encryption, which makes the contents of the messages available only to the sender and the recipient. To break such an encryption to trace one particular individual will endanger the privacy of all the users on the platform. Thus, a clear clash emerges between the work of the police to trace the criminal and the constitutional right to privacy enshrined in Article 21 of the Constitution.[20]

Thus, the primary legal issue here is the fact that the government relied on administrative regulations created by ministries rather than parliamentary debates and passed legislation to make fundamental changes to freedom of expression, right to privacy, and operations of media.

3. Research Gap

There have been many publications by lawyers and other scholars devoted to the 2021 Rules. Nevertheless, there are three significant aspects which are absent from the discussion:

1. Most publications focus on one aspect of the Rules. They either discuss the social media rules within MeitY or news and streaming platforms within MIB. Very little has been published concerning both parts combined.

[18] Daphne Keller, Empirical Evidence of "Over-Removal" by Internet Companies under Intermediary Liability Rules: An Update, Stanford Law School Center for Internet and Society Technical Report, at 12–17 (2018).
[19] A.K. Kraipak v. Union of India, (1969) 2 S.C.C. 262, 268–272 (India).
[20] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, 264–268 (India).

2. Much of the existing literature, meanwhile, was published just after the original rules were first issued in early 2021. There are few legal articles discussing both the amendments from 2022 and 2023 in relation to the original set of rules.

3. As people discussed court stays issued by the Bombay and Madras High Courts in 2021, the entire legal battle around the Fact-Check Unit which took place in the Kunal Kamra case has not been properly linked to the general discussion. The court battle started with the dissenting opinion given by two judges in January 2024, followed by the Supreme Court's interim stay and a final decision given by the third judge in September 2024, which ruled against the rule.

In this regard, this paper seeks to fill in these gaps and explore the entire context of events: the original rules, amendments to the rules and decisions concerning them.

4. Research Objectives

The research seeks to achieve the following objectives in five steps:

1. To clarify the provisions of Section 79 of the IT Act and demonstrate how the introduction of the 2021 Rules transformed the Safe Harbour provision from a straightforward legal protection to a conditional offer that is subject to withdrawal.

2. To analyze the obligations imposed upon major social media platforms, including recruitment of local employees for compliance purposes, use of computerized filtering mechanisms for detecting inappropriate messages, and issuance of monthly reports, and evaluate whether they are reasonable and practicable.

3. To explore Rule 4(2) in terms of the sender traceability and assess its compliance with the right to privacy outlined in the historic Puttaswamy judgment, as well as establish whether the rule violates message encryption.

4. To scrutinize the legality of the imposition of the rules governing digital news platforms and OTT services like Netflix by the central government in accordance with Section 87 of the IT Act, or if the government exceeded the scope of the parent law.

5. To evaluate the complaint mechanism, the Grievance Appellate Committees, and the Fact-

Check Unit set aside in Kunal Kamra in view of the right to freedom of speech guaranteed by Article 19(1)(a) of the Constitution.

5. Research Questions

In this paper, five specific research questions have been addressed below:

1. Will imposing due diligence obligations on the platforms with the possibility of revocation of the safe harbor status defeat the Supreme Court's decision in Shreya Singhal by causing companies to remove content that is not harmful?

2. Is it possible to impose a message traceability obligation under rule 4(2) without violating the right to privacy guaranteed under Article 21 of the Indian Constitution?

3. Was the Central Government exceeding its powers provided under Section 87 of the Information Technology Act, 2000 while prescribing conduct rules and regulating bodies for digital news websites and OTT platforms?

4. Are the government appeals tribunals and fact-finding office mechanisms contrary to the basic principles of natural justice and abridge the freedom of expression guaranteed under Article 19(1)(a)?

5. What are the legal reforms that Parliament needs to undertake in the forthcoming Digital India Act to replace the current mechanism?

6. Scope and Limitations of the Statute

Scope of the IT Rules, 2021

These Rules enjoy wide applicability. According to Section 75 of the parent Information Technology Act, the Rules will be applicable not only to companies registered in India, but to foreign internet companies also, which offer services dealing with computers or users in Indian Territory.[21]

[21] Information Technology Act, 2000, § 75.

Scope of the Statute:

The rules cover three areas primarily:

Firstly, the rules classify social media companies into two categories. While standard social media platforms need to comply with certain requirements only, the Significant Social Media Intermediaries (having 50 lakh or 5 million registered users in India) shall have to adhere to stringent requirements.[22] The large social media companies shall establish their physical presence in India, have designated Indian employees for responding to queries from the police, use automated tools for identifying malicious content, and report each month how many contents they delete.

Secondly, they empower ordinary citizens by providing them with clear measures of protecting their personal dignity. Under Rule 3(2)(b), if any individual complaints that their private photographs and even digitally modified images, either partially or fully naked, are uploaded on the internet, then the company shall take down within 24 hours.[23] This gives victims immediate relief without forcing them to wait for court hearings.

Three, they introduce the concept of regulated systems to online news portals and streaming applications. As far as the latter are concerned, they introduce five age rating categories (U, U/A 7+, U/A 13+, U/A 16+, and A) and introduce the requirement to use password protection of media content suitable only for adolescents and adults.[24]

Limitations on the Legal and Constitutional Levels

1. The Problem of Subordinate Legislation Exceeding Parental Law

The first and most important drawback of the 2021 Rules is their subordinacy to the IT Act of 2000 as secondary legislative acts created by government ministries pursuant to Section 87 of the IT Act.[25] At the time of adoption of the parental legislation, Parliament's intent was to

[22] Ministry of Electronics and Information Technology, Notification Under Rule 2(1)(v) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gazette of India, pt. II sec. 3(ii), S.O. 942(E) (Feb. 26, 2021).
[23] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(2)(b).
[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 9, sch.
[25] Information Technology Act, 2000, § 87(1), (2)(z), (2)(zg).

legalize e-commerce, promote digital signatures, and criminalize computer offenses such as hacking.

It is explicitly stated under Indian constitutional law that an administrative regulation issued by any ministry shall not be beyond the purview of the primary legislation enacted by Parliament.[26] However, through Part III of the Rules that established the ethics code for digital news and created a committee of government officials who can prohibit news websites from operating, the new legislation was adopted without parliamentary approval. Due to such violation of law, the Bombay High Court in Agij Promotion and Madras High Court in the DNPA case declared an immediate injunction on Rules 9(1) and 9(3) as the regulation that allows government officials to control media violates freedom of speech.[27]

2. The Practical Issue of Decryption of Message Transmission

Rule 4(2) provides that any large messaging applications shall disclose to the court or to the senior government official, when requested, the first user of India who has sent the particular message.[28] According to the Rule, the company shall provide information on identity of the sender only, not the contents of the text message.

In reality, this distinction does not work for computer security today. Programs such as WhatsApp and Signal implement end-to-end encryption, wherein the message is encrypted on the sending device and decrypted only upon receipt on the recipient's device. The company behind the software does not possess the keys to decrypt the message.

For purposes of tracing the originator of the forwarding, the app company would need to maintain an everlasting electronic record of all messages sent by each individual within India. It entails altering the entire program and unlocking the security lock for millions of law-abiding individuals.[29] It is antithetical to the principle established in the Puttaswamy decision, as per which intrusion into one's privacy must be minimal whenever the state interferes.[30]

[26] Indian Express Newspapers (Bombay) Pvt. Ltd. v. Union of India, (1985) 1 S.C.C. 641, 689–693 (India); State of Tamil Nadu v. P. Krishnamurthy, (2006) 4 S.C.C. 517, 528–531 (India).
[27] Agij Promotion of Nineteen-One Media Pvt. Ltd. v. Union of India, 2021 SCC OnLine Bom 2938, paras. 12–16; Digital News Publishers Association v. Union of India, 2021 SCC OnLine Mad 5125, paras. 5–8.
[28] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).
[29] Manoj Joshi & V. Kamakoti, *Technical Assessment of Traceability in End-to-End Encrypted Messaging Systems*, Indian Institute of Technology Madras Technical Working Paper, at 7–14 (2020).
[30] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, 308–312.

3. Fear of Deleting Content and Conflict of Interest

These guidelines put great pressure on the operations of tech companies. They are expected to make tough legal decisions on sensitive issues such as defamation, obscenity, and public disorder in limited periods of 36 or 72 hours.[31]

Since being denied the legal protections under Section 79 may expose companies to major lawsuits, it is natural that the company will remove the post when any complaint is received, and not defend the rights of users to express themselves. This means that private companies will be able to censor the public debate in private.

Moreover, by creating Grievance Appellate Committees in 2022 and a Fact-Check Unit in 2023, the government appointed itself as a judge of the disputes on speech. This is a clear conflict of interest, since the government will be the one to decide if something is true or false about itself.

Judicial Intervention: Kunal Kamra Case Law

The aforementioned loophole was directly called into question by the government's addition of Rule 3(1)(b)(v) in 2023. This rule said that platform operators should strive to prevent the users from sharing any information on the functioning of the Central Government in case of the ruling by the State-owned Fact-Check Unit that the post in question is fraudulent or misleading.[32]

Political satirist Kunal Kamra, along with Editors Guild of India and magazine publishers ' associations, contested this rule in the Bombay High Court.[33] They contended that empowering the government with the right to determine the truthfulness of information on its activities goes against the freedom of speech and expression and the right to carry out a lawful profession as defined by Article 19(1)(a) and Article 19(1)(g).

The judges of the bench differed in their opinion in January 2024. Justice Gautam Patel declared the rule unconstitutional and voided it, whereas Justice Neela Gokhale ruled for

[31] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3(1)(d), 3(2)(a).
[32] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, r. 3(1)(b)(v).
[33] Kunal Kamra v. Union of India, 2024 SCC OnLine Bom 294.

keeping the rule.[34]

The case thus went to a third judge – Justice A.S. Chandurkar because of the tie. On September 2024, Justice Chandurkar ruled that the Fact-Check Unit regulation was unconstitutional since it was too wide, vague, and well out of proportion to the restrictions imposed by Article 19(2).[35] This was not all, for before making this final ruling, the Supreme Court had intervened to suspend the notification creating the Fact-Check Unit because of its unconstitutionality.[36]

7. Conclusion and Recommendations

The Information Technology Rules, 2021, are significant in that they serve as a watershed moment in how India will regulate the internet. It is no longer possible to leave online platforms entirely unregulated when algorithmic feeds, deepfakes, and abuse are taking a toll on actual humans.

The 2021 Rules have added many helpful measures:

- They provided victims of non-consensual private imagery a tangible means of getting their content removed within 24 hours;
- They made foreign tech companies establish physical presence in India through which they will be responsible to Indian law enforcement authorities; and
- They provided parents a system of age ratings and parental controls for online programming.

Still, the main problem with the 2021 Rules is the same: the government has tried to make new nationwide policies relating to freedom of expression, press freedom, and personal privacy by resorting to administrative rules under the archaic e-commerce law from 2000.

This policy creates major legal disputes:

- It pressures private platforms to delete posts excessively due to fear of losing their Safe

[34] Kunal Kamra v. Union of India, 2024 SCC OnLine Bom 294, paras. 110–145 (Patel, J.), paras. 180–210 (Gokhale, J.).
[35] Kunal Kamra v. Union of India, 2024 SCC OnLine Bom 3021, paras. 42–56.
[36] Kunal Kamra v. Union of India, 2024 SCC OnLine S.C. 498.

Harbour;

- It invades personal privacy as it calls for changes that will violate message encryption per Rule 4(2); and

- It gives speech control to government committees like the recently dissolved Fact-Check Unit.

In order to solve these systemic issues, India should adopt a comprehensive, transparent, and legal policy of internet governance.

Policy Recommendations and the Path Forward

1. Enact a Modern Primary Legislation in Parliament (Digital India Act)

Ad-hoc notifications cannot substitute laws deliberated and enacted by the elected lawmakers in parliament. The Digital India Act must be drafted, deliberated and enacted by the parliament to repeal the outdated IT Act of 2000.[37]

The Act should stipulate the responsibilities of various platforms, establish proper liability norms, define novel technologies such as generative AI, and outline precisely what the government can and cannot force the platform to do.

2. Establish an Independent Digital Regulatory Authority

The potential for political interference is obvious when complaints and appeal resolutions are left to the discretion of committees composed of ministry officials.

India must establish an independent statutory authority, which may be named the Digital Safety and Platform Standards Authority of India. Like other independent regulatory authorities such as the Telecom Regulatory Authority of India (TRAI), this authority must:

- Be headed by retired judges along with independent technical and civil society members;

[37] Ministry of Electronics and Information Technology, Proposed Digital India Act, 2023: Public Consultation Presentation, Government of India, at 14–22 (Mar. 2023).

- Manage appeals and platform disputes in an open and nonpartisan manner; and

- Ensure that the day-to-day internet moderation remains insulated from political considerations.

3. Revise Rule 4(2) Without Weakening Encryption

It is important to revise Rule 4(2) in a way that it stops requiring applications to compromise end-to-end encryption. Rather than this, law enforcement needs to rely on targeted metadata examinations based on warrant issued by courts.

Investigators must produce necessary evidence before judicial magistrates to secure a written warrant before seeking any information from users, instead of getting approval from the Ministry via Section 69 of the IT Act. This will align Indian policing practices with the essential privacy principles established by the Puttaswamy judgment.[38]

4. Cease Using Safe Harbour As a Threat for Small Delays

At present, an internet company which commits a paperwork oversight or a minor delay in complying with the requirements of Rules 3 and 4 may lose its protection granted by Section 79 of the law. This "all or nothing" approach forces companies to delete posts of their users in order to protect themselves from losses.

The law shall provide a step-by-step penalties scheme:

- Minor delays or mistakes shall be penalized with reasonable monetary sanctions, which would be imposed by an independent regulator;

- Protection under Safe Harbour shall be lost in case a platform is helping criminals, deliberately ignoring the court orders or hosting illegal content.

5. Provide Transparency of Algorithms and Uphold Due Process

Rather than imposing strict governmental demands on top of the companies, digital governance

[38] Modern Dental College & Research Centre v. State of Madhya Pradesh, (2016) 7 S.C.C. 353, 396–402 (India); K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1, 310–315.

shall imply transparency of activities of technology giants:

- Large platforms shall be obliged to provide access to privacy protected data for independent research centers, universities and civil society organizations;

- Audits of platforms should be carried out on a regular basis to ensure that the recommendation algorithms do not deliberately increase hate, violence, and child exploitation for advertising purposes; and

- The platforms should provide legitimate reasons for account suspension and post removal in writing to users and offer them an opportunity to appeal.

India will therefore be able to create a healthy digital environment that will foster technological growth, protect its citizens, and respect democratic freedoms stipulated in its constitution through its comprehensive legislation by the parliament.