

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

© 2021 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com>)

This Article is brought to you for “free” and “open access” by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in International Journal of Law Management & Humanities after due review.

In case of any suggestion or complaint, please contact Gyan@vidhiaagaz.com.

To submit your Manuscript for Publication at **International Journal of Law Management & Humanities**, kindly email your Manuscript at submission@ijlmh.com.

New IT Rules, 2021 in India Privacy vs Public Safety

ABHISHEK BHARDWAJ¹

ABSTRACT

The article talks about the new IT rules [Information Technology (Intermediary Guidelines and Digital Media Ethics Code) rules 2021], notified by the government in February 2021. The rules have been framed in exercise of powers under section 87 of IT Act 2000 and similar provisions which were there before under Information Technology (Intermediary Guidelines) Rules 2011 stand replaced. The article has talked about the two major concepts of 'Privacy' and 'Public Safety' which are the elements of the controversy brought up by the new IT rules. The author has mentioned the salient features of new IT rules in brief. Further, it talks about the controversy and problems arising from such rules. It also includes the reasons for the need of such rules and government control. The author concluded by specifying few of the observations made by the courts by mentioning some of the earlier cases and giving some suggestions in that regard as well.

Keywords: New, IT Rules, Privacy, Safety.

I. INTRODUCTION

The people of India basking under the light of Article 19 of Constitution and Supreme Court's nine-judge bench imprimatur of Right to Privacy in In Puttasawamy Judgement; eagerly waiting for Data Protection Laws to be framed by their democratically chosen representatives after a vigorous discussion, due deliberation & clearance by joint parliament committee. Before this dream of theirs could come true it a fresh debate was brewed when the Government came with the Information Technology Rules, 2021 on 25th February declaring them as supersession of the Information Technology (Intermediaries Guidelines) Rules, 2011.

These new rules brought back highly controversial topic of Privacy vs. Public Safety back into debate and citizens witnessed the crossfire of lawsuits being filed as the Government and Social Media Giants lock horn. Government's rationale against these vicious allegations of Government flirting with the idea of people's right to privacy as stated by Ravi Shankar Prasad, Minister for Law & IT is that no fundamental right including Right to Privacy, is an absolute

¹ Author is a student at Amity Law School, Noida, India.

right and is subject to “reasonable restrictions”.

(A) Some Important Definitions

Rule 2 is definition clause providing clear explanation for the terminologies such as –

Rule 2(w) defines ‘Social Media Intermediaries’ as an intermediary whose prime or sole objective is to capacitate interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.

Rules 2(v) defines ‘Significant Social Media Intermediaries’ as an intermediary having number of registered users in India above such threshold as notified by Central Government (the user threshold has been set at fifty lakh and above)²

(B) Dictates

Part II of the These new Rules specifically dictates that due diligence to be undertaken by an intermediary including social media intermediary and significant social media intermediary. These obligations are inescapable in nature.

Rule 3(a) dictates that an intermediary will be required to publish its user agreement and privacy policies or rules and regulations prominently on either its application or website or both. Some conspicuous examples of information are given under Rule 3(b) which has caused grievance and are unacceptable as per the government are as follows:

- (a) If the content is pornographic, obscene, paedophilic, defamatory in nature
- (b) If it is invasive of another person’s privacy including bodily privacy, insulting or harassing on the grounds of gender
- (c) If the content being shared is racially or ethnically objectionable or libellous
- (d) If the content relates or encourages money laundering or gambling, or otherwise inconsistent with or in contradiction to the prevalent laws of India.
- (e) If the content shown by addressee deceives or misleads about the inception point of the message
- (f) If the addressee intentionally & knowingly communicates any misleading or patently false information passing it off as fact.

² New IT Rules, 2021- Notification dated, the 25th February, 2021 G.S.R. 139(E): the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 | Ministry of Electronics and Information Technology, Government of India (meity.gov.in)

- (g) If the content shared threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States or public order, or causes incitement to the commission of any cognizable offence or prevents investigation of any offence or is insulting any foreign States.³
- (h) If the content shared with an intent to harass or mislead a person, agency or entity for causing injury to any person or incur a financial gain by written or published article which is false and patently untrue.

(C) “Rule”, not a Law

There is a pertinent reason as why they are called rules and not laws. The government has made a paradigm shift in the way the internet is going to work in India without taking up this matter to the Joint Parliament Committee for collaboration and consultation and unless it maintains the just the right balance between people’s right to surveillance and oversight, these newly minted rules are going to sore out like a proverbial sore thumb. The government not only has amended the pre-existing laws but has also widened their ambit by adding OTT and Digital Platforms under it which were not previously included under the original law. This may be related to the case going on at the apex court regarding the PIL against the Amazon series TANDAV, at the time at which these rules were announced, but its still no justifiable to make such elephantine changes to the law without passing it through the parliament.

As its already quite clear from the ongoing protest against farm laws that passing a law from parliament does not guarantee an act as being accepted by the people and constitutional safeguard albeit to altogether skip the parliament proceedings is a deep cause of concern.

(D) The Elastic Stretching of ‘Due Diligence’

New IT Rules directs especially the “significant Social Media Intermediaries” such as Telegram, Facebook, WhatsApp to abide by various rules and duties such as-

- (a)Appointing a Chief Compliance Officer, Nodal Officer, Grievance Redressal Officer according to the Rule 4(1).
- (b)To deploy a technology based automated filtering tool so as to segregate and delete the content depicting child pornography according to Rule 4(4).
- (c) Special expedited mechanisms to take down content being used to harass a person relating to revenge porn.

³ Who Gets To Decide What Is Legitimate Free Speech — Big Government or Big Tech? | The Fletcher School (tufts.edu)

(d) To make a more efficient grievance redressal system and accountability through the perseverance of receipts.

(e) Traceability of the origin of the information for certain specific purposes only when required by a judicial order or when an order is passed under section 69 by a competent authority under the Information Technology (Procedure and Safeguards for Interception, Monitoring and decryption Information) Rules, 2009 as stated by Rule 4(2).⁴

(f) Identification of a physical address of the Social Media Intermediary in India for the purpose of service of a legal notice

Rule 7 threatens to take away immunities provided under Section 79 of the Code and making them legally liable for the acts of third party such as mentioned in Rule 29(b) making them vulnerable to be prosecuted under the Code or Indian Penal Code. Social Industry Giants have never been a fan of the phrase ‘due diligence’ in law as it is too open-ended and gives Judge discretion of setting different criteria of fulfilling who then decides whether such criteria were fulfilled or not. More than a few attempts have been made to get rid of this phrase, one of the prime examples being a tussle between the Government and Parliamentary Standing Committee in 2006, the latter objecting and calling for its reintroduction in the law stating reason that removing an enabling provision which has been there in the principal act itself and leaving it to be taken care by guidelines makes no sense⁵. There is also a prevalent opinion in public that this is the high time for these Silicon Valley Giants to earn the freedoms given them under Section 79 as the News media has been walking on this tight rope for so many decades. But as far as the legislative history of Section 79 of Information Technology Act is concerned, it’s not under the authority of the government to impose preconditions on the Intermediaries savouring the right to immunity.

(E) End-To-End Encryption – Pillar to protect Digital Privacy

As the Digital Media Intermediaries were shellshocked after the announcement of the New IT Rules, it was the foot soldiers of Internet Freedom who were in the battlefield fighting their battles naming latest move as a wolf in watchdog’s clothing and ready to tread on people’s right to privacy. These newly minted laws have put forth freshly brewed debate over the issues of Privacy and End-to-End Encryption, which could be described as veritable bedrock of a safe and secure digital connectivity.

⁴ New IT Rules, 2021- Notification dated, the 25th February, 2021 G.S.R. 139(E): the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 | Ministry of Electronics and Information Technology, Government of India (meity.gov.in)

⁵ New IT Rules: stretching of ‘Due Diligence’ under section 79 (nagalandpost.com)

Cryptography process consists of a mechanism of hiding or encrypting the data in such a way that only the intended party gets to decrypt it after the message has been transferred to him. Between both the ends of transmission of the data it goes through a series of encryption and decryption algorithms using either an Asymmetric (in which 2 keys are used at both ends i.e., Public and Private) or Symmetric Cryptography (in which at both ends only the public key is used). Cypher text is often described as “unreadable text” consisting of not the original message but a string containing alphabet and numbers entailing hash values that goes up to 30 digits. So even if a hacker steals the information or data, without the public or the private key he won’t be able to decipher it, thus securing the private and confidential messages. Most of the Social Media Intermediaries use a mixture of these symmetrical and asymmetrical algorithms to different levels so as to fortify their security.

As the Net IT Rules prescribes traceability of the origin of the information for certain specific purposes like only when required by a judicial order or when a order is passed under section 69 by a competent authority under the Information Technology (Procedure and Safeguards for Interception, Monitoring and decryption Information) Rules, 2009 as stated by Rule 4(2); it also opens the door for hackers and bad elements of society to jam their foot in the door and get access to the confidential and private messages and data of people. Government has averred acute challenges such as child pornography, national security, drug trade, terrorism, blackmailing porn revenge cases, Child Sexual Abuse Messages (CSAM), Fake news etc has led to the Adding of the Rule 4(2) in the New IT Rules.

Appointment of a Chief Compliance Officer, 24x7 available Nodal officer, vide Rule4, an expedited redressal grievance mechanisms have been met by the public with open arms. It is he mandate to break the end-to-end encryption mandate that has produced a clamour across India and Silicon Valley giants because of its inveterate pernicious effect of public safety and privacy of users as well as of state.

In Antony Clement Rubin v. Union of India (TC Civil No. 189 Of 2020) this bone of contention has been brought up about traceability of the originator of the data and information on messaging platforms. At the inception this case was about a PIL seeking linking of Social Media accounts to Aadhar in front of Madras High Court which later transformed into the subject about the traceability of the originators of Information on end-to-end encryption platforms like Telegram, Instagram, WhatsApp, Facebook; thus, being of such an important nature transferred to the Supreme Court. The issue was raised in SC whether there is a method to fulfil traceability requirements without deteriorating the armour of encryption security, safety and privacy concerns to which a solution offered by IIT professor V Kamkoti’s solution

of adding a originator information which ideating a permission based system was declared moot and discounted later by the experts declaring it erroneous and not feasible without breaking the encryption first. The report of Justice Sikrishna Committee on Data Protection has also denounced the government for maintaining low encryption grade & standards in license agreements with telecom service providers stating the fact that “this poses a threat to safety and security of personal data of data principals”.⁶

Even though it is mentioned in Rule (4) that it is not required for a social media intermediary to disclose the contents of the message of originator or its associated users, still the fortification of encryption will be needed to be deciphered which means the data will be unprotected and vulnerable for cyber hackers due to the susceptibility which will arise out of breaking the encryption. This could conspicuously reduce the public’s faith in messaging platforms and is in direct contradiction of Right to Privacy which has been declared as a fundamental right in *Puttaswamy vs Union of India* which changed the ratio decidendi of *Kharak Singh v. State of U.P.*

(F) Iron Fist in Iron Gloves

The new IT Rules ethics per se have not been in so much in question, but the what’s been the question of the hour is the mechanism which the government has installed which could be explained as a disaster in the recipe. Just about anyone has the power to take up an objection up to the grievance redressal officer which through his contemplation is objectionable content regarding wide range of subjects including threat to nation’s integrity, fake news etc which are very debatable topics. So just installing a mechanism does not guarantee better segregation of the information cruising around the internet

Another alarming sign is Rule 8(3) which establishes a 3-tier power structure which is drafted up in a very idea in these rules. It basically gives this as described by the government “soft oversight” mechanism powers to operate as Ministry of Information and Broadcasting for TV Regulation itself that too without any clear legislative backing. There is also a concern if term “remedies” also includes the Rule 13(4) entails much severe actions which includes declaration of apology letters as well as blocking of content. The 3-tier structure has “Self-Regulation by applicable entities at Level I”, Self- Regulation by the self-regulating bodies of applicable entities at Level II”, and right at the apex “Oversight Mechanism by Central Government at Level III”. The term oversight must be clearly defined by the government as soon is possible; does it mean more censorship- and what it will entail or just simply government oversight-

⁶ Explainer: How the New IT Rules Take Away Our Digital Rights (thewire.in)

which at prima facie appears unconstitutional.

PhotoDNA - A risky slope

The Rule 4(4) directs all the Significant Social Media Intermediaries (such as Facebook, Signal, WhatsApp) to deploy a technology based automated filtering tool so as to segregate and delete the content depicting child pornography, whether explicit or implicit, or, any other content which shows similar type of data that has been previously blocked off. AI dependency through machine learning software could be riddled with alarming risks, including underdeveloped AI and imperfect nature of the AI in the current stage of machine learning algorithms. AI automated tools need to study a vast amount of data to learn to segregate the contents, which will need the companies to store a buck load amount of data and AI running interference on the user's sensitive content and information which does not relate in any way to the content which needs to be censored.

According to the experts, coding malfunctioning and biases in the development of an AI often lead to discrimination, lack of transparency, overbreadth and a lack of accountability⁷ and Rule 4(4) goes beyond just the censoring of child sexual abuse material to banning any other content which has been previously banned using targeting of a particular group of content which sounds alarming in the present scenario as it could be used to target a particular group of people speaking against the government policies. So to hand over the public's fundamental right of speech and freedom to be controlled and regulated by AI doesn't sound like a good idea.

(G) Media ethics code of digital media and OTT platforms

The code of ethics for online news, OTT platforms and digital media called for self-classification of content as U (universal), U/A 7+, U/A 13+, U/A 16+ and A (adult). They need to implement parental locks for those content which are classified as U/A 13+ or higher and reliable age verification mechanisms for content which are classified as A. publishers of news on such platforms would be required to observe Norms of Journalistic Conduct of the Press Council of India and the Program Code under the Cable Television Networks Regulation Act.⁸

II. INSIGHTS DONE BY COURT

2018: The Supreme Court (SC) had seen that the Government of India may diagram significant guidelines to murder kid sexual amusement, attack and gangrape imageries, chronicles and

⁷ Explainer: How the New IT Rules Take Away Our Digital Rights (thewire.in)

⁸ "FPJ Explains: What are the Centre's new rules for social media and digital content?", available at: <https://www.freepressjournal.in/india/fpj-explains-what-are-the-centres-new-rules-for-digital-content-and-when-will-they-come-into-effect>.

areas in content working with stages and various applications.

2020: An Ad-hoc gathering of the Rajya Sabha laid its report in the wake of considering the upsetting issue of sexual amusement by means of electronic media and its effect on young people and society all things considered and recommended for engaging unmistakable verification of the essential originator of such substance.

The government brought video electronic over-the-top (OTT) stages under the ambit of the Ministry of Information and Broadcasting.⁹

III. RECENT CONTROVERSY REGARDING IT RULES

These principles return on the of numerous discussions including these stages and expanding worries about their unregulated status.

There has been analysis about acquiring a plenty of new principles that should be regularly set off just through administrative activity.

1. WhatsApp has indicted the Government of India, saying that India's new IT rules disregard the privilege to security of Indian clients and required the web-based media delegate rules to be proclaimed illegal.

It encroaches upon the central right to protection without fulfilling the three-section test set out by the Supreme Court of legitimacy, need and proportionality.

WhatsApp needs the court to guarantee the provision doesn't come into power, and forestall criminal obligation to its workers for resistance.

It abuses the principal right to the right to speak freely of discourse and articulation.

The prerequisite to empower distinguishing proof of the primary originator of the data is ultra vires its parent legal arrangement, Section 79 of the Information Technology Act, 2000.

This denies the delegate of a reasonable plan of action if it can't help contradicting the Government's organization because of an exacting course of events.

Till now online media stages have the invulnerability that clients got from start to finish encryption was that middle people didn't approach the substance of their messages. Forcing this obligatory necessity of recognizability will break this resistance; accordingly debilitating the security of the protection of these discussions. The danger here isn't just one of security however to the degree of attack and hardship from a place of refuge.¹⁰

⁹ New IT Rules 2021 - Drishti IAS, Available at: <https://www.drishtias.com/>, (Last visited on 6 June, 2021).

¹⁰ ETech Explained: Government rules on WhatsApp & the controversy around it, *Available*

2 Twitter is occupied with a significant fight with the focal government over 'controlled media' labels on certain posts by individuals from the decision party Bharatiya Janata Party. While the public authority has advised Twitter to erase the labels, Twitter has not followed up on the mandate. Therefore, individuals from the Delhi Police's uncommon cell apparently struck two of Twitter's workplaces in India.¹¹

3 Modi govt's new IT rules don't engage customers, yet extend State control over online substance - the Narendra Modi government's new column with Twitter over the evacuation of political substance that the public authority thought about provocative and enemies of India. In any case, Twitter contended that nothing in these tweets abused laws on free discourse. While the public authority ultimately won and Twitter brought down a lion's share of the substance it was coordinated to, this happened solely after combative trades between the two gatherings. Media reports hypothesized that Twitter chiefs could confront genuine legitimate repercussions for not agreeing with the public authority's orders.¹²

IV. CONCLUSION

With the New IT Rules, 2021 government has tried to answer the long pending issues of social media, but has presented it with too many loopholes for the bad elements of the society to take advantage of; without much of consultation from the experts in the field of AI; sliding these rules through the back door stretching their legislative powers. These rules in the long run poses a real threat to the blanket privacy and raises some alarming issues of safety even for the state. People will be eagerly waiting for the Data Protection Bill, which is pending before Joint Parliamentary Committee, to finally pass, and then to mediate any conflicts if any arises between the two, it will be amusing to see which, if any, will prevail.

at:<https://economictimes.indiatimes.com/> , (last visited on 6 June , 2021).

¹¹ Twitter And WhatsApp Vs India's New IT Rules, *Available at:*<https://inc42.com/>, (Last visited on 6 June , 2021).

¹² Modi govt's new IT rules don't empower consumers, but expand State power over online content, *Available at:*<https://theprint.in/>, (Last visited on 6 June, 2021).