IT Rules, 2021 - A Paradigm Shift in Internet Norms : By Adv. K. Vaitheeswaran

Date : March 04,2021

Advocate K. Vaitheeswaran

Advocate Lavanya Lakshmi G

The Central Government has notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code), Rules, 2021 (hereinafter called DMEC). The Press Release dated 25.02.2021 states that there has been an extensive spread of mobile phones, internet, etc., enabling many social media platforms to expand their footprints in India and after acknowledging the right of the public to criticize and disagree as an essential element of democracy, it also states that the Social Media platforms are accountable to the Constitution and the laws of India.

The 'Why'

Social causes cited by the Government for introducing these Rules are persistent spread of fake news; posts severely affecting the dignity of women; misuse of platforms to settle corporate rivalry; use of abusive language; defamatory and obscene content; blatant disrespect to religious sentiments; misuse of social media by criminals, anti-national elements including but not limited to recruitment for terrorists, circulation of obscene content, spread of disharmony, financial frauds, incitement of violent, public order, etc.

The Rules have also been introduced to have a better regulation of content streamed in Over-The-Top (OTT) Platforms. The Government endeavours to create a level-playing field vide these regulations by bringing the OTT into the realms of enactments such as the Programme Code under the Cable Television Network Act; the journalistic conduct of Press Council of India which are presently applicable for print and television.

Source of Power

The DMEC has been issued by the Central Government in exercise of powers conferred under Section 87(1) and Section 87(2)(z) and (zg) of the Information Technology Act, 2000 and in supersession of the Information Technology (Intermediary Guidelines) Rules, 2011.

Section 87(2)(z) deals with power to make rules in connection with the procedure and safeguards for blocking for access by the public under Section 69A(2); and 87(2)(zg) deals with guidelines to be observed by the intermediaries under Section 79(2) of the IT Act, 2000.

Section 69A confers powers to issue directions for blocking for public access of any information through any computer resource. The circumstances for exercise of this extreme power are identified as *interest of the sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence relating to the above.*

Section 69A of the IT Act, 2000 was upheld by the Supreme Court in the case of ***Shreya Singhal Vs. UoI (2015) 5 SCC 1,*** even though Section 66A was struck down as unconstitutional. The Supreme Court held that Section 69A unlike Section 66A is a narrowly drawn provision with several safeguards. First and foremost, blocking can be only resorted to where the Central Government is satisfied that it is necessary so to do. Secondly, such necessity is relatable only to some of the subjects set out in Article 19(2). Thirdly, reasons have to be recorded in writing in such blocking order so that they may be assailed in a Writ Petition under Article 226. The Rules further provide for a hearing before the committee set up which committee then looks into whether or not it is necessary to block such information. Section 79 was considered as valid subject to Section 79(3)(b) being read down 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, then fails to expeditiously remove or disable access to such material. The Court upheld the IT Intermediary Guidelines, 2011 subject to Rule 3(4) being read down in the manner indicated in the judgement.

The New Rules

The New Rules have introduced certain definitions which are of significance.

(i) *'access control mechanism' – any measure, including a technical measure, through which access to online curated content may be restricted based on verification of the identity or age of user;*

(ii) 'content descriptor' – means the issues and concerns which are relevant to the classification of any online curated content, including discrimination, depiction of illegal or harmful substances, imitable behaviour, nudity, language, sex, violence, fear, threat, horror and other such concerns as specified in the Schedule annexed to the rules;

(iii) 'digital media' means digitised content that can be transmitted over the internet or computer networks and includes content received, stored, transmitted, edited or processed by – (i) an intermediary; or (ii) a publisher of news and current affairs content or a publisher of online curated content;

(iv) 'publisher of news and current affairs event'– an online paper, news portal, news aggregator, news agency and such other entity called by whatever name, which is functionally similar to publishers of news and current affairs content but shall not include newspapers, replica e-papers of the newspaper and any individual or user who is not transmitting content in the course of systematic business, professional or commercial activity.

(v) 'publisher of online curated content' – a publisher who, performing a significant role in determining the online curated content being made available, makes available to users a computer resource that enables such users to access online curated content over the internet or computer networks, and such other entity called by whatever name, which is functionally similar to the publishers of online curated content but does not include any individual or user who is not transmitting online curated content in the course of systematic business, professional or commercial activity;

(vi) 'significant social media intermediary' – social media intermediary having number of registered users in India above such threshold as notified by the Central Government.

(vii) 'social media intermediary' – intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;

Due Diligence by Intermediaries

Part II of the Rules describes the due diligence that ought to be undertaken by the intermediaries. The Rules also specify the additional due diligence that ought to be observed by significant social media intermediary. The threshold for specifying organisations which form a part of the significant social media intermediary shall be notified by the Government in due course.

Multiple compliance measures have been mandated in detail in relation to the due diligence to be undertaken by an intermediary including Social Media Intermediaries and significant Social Media Intermediary. Some of the key ones are:

(i) Publishing the rules and regulations, privacy policy and user agreement or usage of its computer resource by any person.

This provision mirrors the principles set forth under Article 12 of the European Union General Data Protection Regulation (Transparent information, communication and modalities for the exercise of the rights of the data subject). This also resonates with the principles under Clause 17 of the Data Protection Bill, 2019 which provides for Right to Confirmation and access for the Data Principal.

(ii) The intermediary through rules and regulations, privacy policy or user agreement, shallInform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update, or share any information that belongs to another person; defamatory/ obscene/pornographic/paedophilic/invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling or otherwise inconsistent with or contrary to the laws in force; harmful to child; infringes any IPR; violates any law for the time being in force; deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact; impersonates another person; threatens the unity, integrity, defence, security or sovereignty of India;

There are totally 10 items in this elaborate list where the intermediary including social media intermediary and significant social media intermediary will have to exercise due diligence. These intermediaries will have to watch out for users violating the user agreement by uploading, etc. information which is categorising Rule 3(1)(b). It is relevant to note that out of the 10 items specified therein, item (viii) is the only one that adopts the language used in Section 69A.

It is pertinent to note that Supreme Court while upholding Section 69A observed that Section 69A is a narrowly drawn provision with several safeguards. Rule 3(1) of the 2021 Rules appears to have travelled beyond the mandate specified in Section 69A.

(iii) An intermediary is required to inform its user's atleast once every year that if there is non-compliance, it has the right to terminate the access or usage rights of the users or to remove non-compliant information.

From the user perspective there is a general feeling that the user has no say whatsoever and if a significant social media intermediary decides to block an account nothing can be done. Given the new set of Rules, the fear of non-compliance would have the potential to drive the intermediary to virtually act as a moral, legal and a judicial censor given the broad type of restrictive information set out in the Rules.

(iv) The intermediaries are prohibited to host/store/publish the information in violation of the guidelines, after the said information has come to their knowledge. The information must be removed within 36 hours of the receipt of the court order or on being notified by the Government or its agency. Temporary/ transient and intermediate storage are excluded from scrutiny. Information ought to be preserved (for evidence) by the intermediary, if instructed by the Government or its agency.

(v) The intermediary must publish the name of the Grievance Officer and his contact details. In case of receipt of complaint, the Grievance Officer is to acknowledge the complaint within 24 hours and dispose the same within 15 days of its receipt; receive orders / notice / directions issued by the Appropriate Government, any competent authority or a Court of competent jurisdiction.

(vi) The Intermediary shall within 24 hours of receipt of a complaint made by an individual or any person on his behalf in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual or shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practical measures to remove or disable access to such content.

This is a significant and welcome provision since it enables a complaint and redressal mechanism for many innocent victims who could only approach the cyber cell of the police department for action but could not immediately have the offensive content removed.

Significant Social Media Intermediaries

In addition to the due diligence under Rule 3 (Due Diligence for Social Media Intermediaries), the Significant Social Media Intermediaries must appoint a Chief Compliance Officer to ensure compliance with the Act and to be liable for any proceedings under the Act. A nodal person must also be appointed to coordinate with the law enforcement agencies 24*7. A resident Grievance Officer must be appointed. A periodic compliance report must be published every month mentioning the details of complaints received. The Rules further elaborate on the measures to be undertaken specifically by significant social media intermediaries.

This is likely to be a huge challenge since companies which have no presence in India will now be required to appoint a Chief Compliance Officer; Nodal Officer; a Grievance Officer who is a resident in India. Getting a Chief Compliance Officer would also be a challenge the said person would be liable in any proceedings relating to any relevant third-party information, data or communication link made available or hosted by that intermediary where he fails to ensure that such intermediary observes due diligence while discharging its duties under the Acts and Rules. Further, the CCO should be a key managerial personnel or senior employee and resident in India.

The nodal contact person should be an employee of the significant social intermediary, other than CCO and resident in India. The resident Grievance Officer must be an employee of significant social intermediary and resident in India.

It is interesting to note that the term 'resident in India' is not defined in the 2021 Rules or in the Information Technology Act, 2000.

Compliance cost would also go up on account of these factors in addition to requirements such as periodic compliance reports mentioning details of complaints received. Given the fact that all complaints may not be genuine and there could be agenda / harassment / driven complaints, the periodic reports by themselves would be a huge source of data and would again open up questions on privacy.

On one side when localization of data is yet to take concrete shape, the Rules are now calling for a local data officer

Intermediary in Relation to news and Current Affairs Content

This category of intermediaries, in addition to the stipulations for Social Media Intermediaries and Significant Social Media Intermediaries must publish a clear and concise statement informing publishers of news and current affairs that in addition to the common terms of service for all users, such publishers shall furnish the details of their user accounts on the services of such intermediary to the Ministry as may be required under Rule 18. This rule is applicable only to news and current affairs content and shall be administered by the Ministry of Information and Broadcasting.

Rule 18 deals with furnishing of information. What is interesting is that the intermediary will have to require publishers to furnish details of their user accounts on the services of such intermediary to the Ministry as may be required under Rule 18. This seems to be a bizarre requirement since a printed newspaper does not have any clue as to the identity of its readers whereas a publisher of digital news or online content should provide details of user accounts. User accounts means the account registration of a user with an intermediary or a publisher and includes profiles, accounts, pages, handles and other similar presences by means of which a user is able to access the services offered by the intermediary or publisher.

Part III of the Rules – Code of Ethics and Procedure and Safeguards in Relation to Digital Media

This part is applicable to publishers of news and current affairs content; publishers of online curated content. They must observe the Code of Ethics enclosed in the Appendix of the Rules. News and current affairs should follow the norms of journalistic conduct of the Press Council of India; programme code under Section 5 of the Cable Television Network Regulations Act and ensure that there is no publishing or transmitting of content which is prohibited under any law.

In so far as online curated content is concerned, a publisher should not transmit or publish content prohibited under any law or prohibited by any court. Further, while deciding to feature or publish any content, the publisher must exercise due caution and discretion in the context of content and the element of Section 69A are identified herein. A publisher should also take into consideration India's multi-racial and multi-religious context and exercise due caution and discretion when featuring the activities, belief, practices or views of any racial or religious group.

Contents classification would require rating category such as 'U' / 'U/A' '7+' / 'U/A 13+' / 'U/A 16+' / 'A'. Further, content should be classified on the basis of themes and messages, violence, nudity, sex, language, drug and substance abuse, horror.

The publisher of online curated content should implement a reliable age verification mechanism for viewership of adult content.

Grievance Redressal Mechanism

The Rules establish a three-tier structure for observance and adherence to this Code.

(a) Level I – Self-Regulation by the publishers

(b) Level II – Self-Regulation by the self-regulating bodies of the publishers

(c) Level III – Oversight mechanism by the Central Government

The Rules elaborate on the methodology for handling the grievances on a self-regulatory basis. At Level I of self-regulation, the publisher must establish a grievance redressal mechanism and appoint a Grievance Officer, the details of whom shall be provided in the publisher's interface. This Officer, in receipt of a grievance, shall take a decision on the same within 15 days

and communicate the same to the complainant.

At the Level II of self-regulation, where there may be one or more self-regulatory bodies of publishers. This shall be headed by a retired Judge of the Supreme Court, a High Court or an independent eminent person from the field of media, broadcasting, entertainment, child rights, human rights or such other relevant field, and have other members, not exceeding six, being experts from fields aforementioned. They must register with the Ministry within a period of 30 days form the date of its constitution. The body shall oversee the Publisher's adherence to the Code of Ethics, address grievances within a period of 15 days and provide guidelines for the Publisher's adherence to the Code of Ethics. Where the publisher fails to comply with the guidance and advisory, the matter shall be referred to the Oversight Mechanism within 15 days of expiry of the specified date.

At Level III of Self-Regulation Mechanism, the Ministry is to co-ordinate and facilitate the adherence to the Code of Ethics by publishers and the self-regulating bodies. They must make charters for the self-regulating bodies, including Codes of Practices; establish an Inter-Departmental Committee for addressing grievances, issue guidance and advisories to publishers, etc.

The Inter-Departmental Committee, in turn, shall consist of representatives from the Ministry of Information and Broadcasting, Ministry of Women and Child Development, Ministry of Law and Justice, Ministry of Home Affairs, Ministry of Electronics and Information Technology, Ministry of External Affairs, Ministry of Defence, and such other Ministries and Organisations, including Domain Experts.

Concluding Thoughts

The enactment of Data Protection Bill, 2019 is yet to happen but there is a deluge of information and one cannot deny the fact that what appears true could be false and what appears false could be true and the web space has truly become 'maya'.

It has now come to such a stage that every reader of a message or information is forced to check or carry out his limited investigation techniques to attempt to verify the truth before he embarks upon the journey of forwarding and sharing the information. From that perspective the measures to protect the citizens from misinformation as well as cyber threats is laudable.

The new rules to a large extent have resemblance to the General Data Protection Regulation and EU Code of Practice on Disinformation. The measures also seem to extract a few ideas from the Data Protection Bill, 2019. Borrowed from many, the Rules are quite comprehensive in nature.

However, increase in regulations and shifting the onus to the intermediary could have the effect of choking the very free nature of information. Some of the elements which fall in the restricted lists are very general in nature and have scope for misuse. The increased regulations around expression of thoughts or views are not based on empirical factors. On the other hand, without conferring rights to the user through a comprehensive data protection law it would not be correct to only deal with the duties of the user.

In this age of information, artificial intelligence and machine learning, data sharing cannot be prevented. Sharing of data has now become a reflex action and mere removal of information from the source may not serve the purpose. Every single person or user in the chain cannot be traced and be held liable. Therefore, the self-regulatory mechanisms established by the social media intermediaries can only do so much. Moreover, one cannot assure that there would not be any misuse either by the authorities concerned or by complainants or by the intermediary itself. Creator bias is also a possibility.

When a foreign chef has to provide an interesting dish and local experts have to be appointed who are required to monitor the process and the recipe is quite complicated through multiple regulations and the chef has to deal with multiple complaints; provide redressal and keep changing the ingredients all the times, the dish is likely to be a huge challenge.

Mere laws would not bring about change and society will have to be aware of the serious damage that can be caused on account of misinformation or disinformation. The need of the hour is a law for data protection which deals with both rights and duties. Similarly, having provisions which are couched with general and wide terms and conferring significant power on the executive without accountability is equally dangerous. In the world of 'deep fakes' and 'bots', regulating information should be only on specified segments and that too in areas which are directly relatable to sovereignty and security and a wider net can only increase the scope for misuse.

It is quite possible that the validity of the new Rules would be tested in Courts given the fact that in the first round of litigation before the Supreme Court, the Court had observed that the intermediary applying its own mind to whether information should or should not be blocked is noticeably absent in Section 69A read with the 2009 Rules. The Court observed that the knowledge spoken of in the said sub-rule must only be through the medium of a court order and subject to that the 2011 Guidelines were considered as valid. The 2021 Rules have shifted the onus and the judgment to the intermediary and hence one cannot rule out another round of litigation.