PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9543 / +41 22 917 9738 • FAX: +41 22 917 9008 • E-MAIL: registry@ohchr.org

Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
OL IND 3/2019

14 February 2019

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

In this connection, I make reference to the call for public comments by the Ministry of Electronics and Information to **The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018** ("the proposed Amendment").

I welcome the opportunity to submit this comment to the proposed Amendment, reviewed in light of international human rights standards on the right to freedom of opinion and expression, and I stand ready to engage further with your Excellency's Government on this matter.

According to the information received:

On 26 July 2018, the Honorable Minister for Electronics and Information Technology proposed an amendment to the Information Technology (Intermediaries Guidelines) Rules established under Section 79 of the Information Technology Act.

Section 79 states that an intermediary "shall not be liable for any third party information, data, or communication link made available or hosted by him" provided that the intermediary, *inter alia*, "observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf."

On 24 December 2018, the Ministry of Electronics and Information announced its proposal for The Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018 ("the proposed Amendment"). The proposal

purportedly addresses the need to combat the misuse of social media platforms and the spread of "fake news."

The proposed Amendment would impose additional obligations on intermediaries to prohibit online content and provide assistance to Government investigations into online content.

In particular, intermediaries would be required to, *inter alia*, prohibit an expanded range of online content, assist the Government in tracing prohibited information to their originator, establish physical presence and personnel dedicated to law enforcement cooperation, remove illegal online content within twenty-four hours, retain user data, and proactively monitor and filter online content.

Before explaining my concerns with the proposed Amendment, I wish to remind your Excellency's Government of its obligations under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), acceded by India on 10 April 1979. Article 19(1) of the Covenant establishes "the right to hold opinions without interference." The right to hold opinions is so fundamental that it is "a right to which the Covenant permits no exception or restriction" (CCPR/C/GC/34). Accordingly, this right is not simply "an abstract concept limited to what may be in one's mind," and may include activities such as research, online search queries, and drafting of papers and publications"(A/HRC/29/32).

Article 19(2), in combination with Article 2 of the Covenant, establishes State Parties' obligations to respect and ensure the right "to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Since Article 19(2) "promotes so clearly a right to information of all kinds," this indicates that "States bear the burden of justifying any withholding of information as an exception to that right" (A/70/361). The Human Rights Committee has also emphasized that limitations should be applied strictly so that they do "not put in jeopardy the right itself" (CCPR/C/GC/34). The General Assembly, the Human Rights Council and the Human Rights Committee have concluded that permissible restrictions on the Internet are the same as those offline.

Article 19(3) establishes a three-part test for permissible restrictions on freedom of expression:

First, restrictions must be "provided by law." In evaluating the *provided by law* standard, the Human Rights Committee has noted that any restriction "must be made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly" (CCPR/C/GC/34). Moreover, it "must not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution" (CCPR/C/GC/34).

Second, restrictions must only be imposed to *protect legitimate aims*, which are limited to those specified under Article 19(3), that is "for respect of the rights or

reputations of others" or "for the protection of national security or of public order (*ordre public*), or of public health and morals". The term "rights…of others" under Article 19(3)(a) includes "human rights as recognized in the Covenant and more generally in international human rights law" (CCPR/C/GC/34).

Third, restrictions must be *necessary to protect one or more of those legitimate aims*. The requirement of necessity implies an assessment of the proportionality of restrictions, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons" (A/70/361). The ensuing interference with third parties' rights must also be limited and justified in the interest supported by the intrusion. Finally, the restriction must be "the least intrusive instrument among those which might achieve the desired result" (CCPR/C/GC/34).

In light of these standards, the proposed Amendment raises the following concerns:

Draft Rule 3(1): Additional prohibitions on online content

The existing Rule 3(1) requires intermediaries to prohibit, *inter alia*, information that is "grossly harmful, libelous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging," or that "threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order."

The proposed Amendment would also require intermediaries to prohibit the "host[ing], display[ing], upload[ing], modify[ing], publish[ing], transmit[ting], updat[ing] or shar[ing]" of information that "threatens public safety" or "threatens critical information infrastructure."

The Human Rights Committee has concluded that, under Article 19 of the ICCPR, "[a]ny restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3." Accordingly, Rule 3(1) and any proposed changes must be compatible with the criteria of legality, legitimacy and necessity.

While public order and national security are legitimate grounds for restriction, the existing and proposed Rule 3(1) may impose disproportionate restrictions on freedom of expression. Existing Rule 3(1) criteria, such as the prohibition of information that is "racially, ethnically objectionable, disparaging," are vaguely formulated and prone to highly subjective interpretation, creating uncertainty about how intermediaries should restrict such content. The proposed Amendment exacerbates this vagueness and uncertainty, expanding the range of prohibited information to include information that "threatens public safety" and "critical information infrastructure."

In my June 2018 report to the Human Rights Council, I cautioned that vaguely formulated standards like draft Rule 3(1) "involve risks to freedom of expression, putting significant pressure on companies such that they may remove lawful content in a broad effort to avoid liability" (A/HRC/38/35). They also "involve the delegation of regulatory functions to private actors that lack basic tools of accountability," and "whose motives are principally economic" (A/HRC/38/35). Since decisions regarding the lawfulness of expression involve "[c]omplex questions of fact and law," I urge Your Excellency's Government to ensure that public institutions retain the authority to adjudicate these questions. In particular, restrictions on online content should only be imposed "pursuant to an order by an independent and impartial judicial authority, and in accordance with due process and standards of legality, necessity and legitimacy" (A/HRC/38/35).

Draft Rule 3(5): Mandatory assistance orders

Rule 3(5) of the proposed Amendment would require intermediaries to provide "information or assistance" as asked by "any government agencies who are lawfully authorized," including by "enabl[ing] tracing of originator of information on its platform as required by government agencies who are legally authorised."

Under draft Rule 3(5), authorized government agencies may seek such information and assistance for the "investigation or detection or prosecution or prevention of offence(s); protective or cyber security and matters connected with or incidental thereto."

I am concerned that compliance with this draft Rule will require intermediaries to match the identity of users to the information at issue, which may in turn necessitate the circumvention of encryption and other digital security measures. As I have explained in my June 2015 report to the Human Rights Council, encryption and anonymity technologies establish a "zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks" (A/HRC/29/32). As a result, restrictions on these technologies must meet the well-known three-part test" established under Article 19(3). (A/HRC/29/32)

Laws that mandate or effectively require decryption may compel intermediaries to introduce security vulnerabilities or otherwise weaken encryption in a manner that undermines encryption and digital security protocols for all users across the platform. Even in cases where mandatory decryption orders are targeted at an individual account for a specific investigation, the ensuing security and privacy risks to large numbers of users may disproportionately chill and hinder their exercise of freedom of expression. The prospect that such decryption measures may be sought on vaguely formulated grounds under draft Rule 3(5), such as for the protection of "cyber security" and any related matters, heightens the disproportionality of such measures.

Draft Rule 3(7): Mandatory incorporation and appointment of personnel

Draft Rule 3(7) requires intermediaries with "more than fifty lakh users in India," or on the list of intermediaries notified by the government, to be incorporated in India according to the Companies Act, and to have a permanent registered office in India with physical address. Furthermore, under Rule 3(7), intermediaries must appoint a "nodal person of contact" and "alternate senior designated functionary" in order to ensure "24x7 coordination with law enforcement agencies."

While I appreciate that this proposed rule change may be an effort to enhance the accountability of intermediaries to local users, I am concerned that the burden of incorporation and associated compliance measures would outweigh its purported objectives. The requirement to establish a permanent registered office and appoint compliance personnel within an unspecified timeline is likely to impose costs that may unduly restrict the creation and operation of small, medium-sized or non-profit intermediaries. The potentially disproportionate impact on these intermediaries may contribute to the dominance of major, multi-national platforms in the country and diminish media pluralism. The Human Rights Committee has found that "undue media dominance or concentration by privately controlled media groups in monopolistic situations ... may be harmful to a diversity of sources and views" (CCPR/C/GC/34). The potential effects of Draft Rule 3(7) would run counter to the State's duty to take "appropriate action" to prevent undue dominance and ensure media pluralism (CCPR/C/GC/34).

Draft Rule 3(8): 24-hour window for content removals and data retention requirements

Draft Rule 3(8) requires intermediaries to remove or disable access to unlawful content within 24 hours upon receiving a court order or notification from the appropriate Government or its agency. In addition, intermediaries must retain such information and associated records for at least one hundred and eighty days for "investigation purposes" or "for such longer period a may be required by the court or by government agencies."

I am concerned that the twenty-four hour rule provides extremely limited opportunity for review or appeal of removal orders, whether before a judicial body or other relevant appeals mechanisms. In my June 2018 report to the Human Rights Council, I warned against domestic requirements "to monitor and rapidly remove user-generated content," which establish "punitive frameworks likely to undermine freedom of expression even in democratic societies" (A/HRC/38/35). Furthermore, the lack of independent and external review or oversight of government-issued orders would effectively confer significant discretion on government authorities to restrict online content based on vague criteria, raising concerns of due process and increasing the risk of government overreach. Consistent with this past reporting, I urge Your Excellency's Government to refrain from adopting a model of regulation "where government agencies, rather than judicial authorities, become the arbiters of lawful expression" (A/HRC/38/35).

The proposed data retention requirements also raise necessity and proportionality concerns. These requirements effectively compel intermediaries to create databases of personal and sensitive information about users that are readily accessible to the government for an unspecified range of "investigative purposes." I have observed that broad data retention mandates heighten the risk of government access to user data that violates "established due process standards, such as the need for individualized suspicion of wrongdoing" (A/HRC/35/22). These mandates also render users vulnerable to security breaches and unauthorized third-party access. Additionally, I am concerned that Rule 3(8)'s data retention requirements, together with the proposals for proactive monitoring of online content and closer cooperation between intermediaries and law enforcement, will create a broad and intrusive surveillance regime that chills the exercise of the right to seek, receive and impart information on internet platforms.

Draft Rule 3(9): Automated content monitoring and removals

Draft Rule 3(9) states that an "intermediary shall deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying and removing or disabling public access to unlawful information content."

I am concerned that this proposed rule change would impose an affirmative obligation on intermediaries to regularly monitor content and restrict content at the point of upload, based on their own determinations of legality under highly subjective criteria (such as threats to "public safety" and "critical information infrastructure" as outlined above). As I discussed above, content review systems deployed by private intermediaries, which lack the due process safeguards and democratic legitimacy of the judicial process, are ill-equipped to make such determinations. The threat of criminal or civil penalties is also likely to incentivize intermediaries to err on the side of caution and restrict content that is perfectly legitimate or lawful.

Overreliance on automated tools would exacerbate these concerns. Automation tools range from keyword filters and spam detection tools to hash-matching algorithms (which filter images based on their unique digital "fingerprint") and Natural Language Processing tools (which parse different features of text to determine whether it is a targeted category of speech).[1] These tools have become useful means of parsing text, images and video based on highly specific and objective criteria (such as matching the digital "fingerprints" of images to those of images already deemed unlawful). However, when applied to evaluations of online content that require an understanding of context or an assessment of highly subjective criteria (such as hate speech or libel), automated tools are prone to unreliable and discriminatory outcomes. In my September 2018 report to the General Assembly, I explained that these tools are still largely unable to meaningfully process "widespread variation of language cues, meaning and linguistic and cultural particularities" (A/73/348). Automated content moderation tools may also be "grounded in datasets that incorporate discriminatory assumptions" about race, gender and other

[1] CTR. FOR DEMOCRACY & TECH., MIXED MESSAGES?: THE LIMITS OF AUTOMATED SOCIAL MEDIA CONTENT ANALYSIS 1, 9 (2017), https://cdt.org/files/2017/11/Mixed-Messages-Paper.pdf.

protected characteristics, creating a high risk that such tools will remove content "in accordance with biased or discriminatory concepts" (A/73/348).

As a result, overreliance on automated tools may both overlook content susceptible to lawful restriction under Article 19(3) and increase censorship of legitimate expression. Inherent difficulties in scrutinizing and explaining the logic of automated tools further problematize their use in regulating contested areas of expression (A/73/348).

I urge the your Excellency's Government to ensure that any amendment to its rules on intermediary liability addresses these concerns and is consistent with Article 19 of the ICCPR and related human rights standards.

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website within 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression