PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND

Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on the right to privacy

REFERENCE:
OL IND 8/2021

11 June 2021

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association and Special Rapporteur on the right to privacy, pursuant to Human Rights Council resolutions 43/4, 41/12 and 46/16.

In this connection, we would like to offer the following comments on the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, published on 25 February 2021 under the Information Technology Act, 2000.

In this letter, we address a number of provisions of the Rules that do not appear to meet the requirements of international law and standards related to the rights to privacy and to freedom of opinion and expression, as protected by Articles 17 and 19 of the International Covenant on Civil and Political Rights, acceded to by India on 10 April 1979.

We appreciate the commitment of your Excellency's Government to ensure social media intermediaries are more transparent and accountable about their operations, including by providing opportunities for redress when content is restricted. We also welcome that under rule 4 (8) (a) intermediaries shall provide information on the rationale for removing or disabling access to information or data. However, we express serious concern that some parts of their due diligence obligations may result in the limiting or infringement of a wide range of human rights. We encourage withdrawal, review and reconsideration of certain key aspects of this legislation to ensure that the Rules are in compliance with your Excellency's Government's international human rights obligations. Given the wide-ranging impact of social intermediary legislation on a range of human rights, they should be closely scrutinized and therefore, we urge your Excellency's Government to undertaken wide consultations with all relevant stakeholders.

I. Scope of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Section 2(i) defines "digital media" as "digitized content that can be transmitted over the internet or computer networks and includes content received, stored, transmitted, edited, or processed by (i) an intermediary; (ii) a publisher of news and current affairs content or a publisher of online curated content". The Rules further define "significant social media intermediary" and "social media intermediary." The Rules therefore apply to a broad and heterogeneous set of actors, including online outlets of traditional media, as well as small independent media outlets, social media, ISPs, web hosts, email hosts, amongst others.

Section 3(1)(b) of the Rules requires intermediaries – including social media and significant social media intermediaries – to perform certain 'due diligence', which includes publishing a user agreement requiring users not to "host, display, upload, modify, publish, transmit, store, update or share any information that:

(i) belongs to another person and to which the user does not have any right;
(ii) is defamatory, obscene, pornographic, pedophilic, invasive of another's privacy, including bodily privacy, insulting or harassing on the basis of gender, libelous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;
(iii) is harmful to child;
(iv) infringes any patent, trademark, copyright or other proprietary rights;
(v) violates any law for the time being in force;
(vi) 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;
(vii) impersonates another person;
(viii) 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 other nation;
(ix) contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;
(x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person."

The Rules further provides in article 3(1)(d) that "unlawful information, which is prohibited under any law for the time being in force in relation to the interest of the sovereignty and integrity of India; security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence relating to the above, or any information which is prohibited under any law for the time being in force" must not be hosted, stored or published. The intermediary must remove or disable access to that information, on the basis of a court order or notice from "the Appropriate Government or its agency" as early as possible, and at most 36 hours from receipt of notice.

Pursuant to section 3(1)(j), an intermediary must comply within 72 hours with government orders to "provide information under its control or possession, or assistance to the Government agency which is lawfully authorized for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents

The new rules further require all social media intermediaries to establish a grievance redress mechanism should “a user or a victim make [a] complaint against violation of the provisions of this rule or any other matters pertaining to the computer resources made available by it” (article 3(2)). Grievance officers that will be established will have twenty-four hours to acknowledge the complaint and fifteen days to respond to the grievance brought to her or his attention (or 24 hours to remove non-consensual intimate imagery).

Section 4 specifies that designated “significant social media intermediaries,” defined as a social media intermediary having a number of registered users in India above such threshold as notified by the Central Government, will have additional duties. In particular, these intermediaries will have to appoint three different responsible company employees, all of which need to reside in India — a Chief Compliance Officer responsible for ensuring compliance with the Act, a nodal contact person for 24×7 law enforcement coordination, and a grievance officer. The Chief Compliance Officer will be criminally liable for any failure to comply with the Rules.

Under Section 4 of the Rules, significant social media intermediaries providing services primarily in the nature of messaging shall enable the identification of the first originator of a particular message, in the context of the prevention, detection, investigation, prosecution or punishment of an offence. Significant social media intermediaries must also “deploy technology-based measures, including automated tools” to proactively identify non-consensual sexual conduct and previously removed content (Section 4(4)).

Section 6 of the Rules provides that “the Ministry may by order, for reasons to be recorded in writing, require any intermediary, which is not a significant social media intermediary, to comply with all or any of [its] obligations”.

II. International human rights norms and standards on freedom of opinion and expression

Before sharing our comments about the new Rules, we would like to recall that Article 19 of the International Covenant on Civil and Political rights (ICCPR) protects the right of everyone to freedom of opinion without interference. Article 19 of the ICCPR also protects the right to freedom of expression, including the right of everyone to freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, through any media of communication. Furthermore, the Human Rights Council has previously affirmed that “the rights that individuals enjoy offline must also be protected online” (A/HRC/RES/20/8).

Pursuant to Article 19 (3) of the ICCPR, restrictions on the right to freedom of expression must be “expressly prescribed by law” and necessary “for respect of the rights or reputations of others” or for “the protection of national security or of public order, or of public health or morals”.

Under Article 20 of the ICCPR, the State must also prohibit propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, violence or hostility, while complying with the requirements in Article 19(3) (CCPR/C/GC/34 para. 50). We appreciate the responsibility of the State to regulate expressions that meet the requirement of Article 19 (3) and Article 20 of the ICCPR. However, we would like to caution against the adoption of broadly defined

legislation which may result in undue restrictions to freedom of opinion and expression.

a) Grounds for restrictions

Under international law, restrictions must be provided by law and be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly. In this regard, terms such as content that is "racially or ethnically objectionable", "harmful to child", "impersonates another person", "threatens the unity… of India," "is patently false and untrue", "is written or published with the intent to mislead or harass a person […] to cause any injury to any person", are overly broad and lack sufficiently clear definitions and may lead to arbitrary application. The terms do not rigorously define grounds for restrictions and fail to provide adequate guidance on the circumstances under which content may be blocked, removed or restricted, or access to a service may be restricted or terminated, thereby falling short of the legality requirement under international human rights law.

More specifically, we would like to underscore that false and untrue information is protected under international human rights law. In its General Comment no. 34, the Human Rights Committee has made clear that the ICCPR does not permit general prohibition of expressions of an erroneous opinion (CCPR/C/GC/34 para. 49). The Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda[1] published by my mandate and regional experts on freedom of expression, sets out the applicable human rights standards in this context. While noting with concern that disinformation may harm individual reputations and privacy, or incite to violence, discrimination or hostility against identifiable groups in society, the Joint Declaration made clear that general prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news," are incompatible with international standards for restrictions on freedom of expression, and" should be abolished".

Similarly, removing content that may "mislead" and cause "any" injury to a person is excessively broad. As social media intermediaries deal with a huge amount of content, a rigorous definition of the restriction of freedom of expression is critical for them to protect speeches that are legitimate under international law, such as the expression of dissenting views. A sufficiently precise definition is essential to prevent the possibility that legitimate expressions is taken down on political or other unjustified grounds. It will ensure that the new rules do not have a chilling effect on independent media reporting.

b) Role of companies

We express serious concern about the obligations on companies to monitor and rapidly remove user-generated content, which we fear is likely to undermine the right to freedom of expression. In particular, we worry that intermediaries will over-comply with takedown requests to limit their liability, or will develop digital recognition-based content removal systems or automated tools to restrict content. As emphasized by our predecessors, these techniques are unlikely to accurately evaluate cultural contexts and identify illegitimate content. We are worried that the short deadlines, coupled with the aforementioned criminal penalties, could lead service

[1] https://www.ohchr.org/Documents/Issues/Expression/JointDeclaration3March2017.doc

providers to remove legitimate expression as a precaution to avoid sanctions.

Private companies have a responsibility to respect human rights, per the UN Guiding Principles on Business and Human Rights. However, the outsourcing of content moderation by requiring private companies to remove broad categories of content, without an order of a court or independent administrative authority, may run contrary to international standards on freedom of expression. Content removals must be undertaken "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, para. 66). We note as well the judgement of the Supreme Court in the case *Shreya Singhal vs. Union of India*, of 24 March 2015, in which the Supreme Court clarified that content restrictions may only come from a reasoned order from a judicial, administrative, or government body.

Noting that the Ministry of Electronics and Information Technology directed Twitter to shut down over 1,000 accounts under Section 69A of the Information Technology Act, on 31 January 2021, on grounds that these accounts were spreading misinformation about farmers' protests, we worry that the new Rules may provide the authorities with the power to censor journalists who expose information of public interest and individuals who report on human rights violations in an effort to hold the government accountable. We would like to emphasize that the respect for diversity, pluralism and independent information is a necessary condition for the functioning of any democratic society.

Lastly, we are seriously concerned about the ability foreseen in the Rules to subject individual employees to criminal liability, given the availability of less punitive measures. The severity of the envisaged penalties incentivizes the restriction of content and is likely to have a chilling effect on freedom of expression.

III. International human rights standards related to the right to privacy

Article 17 of the ICCPR provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence". It permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant", is in pursuit of "a legitimate aim" and "meet[s] the tests of necessity and proportionality" (A/69/397, para. 30).

The rights to privacy and to freedom of expression are interlinked in the digital age -- and encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40). As pointed out by our predecessors, encryption and anonymity provide individuals, including journalists, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, human rights defenders and others, with a zone of privacy to hold, share and develop opinions and exercise their freedom of expression without arbitrary and unlawful interference or attacks (A/HRC/29/32).

The Special Rapporteur on the right to privacy has consistently supported encryption as an "effective technical safeguard" that can, among other technical solutions, contribute to the protection of the right to privacy (A/HRC/31/64, para 50). He has made recommendations in favor of the incorporation of encryption capabilities to software applications and hardware devices through "privacy by design" (ibid) and

welcomed court decisions rejecting the breaking of encryption as "disproportionate, privacy-intrusive measures" (A/HRC/31/64, para 58). See also recommendations to States to provide comprehensive protection for secure digital communications by promoting strong encryption and anonymity-enhancing tools, products and services (A/HRC/43/52 paras 28(b), 45(k), 52(a)(b); 2018 A/73/45712, para 117(d)).

It is also for this reason that the Human Rights Committee has affirmed that attacks on a person because of the exercise of his or her right to freedom of expression may not be justified by article 19 (3) of the ICCPR. While these principles apply in all cases of targeted surveillance, they have particular force when expression in the public interest is implicated. The Human Rights Committee notably singled out the importance of protecting journalists and persons who engage in the gathering and analysis of information on human rights situations and who publish human rights-related reports, including judges and lawyers (CCPR/C/GC/34 para. 23). If users fear that their conversations are no longer private, there is a serious concern that the new Rules will create a climate of self-censorship.

We are seriously concerned that Section 4 may compromise the right to privacy of every Internet user. We are notably concerned by the ability of executive authorities to issue orders to access to user data and restrict content, which seems to take place outside of any judicial oversight mechanism that would hold authorities accountable. Ineffective procedural safeguards and oversight can only contribute to limiting opportunities for accountability, which in turn can generate further human rights violations.

We are further concerned that Section 4 establishes a general monitoring obligation that will lead to the monitoring and filtering of user-generated content at the point of upload. This form of restriction would enable the blocking of content without any form of due process even before it is published, reversing the well-established presumption that States, not individuals, bear the burden of justifying restrictions on freedom of expression (A/73/348).

Lastly, we are troubled that these provisions will in effect not only apply to "Significant social media intermediary", but potentially to any intermediary. In fact, Section 6 of the Rules provides that "the Ministry may by order, for reasons to be recorded in writing, require any intermediary, which is not a significant social media intermediary, to comply with all or any of [its] obligations". Such an unfettered discretion conferred to the executive authorities poses serious risks for the freedom of expression and the right of privacy of every Internet user.

IV. Concerns regarding interference with media freedom

Part III of the Rules applies to publishers of news and current affairs, which includes "newly received or noteworthy content, including analysis, especially about recent events primarily of socio-political, economic or cultural nature, made available over the internet or computer networks"; as well as publishers of online curated content, defined as "any curated catalogue of audio-visual content, other than news and current affairs content, which is owned by, licensed to or contracted to be transmitted by a publisher of online curated content, and made available on demand, including but not limited through subscription, over the internet or computer networks". As such, it could apply to domestic and international news outlets alike, but also to any publications from bloggers, human rights defenders and others.

Publishers of digital news media are required to establish a grievance procedure, appoint a grievance officer, establish a self-regulatory body, register with the Ministry of Information and Broadcasting and adhere to the Code of Ethics provided in the Appendix.

In order to ensure the adherence to the Code of Ethics by publishers, the Rules create under section 14 an Inter-Departmental Committee consisting of representatives of Government officials only. During a hearing related to complaints regarding alleged violations or contraventions of the Code of Ethics, the Committee shall make recommendations for the Ministry to take various actions, including warning, censoring, admonishing or reprimanding such entity; or even block, delete or modify content. Section 16 provides that "in any case of emergency nature, for which no delay is acceptable", the Secretary, Ministry of Broadcasting may if s/he considers it "necessary or expedient and justifiable" issue an order to block content without hearing.

We are seriously concerned that such broad powers given to the executive authorities, without judicial review, is likely to unduly restrict the free flow of information, which is protected by Article 19 (2) of the ICCPR. It is essential that the oversight mechanism be an autonomous body, independent from any pressure, especially political pressure. We worry that the Rules grant a government agency extensive powers to order the blocking of content in the absence of any meaningful safeguards in violation of international standards on freedom of expression. Moreover, website blocking is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in line with international standards on human rights. In practice, website blocking is disproportionate in the vast majority of cases since blocking orders are not sufficiently targeted and involve the restriction of access to perfectly legitimate content.

Regarding the Code of Ethics itself, Part II provides that: "A publisher shall take into consideration India's multi-racial and multi-religious context and exercise due caution and discretion when featuring the activities, beliefs, practices, or views of any racial or religious group".

As repeatedly emphasized in this letter, broadly or vaguely worded provisions that may be used to restrict the freedom of expression are not only incompatible with the requirement of legality, but risk that the scope of the restrictions are broader than necessary to achieve the legal objective. We are particularly concerned that broad wording may result in the arbitrary targeting of anyone who may criticize the government, or express ideas or opinions that are unpopular, controversial or minority. In fact, we are seriously concerned that such expansive definitions could be interpreted to unduly restrict the exchange of ideas and information online, which would in turn jeopardize the independence of India's digital news media.

Concluding observations

We are concerned that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, in their current form, do not conform with international human rights norms. As noted in previous communications sent to your Excellency's Government, we are concerned that these new rules come at a time of a global pandemic and of large-scale farmer protests in the country, where the

enjoyment of the freedom of opinion and expression, including the right to receive information, and the right to privacy, is particularly important for the realization of several other civil, cultural, economic, political and social rights. We would like to recall that restrictions to freedom of expression must never be invoked as a justification for the muzzling of any advocacy of multiparty democracy, democratic tenets and human rights (CCPR/C/GC/34 para. 23).

As a global leader in technology innovation, India has the potential to develop a legislation that can place it at the forefront of efforts to protect digital rights. However, the substantially broadened scope of the Rules is likely to do just the opposite.

We would therefore encourage the Government to take all necessary steps to carry out a detailed review of the Rules and to consult with all relevant stakeholders, including civil society dealing with human rights, freedom of expression, privacy rights and digital rights. We understand the new Rules were issued under the Information Technology Act of 2000 and therefore, were not subject to parliamentary review or opened for consultation with stakeholders. We believe such consultations with relevant stakeholders are essential in order to ensure the final text is compatible with India's international legal obligations, in particular with Articles 17 and 19 of the ICCPR. We stand ready to provide your Excellency's Government with any technical advice it may require in this endeavour.

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 after 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 our highest consideration.

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

Clement Nyaletsossi Voule
Special Rapporteur on the rights to freedom of peaceful assembly and of association

Joseph Cannataci
Special Rapporteur on the right to privacy