TRILEGAL

Information Technology Rules, 2021

(Guidelines for Intermediaries and Digital Media Ethics Code)

This analysis covers:

ANALYSIS

On 25 February 2021, the Ministry of Electronics and Information Technology (MeitY) notified the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 (Rules) in consultation with the Ministry of Information and Broadcasting (MIB). The Rules have been issued pursuant to the government's rule making powers under Section 87 of the Information Technology Act, 2000 (IT Act) which includes rules in relation to the guidelines to be followed by intermediaries, and blocking of access to content under the IT Act. The Rules supersede the erstwhile Information Technology (Intermediary Guidelines) Rules, 2011 (Old Intermediary Guidelines), and considerably expand the scope to impose additional obligations on social media intermediaries and digital media entities.

The Government has notified new rules to regulate intermediaries and digital media. The rules impose additional obligations on certain social media intermediaries and aim to regulate online content by prescribing a code of ethics and a three-tiered grievance redressal mechanism for publishers.

Changes to the Old Intermediary Guidelines have been in the pipeline for years. In 2018, draft amendments to the Old Intermediary Guidelines were released by MeitY for public consultation (2018 Draft). Since then, Indian courts have discussed issues such as the dissemination of fake news and sexually violent/ explicit content on intermediary platforms, and the traceability of originators of messages or information on messaging platforms, highlighting the need for an updated legal framework that promotes accountability.

At the same time, multiple public interest litigations have been filed before various high courts seeking regulation of online content published by over the top (OTT) platforms. While the industry has adopted various self-regulatory codes to address the MIB's concerns, the government has time and again expressed its dissatisfaction and found the codes to lack independent third-party monitoring.

These Rules seek to address all these issues and to regulate the following categories of intermediaries and digital media entities:

1. intermediaries and social media intermediaries (including significant social media intermediaries)
2. publishers of news and current affairs content, including news aggregators, news agencies, and individual news reporters to the extent they are transmitting content in the course of a systematic business, professional or commercial activity; and
3. publishers of online curated content, which appear to include publishers (including individual creators) transmitting content in the course of a systematic business, professional or commercial activity.

The Rules are divided into two parts –

Due diligence obligations	Code of ethics and related safeguards and procedures
Due diligence obligations applicable to intermediaries, including social media intermediaries, which will be administered by the MeitY.	Code of ethics and related safeguards and procedures applicable to entities in the digital media space, which will be administered by the MIB.

This update provides a brief overview of the provisions introduced by the Rules.

1 Part A – Intermediaries

1.1 Obligations applicable to intermediaries

Under the IT Act, intermediaries will be entitled to safe harbour protections from liability in relation to any third-party information, data, or communication link made available or hosted by them (Safe Harbour Protection) if they observe due diligence, as prescribed under the Rules (Due Diligence Requirements), and additionally meet the content neutrality conditions under section 79 of the IT Act.

The Rules transpose the requirements that existed under the Old Intermediary Guidelines (such as the requirement to prominently publish the terms of use, privacy policy and user agreement), and prescribe the following additional requirements:

a. Annual notifications to users[1]: All intermediaries must periodically, and at least once every year, inform its users of any change to the rules and regulations, terms of use or privacy policy and the consequences of non-compliance (such consequences include the termination of the access/usage rights of the user and/or the removal of non-compliant information).

   The Rules expand the list of prohibited information under the Old Intermediary Guidelines to include any information that (i) is patently false and untrue and has been written or published with the intent to harass or mislead for financial gain, or cause injury to any person; (ii) is patently false or misleading, but is knowingly and intentionally communicated and can be reasonably perceived as a fact; and (iii) is invasive of a person's bodily privacy and is insulting or harassing on the basis of gender.

b. Take down procedure: The Rules prescribe the following take-down procedure:

   i. In line with section 79(3)(b) of the IT Act, the Rules provide that upon receipt of actual knowledge in the form of a court order or upon being notified by the appropriate government or its agency, the intermediary should not host, store or publish any unlawful information. The intermediaries must remove or disable access to unlawful content within 36 hours from the receipt of such order or direction and may also voluntarily take down any prohibited information. Compliance with take down requests or voluntary removal of information will not dilute the Safe Harbour Protection.

   ii. As a limited exception to the requirement of a court order mentioned above, on receipt of any complaint from an individual or person on their behalf regarding content which is prima facie in the nature of any material depicting nudity or any sexual act, or the impersonation of any person including artificially morphed images, the intermediary must take all reasonable measures to remove or disable access to such content within 24 hours of receipt of the complaint.

   This will not apply to information that is temporarily or transiently stored by the intermediary in an automatic manner, and which does not involve any human, automated or algorithmic editorial control.

[1] A user is any person or publisher who accesses or avails the computer resource of an intermediary for the purpose of hosting, publishing, sharing, transacting, viewing, displaying, downloading or uploading information. It includes other persons jointly participating in using such computer resource, including the addressee and originator. The definition of users has been expanded to include users that view or download the content, or are involved in indirect use/access of the intermediary's computer resource.

c. Grievance redressal mechanism: In addition to the requirement to appoint a grievance officer and publish their name and details as provided under the Old Intermediary Guidelines, the Rules require an intermediary to constitute a grievance redressal mechanism and to acknowledge receipt of user complaints within 24 hours and resolve disputes within 15 days (as compared to the earlier requirement of 30 days). The grievance officer is also required to receive and acknowledge any order, notice or direction issued by the appropriate government, competent authority or a court.

d. Retention of records: Intermediaries must retain information and user registration records for a period of 180 days (as compared to the earlier requirement of just 90 days) from (i) date of removal or disabling access to any unlawful information pursuant to receipt of actual knowledge or on voluntary basis or upon receipt of any grievances received by it and (ii) additionally in case of any cancellation of registration or withdrawal of a user.

e. Assistance to the Government Agencies: While there was always a requirement to provide any information or assistance to authorised government agencies for verification of identity, prevention, detection, investigation or prosecution of unlawful offences or for cyber security incidents, the Rules require this information to be provided within 72 hours from the receipt of the order.

f. Obligations for News and Current Affairs Content: In addition to these compliances, any intermediary which transmits News and Current Affairs (defined in Part B below) content on behalf of publishers, such as an entity aggregating and displaying News and Current Affairs created by publishers on its platform, must comply with the following additional requirements:

   i. publish a clear and concise statement on its website and/or mobile application, informing publishers to furnish details of their user accounts to the MIB.

   ii. provide a demonstrable mark visible to all users of the compliance by the publisher of the requirement to share information with the MIB.

1.2 Additional Obligations for Significant Social Media Intermediaries

The Rules create a subset of intermediary, called 'significant social media intermediary' (SSMI), which is defined as a social media intermediary with 50 lakh (5 million) registered users. The term 'social media intermediary' (SMI) has been defined as an 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.

Given that the definition of SMI uses the word ‘primarily’ without providing any further details, it is unclear as to what extent entities that enable social online interaction between users otherwise than in a purely social media setting, such as search engines (Google’s hyperlocal social search), e-commerce entities (Flipkart’s review features), cloud telephony providers, etc., would be covered by this definition. There is also room for considerable uncertainty in the definition of SSMI as it is not immediately apparent how registered users would be identified by intermediaries that do not have a real name policy or which have not been designed to classify users along geographical lines.

SSMIs are subject to additional obligations which must be complied with over the next 3 months (i.e. before 24 May 2021). The additional obligations applicable to SSMIs are as follows:

a. **Resident Officers and Local Presence**: Each SSMI must appoint an Indian resident employee as Chief Compliance Officer (CCO), Grievance Redressal Officer (GRO) and the nodal person of contact of the SSMI. Of these, the CCO must be a senior employee or a key managerial personnel. The SSMI must also have a physical contact address in India to receive communications. There will, no doubt, be tax implications, such as the implication of having a 'Permanent Establishment' in India, as a result of complying with this requirement. There is however no requirement to incorporate a local entity under the Rules.

b. **Identification of the first originator**: SSMIs that provide messaging services must enable the identification of the first originator of information if required by an order passed by a court or competent authority under section 69 of the IT Act. It must provide the court or government authority with a copy of the information relating to the first originator in electronic form. Such order can be issued in the interest of sovereignty and integrity, security, public order, defamation, etc. If the first originator is located outside the territory of India, then the first originator for the information in India must be identified by the SSMI.

   The Rules clarify that there is no obligation on SSMIs to disclose the content of the communication while complying with such order. Despite this, intermediaries may be required to do so under section 69 of the IT Act which empowers the government to pass orders for interception or monitoring or decryption of any information in the interest of sovereignty and integrity, defence, security of the State, friendly relations with foreign States or public order or for prevention of incitement of any cognizable offence relating to the same or for investigation of any offence. This issue of traceability of originators of message or information on messaging platforms is currently before the Supreme Court in several cases, such as Antony Clement Rubin v. Union of India[2]. The Supreme Court is likely to rule on this point and its judgement may impact this requirement under the Rules.

c. **Use of technology-based and automated tools**: SSMIs must endeavour to use automated tools to proactively identify and remove unlawful content, including content depicting rape and child sexual abuse in any form. While doing so, it must ensure that the use of such tools is balanced against the interests of its users, including their freedom of speech and expression and privacy. SSMIs must also implement appropriate mechanisms to ensure human oversight in order to evaluate the accuracy and frequency of these tools, their propensity for bias and discrimination and their possible impact on privacy and security.

d. **Monthly Compliance Report**: SSMIs must publish monthly compliance reports indicating details of complaints received, action taken thereon, and the number of specific communication links or parts of information removed or access disabled as a result of proactive monitoring using automated tools.

   The obligation to publish these details appears to be quite extensive since this will require the publication of baseless complaints as well and is expected to result in a slightly increased compliance cost for organisations.

e. **Grievance redressal mechanism**: In addition to implementing appropriate mechanisms for grievance redressal, SSMIs must also enable the tracking of the status of complaints by providing a unique ticket number for every compliant or grievance received. It must also, to the extent possible, provide reasons to the complainant for any action taken or not taken.

[2] WP Nos. 20774 and 20214 of 2018.

f. Advertised or marketed services: If an SSMI provides services or transmits information on behalf of another person, to which it owns a copyright or has entered into an exclusive licensing or contractual arrangement, for direct financial benefit, or which targets the receiver of the information, it must clearly indicate that the information is being advertised, sponsored or exclusively targeted to the recipient.

   It is not clear how an entity that carries out such targeting will be able to meet the content neutrality conditions under Section 79 of the IT Act. It is also unclear whether such requirement would be met by labelling the information appropriately, or whether it would require general or specific statements to be published for each advertised/sponsored piece of information.

g. Voluntary Verification for Users: SSMIs must enable voluntary verification for users registering for its services from India or using their services in India, by using mechanisms such as verification by active mobile number of such user. Once such verification is completed, the user must be provided with a demonstrable mark of verification visible to all other users of the services.

h. Notification of action taken against prohibited content: If an SSMI voluntarily removes or disables access to unlawful content, it must

   i. notify the user who had created, uploaded, shared, disseminated or modified such content;

   ii. provide reasonable opportunity to such user to dispute such action and request for reinstatement; and

   iii. ensure that the grievance officer maintains oversight over such dispute resolution.

   Under the Rules, MeitY can pass an order requiring an intermediary (which is not an SSMI) to comply with the above additional due diligence requirements applicable to SSMIs, if it believes that such intermediary's services create a 'material risk of harm' to the sovereignty and integrity of India, security of the State, friendly relations with foreign States or public order. The order can also be passed for a specific part of an intermediary's services, and the assessment must include whether the intermediary's services allow for interaction between users, and whether the publication or transmission of information results in widespread dissemination of such information.

1.3 Consequences of Non-Compliance with Part A

In case of non-compliance with Part A, intermediaries may lose their Safe Harbour Protection and be subject to the various liabilities as provided under the IT Act and other content agnostic laws such as Indian Penal Code 1860.

2 Part B – Digital Media - Regulation of Publishers of News and Current Affairs and Online Curated Content

2.1 New Definitions introduced

This part of the Rules is administered by the MIB and prescribes obligations on publishers of news and current affairs content and online curated content. In this context, the Rules lay down certain key definitions, which are set out below.

a. News and Current Affairs

The term news and current affairs content (News and Current Affairs) has been defined to include newly received or noteworthy content, such as analysis about recent events primarily of socio-political, economic or cultural nature.

b. Online Curated Content

The term online curated content (Online Curated Content) has been defined as any curated catalogue of audio-visual content, which is owned by, licensed to or contracted to be transmitted by a publisher of Online Curated Content, and made available on demand, by way of subscription or otherwise. It includes films, audio visual programmes, documentaries, television programmes, serials, podcasts and other such content, but excludes News and Current Affairs content.

c. Publisher of News and Current Affairs

A publisher of News and Current Affairs content has been defined as an online paper, news portal, news aggregator, news agency or any entity whose functions are similar to publishers of News and Current Affairs content but excluding print media such as newspapers and their replica e-papers and individuals publishing such content pursuant to non-commercial activities.

d. Publisher of Online Curated Content

A publisher of Online Curated Content has been defined as a publisher who makes available to users, a computer resource through which they can access Online Curated Content and performs a significant role in determining what Online Curated Content is made available but excludes individuals publishing such content pursuant to non-commercial activities.

e. News Aggregator

A news aggregator has been defined as an entity which makes, aggregates, curates and presents News and Current Affairs content. It makes available a computer resource to users through which they can access News and Current Affairs and performs a significant role in determining what News and Current Affairs content is available.

2.2 Key Obligations

The key obligations under this Part are as follows:

a. Code of Ethics

Publishers of News and Current Affairs Content and Online Curated Content, which operate in India[3], or systematically make their content available in the territory of India, must observe, and adhere to, the Code of Ethics prescribed under the Rules. For instance, publishers of News and Current Affairs Content must, amongst other requirements, comply with the Norms of Journalistic Conduct issued by the Press Council of India, whereas publishers of Online Curated Content must self-classify such content on the basis of context, impact, target audience, etc., and restrict access to 'A' rated content by a child through the implementation of appropriate access control measures[4].

A summary of the Code of Ethics is provided as an Annexure to this update.

b. Requirement to Furnish Information

The Rules require a publisher operating in the territory of India, to furnish certain information (such as details of the entity) to the MIB within 30 days of publication of the Rules. These publishers are also required to publish monthly compliance reports with the details of the grievances received.

c. Adoption of a three-tiered regulatory framework for grievances

The Rules envisage a three-tier regulatory framework for grievance redressal. This framework is applicable to publishers that operate in India. It is not clear whether this framework will apply to publishers who have no physical presence in India.

i. **The first level (Self-Regulation by publisher):** Each individual publisher must establish a grievance redressal mechanism, appoint a Grievance Officer in India and publish the name and contact details of this officer on its platform. The Grievance Officer will be the point of contact for all grievances relating to the Code of Ethics and will also act as the nodal point for all interactions with the complainant, the self-regulating body and the MIB.

ii. **The second level (Creation of self-regulating body):** The Rules provide for the creation of one or more self-regulating bodies consisting of publishers/industry experts which would be headed by a retired judge of the Supreme Court/High Court and registered with the MIB. The MIB will publish a charter for these self-regulating bodies including codes of practice. The publisher must become a member of any one of theself-regulating bodies and abide by the terms and conditions of such body. The self-regulating body can address grievances that the publisher fails to resolve within 15 days, hear appeals from the complainant and issue guidance or advisories to the publishers requiring them to issue apology, censor the content or include disclaimers or warning cards. In addition, the self-regulating body will also oversee and ensure that the publisher adheres to the Code of Ethics. If the publisher fails to comply with any guidance or advisory issued by the self-regulating body, then the latter can refer such grievance to the oversight mechanism set up by the government (Oversight Mechanism) within 15 days. The self-

[3] Under the Rules, a publisher is deemed to 'operate in the territory of India' where such publisher has a physical presence in the territory of India.
[4] Access control mechanism has been defined as any measure through which access to online curated content may be restricted based on the verification of the identity or age of a user, including any technical measures implemented in this regard.

regulating body cannot, itself, issue any direction for the removal or modification of unlawful content - it can only refer such content to the Oversight Mechanism.

iii. **The third level (Oversight by the Government):** The MIB has the power to establish an Inter-Departmental Committee (Committee) for hearing and examining grievances. This Committee can only issue its recommendations to the MIB and cannot pass any direction or order against the publisher. MIB can also issue guidance, advisories, order and direction to the publishers for adherence with the Code of Practice.

At the hearing stage, after examining the grievance, the Committee can issue recommendations to the MIB requiring removal or modification of the content in the interest of sovereignty, integrity, defence, or in order to prevent cognizable offence. In case of recommendations pertaining to the removal or modification of content, the authorised officer appointed by the MIB (Authorised Officer) is required to place the Committee's recommendation before the MIB for its consideration, who upon receiving approval from the MIB can issue directions to the publisher or the intermediary seeking removal or modification of the relevant content. The Rules provide that the orders and directions issued by the Authorised Officer can only be in respect of a specific piece of content and cannot require any entity to cease its operations.

In an 'emergency' where no delay is acceptable, the Authorised Officer will review the content and determine whether it violates the grounds relating to sovereignty and integrity, defence, security of the State, friendly relations with foreign States or public order or for prevention of incitement of any cognizable offence relating to the same as provided under Section 69A of the IT Act and can submit its recommendations to the MIB for removal of such content. If the MIB is satisfied, then it may issue an interim order under Section 69A for immediate blocking of this content without giving any opportunity of hearing.

It appears that, in the garb of self-regulation, the MIB could well exercise considerable regulatory control over publishers as well as the content posted on online platforms.

d. Disclosure Requirements on the Publisher

Publishers operating in India must publicly disclose, and display details of all grievances received by it, the manner in which the grievances are disposed of, the action taken on the grievances, replies sent, orders or directions received, and action taken. This information must be updated monthly.

This will create additional and onerous obligations on publishers and will require them to provide far more information than necessary.

e. Retention of records

The Rules require publishers to preserve the records of content transmitted by it for a minimum period of 60 days and make this information available to the self-regulating body or the Central Government or other government body, if requisitioned.

2.3 Statutory basis for Part B and Consequences of non-compliance

Both Part A and Part B (as discussed above), have been notified under the IT Act. However, the Rules do not make it clear what the statutory basis for Part B is. While the provisions that empower the Central Government to make rules is wide, as per the recent amendment to the Allocation of Business Rules, 1961 (Business Rules), digital media, news and Online Curated Content fall within the purview of the MIB and not the MeitY or the IT

Act. The Business Rules expressly state that digital/online media consisting of (i) films and audio-visual programmes made available by online content providers and (ii) news and current affairs content on online platforms would be governed by the MIB. It is not entirely clear how MeitY has issued Rules on the regulation of digital media, news and Online Curated Content, or whether the MIB can even enforce rules issued by MeitY.

Further, other than the limited exception of content that may be taken down in extreme circumstances under Section 69A of the IT Act, by virtue of issuing take down orders either to the publisher or the intermediary, it is also unclear what the statutory consequences for non-compliance with Part B would be. Several other issues can be inferred from the Rules, including the applicability of the Rules to foreign publishers due to the lack of consistency in the applicability of Part B.

3 Analysis and way forward

While the regulation of content hosted by intermediaries might be necessary, given the increased use of social media, the scope of the obligations as well as the inclusion of digital media will mean that the Rules will have far reaching consequences.

The definition of social media intermediaries is vague and could include any service provider that enables interactions amongst users. The increase in compliance requirements is likely to result in higher volumes of user complaints and access requests by government agencies, making it difficult for entities to address them in the short time frames that have been prescribed under the Rules. Their impact on the delivery of content over the internet is significant and entails practical risks and compliance costs for entities. Provisions such as permitting the tracing of originator of the information drastically undermines the privacy of individuals.

Besides this, the fact that blocking orders can be issued by the MIB to publishers of News and Current Affairs or Online Curated Content in cases of 'emergency nature' provide extensive powers under the garb of self-regulation. The Rules issued by the MeitY and under the IT Act also aim to regulate digital media entities, which are currently allocated to the MIB, and this raises concerns regarding the legislative backing of the Rules.

4 Annexure - Code of Ethics

4.1 News and Current Affairs Content:Publishers of News and Current Affairs content are required to:

a. adhere to the Norms of Journalistic Conduct issued by the Press Council of India, and Programme Code under the Cable Television Networks (Regulation) Act, 1994;

b. not publish or transmit content which is prohibited under any law.

4.2 Online Curated Content:Publishers of Online Curated Content are required to:

a. display ratings of the Online Curated Content such as 'U', or 'U/A 7+,' or 'U/A 13+', or 'U/A 16+', or 'A' prominently to its users in a manner that will ensure that the users are aware of the ratings before accessing such content;

b. self-classify the Online Curated Content on the basis of context, tone and impact, target audience and theme (i.e. violence, nudity, sex, language, drug abuse and horrors);

c. ensure that Online Curated Content which is prohibited by law or by court of competent jurisdiction is not transmitted or published or exhibited by it;

d. 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 in the Online Curated Content;

e. take into consideration and take due caution and precaution before transmitting or hosting any content which (i) affects the sovereignty and integrity of India, threatens, endangers or jeopardises the security of the State; (ii) is detrimental to India's friendly relations with foreign countries; and (iii) likely to incite violence or disturb the maintenance of public order;

f. restrict access to 'A' rated content by a child through the implementation of appropriate access control measures; and

g. take reasonable efforts to improve the accessibility of online curated content transmitted by it to persons with disabilities through the implementation of appropriate access services.