ERGO

KHAITAN &CO ADVOCATES SINCE 1911

# Amendment to Rule 3(1)(d) of the IT Rules, 2021 – A step towards greater accountability in Takedown Orders to Online Intermediaries

24 October 2025

## Background

On 22 October 2025, the Ministry of Electronics and Information Technology (MeitY) amended Rule 3(1)(d) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (2021 Rules), which imposes an obligation on intermediaries (such as social media platforms, online marketplaces, etc.) to takedown unlawful content. The amendment will come into force on 15 November 2025.

The stated objectives of this amendment are to bring greater transparency and accountability to governmental processes in issuing takedown orders under Rule 3(1)(d), and to ensure that there are reasonable safeguards in place to balance the freedom of speech with legitimate regulatory oversight.

In particular, this amendment narrows the category of officers empowered to issue takedown orders, mandates disclosure of reasons for issuing such orders, and institutes a monthly review of issued takedown orders in order to ensure that regulatory intervention is proportionate and compliant with legal standards.

## Key Changes under the Amended Rule 3(1)(d)

Prior to the amendment, Rule 3(1)(d) of the 2021 Rules required intermediaries to remove or disable access to information available on their platforms, pursuant to a court order, or a direction from *the "Appropriate Government, or its agency"*. The Information Technology Act, 2000 (IT Act) defines "*Appropriate Government*" to mean either the Union or State Government. The pre-amendment version of Rule 3(1)(d) therefore authorised any department or agency of the Union or State Government to issue content takedown orders to intermediaries.

The only restrictions imposed by Rule 3(1)(d) – prior to the amendment – were in respect of the nature of content in relation to which a takedown order could be issued (although this effectively covers any and all unlawful content)[1], and that the order had to be issued by an officer specifically authorized to do so. This formulation allowed a wide range of government and law enforcement officers and agencies—often at relatively junior levels—to issue takedown requests.

A number of intermediary platforms raised concerns regarding this practice, which was leading to tremendously large volumes of takedown requests, many lacking clarity on the legal basis, factual context, or specific URLs/content to be taken down.

In addition, intermediaries also raised concerns regarding the difficulty in determining whether a particular officer was in fact authorized to issue takedown orders. This absence of standardisation often made it difficult to assess or comply with such requests in a timely manner.

---

[1] Rule 3(1)(d) both prior, and subsequent to amendment provide that takedown orders may be issued in respect of, "*any 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*".

While the amended rule does not narrow down the scenarios in which a takedown order can be issued, it takes steps towards addressing some of the above concerns through additional procedural safeguards, namely:

- Restricting the authority to issue takedown orders to:
    - officers of a rank equivalent to Joint Secretary, or where an officer at such rank is not appointed, a Director, in respect of the Government of India, or State Government, or their respective agencies; or
    - officers of a rank equivalent to the Deputy Inspector General of Police in the case of law enforcement agencies.
- Requiring that all such orders set out reasons for their issuance; and
- Instituting a monthly review of all takedown orders, to ensure that such orders are necessary, proportionate, and consistent.

This stricter authorisation threshold represents a marked departure from the earlier position, creating a more disciplined and reason-oriented approach to takedown governance.

Interestingly, this amendment also arrives in the wake of a push lead by the Ministry of Home Affairs, through the Indian Cyber Crime Coordination Centre (I4C), to have Union and State Governmental departments and law enforcement agencies to duly designate nodal officers, as required by (pre-amendment) Rule 3(1)(d), and to onboard these governmental departments, law enforcement agencies, and intermediaries onto the Sahyog Portal, a single-window platform to process takedown and data disclosure orders.

## Unresolved Overlaps and the Continuing Section 69A Question

The revised framework brings Rule 3(1)(d) conceptually closer to the process prescribed under Section 69A of the IT Act and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (**Blocking Rules**). Under Section 69A, blocking directions can only be issued by officers of a rank of Joint Secretary of the Government of India, and must adhere to detailed procedural safeguards, including inter-departmental review and recording of reasons in writing.

The Supreme Court in *Shreya Singhal v. Union of India* (2015) rejected a challenge to the validity of Section 69A, partly because of these safeguards. By adopting similar procedural rigour—particularly the requirement that reasons be disclosed—the amendment reflects a conscious move towards greater consistency between the takedown and blocking frameworks.

While this alignment enhances procedural credibility, it also intensifies an ongoing ambiguity between the scope of Section 69A and Rule 3(1)(d).

Section 69A empowers the Government to *block* access to information on grounds of sovereignty, integrity, public order, and national security, following a closed internal process. Rule 3(1)(d), on the other hand, allows the Government to *require intermediaries to remove or disable access* to information that is *unlawful under any law for the time being in force*—a potentially broader and more open-ended formulation, that nonetheless includes each of the grounds set out in Section 69A. To compound the confusion, the Blocking Rules framed under Section 69A also provide for a mechanism where the Government issues blocking orders directly to intermediaries.

The two mechanisms thus coexist uneasily. The new amendment, by making the procedural architecture under Rule 3(1)(d) more similar to Section 69A, may accentuate questions as to when a particular direction should be issued under one provision rather than the other.

Notably, in a recent case, the Karnataka High Court dealt with a challenge to the legality of the Sahyog Portal and Rule 3(1)(d) of the 2021 Rules, including on the grounds that Rule 3(1)(d) of the 2021 Rules, and Section 69A of the IT Act operate in the same circumstances, but (the unamended) Rule 3(1)(d) allows for fewer checks and balances, allowing Government and law enforcement agencies to effectively bypass necessary safeguards.

While the Karnataka High Court has upheld the legality of the Sahyog Portal, its judgment does not deal with this objection or otherwise reconcile how Rule 3(1)(d) and Section 69A are to be reconciled. This issue therefore remains an open question for the moment.

## Practical Implications for Intermediaries and Enforcement Agencies

From a compliance perspective, the amendment offers several practical benefits.

- **Greater clarity and accountability:** Intermediaries have long raised concerns that takedown orders were frequently issued by junior officers without adequate reasoning or specificity. The requirement that only senior officers issue reasoned directions should enhance the quality of orders and reduce interpretative ambiguity.
- **Improved operational efficiency:** Law enforcement agencies have conversely argued that intermediaries are often slow to act on legitimate requests, citing lack of clarity. A more structured process—backed by reasoned orders and clear chain of command—could enable quicker and more definitive responses.
- **Facilitating constructive engagement:** The Sahyog Portal also allows intermediaries to indicate when a takedown request lacks necessary information or appears to have other defects. This feature, coupled with the amendment's emphasis on reasoned orders, could foster a more transparent and iterative exchange between intermediaries and government authorities – fostering a more cohesive, and less adversarial regulatory regime, without compromising the freedom of speech of individual users of intermediary platforms.

- *Supratim Chakraborty (Partner); Madhav Khosla (Counsel) and Himeli Chatterjee (Associate)*

## About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**