



Bills and Acts: India Amended Information Technology Rules

For Prelims: Amendments to the Information Technology Rules 2021, Article 14, Article 19, Article 21

For Mains: Amendments to the Information Technology Rules 2021, Government Policies & Interventions

Why in News?

Recently, the Ministry of Electronics and IT (MeitY) has notified amendments to the [Information Technology \(Intermediary Guidelines and Digital Media Ethics Code\) Rules, 2021 \(IT Rules, 2021\)](#).

- In a bid to keep up with the issue of regulating **social media intermediaries (SMIs)**, India in 2021, replaced its decade old regulations on SMIs with the IT Rules, 2021 that were **primarily aimed at placing obligations on SMIs** to ensure an open, safe and trusted internet.

What are the New Amendments?

- **New Guidelines for Social Media Intermediaries:**
 - Currently, intermediaries are only required to inform users about not uploading certain categories of harmful/unlawful content. **These amendments impose a legal obligation on intermediaries** to take reasonable efforts to prevent users from uploading such content. The new provision will ensure that the intermediary's obligation is not a mere formality.
 - The amendment **requires intermediaries to respect the rights guaranteed to users under the [Articles 14, 19 and 21](#)** of the Indian Constitution, therefore, including a reasonable expectation of due diligence, privacy and transparency.
 - The amendments also mandate that **"rules and regulations, privacy policy and user agreement"** of the platform should be made available in all languages listed in the eighth schedule of the Constitution.
- **Amendments to the Rule 3:**
 - The grounds in **subclause 1 of rule 3 (rule 3(1)(b)(ii))** have been rationalized by removing the words **'defamatory' and 'libellous'**.
 - Whether any content is defamatory or libellous will be determined through judicial review.
 - Some of the content categories in subclause 1 of rule 3 (rule 3(1)(b)) have been **rephrased to deal particularly with misinformation, and content that could incite violence between different religious/caste groups.**
- **Expedient Removal of Prohibited Content:**
 - SMIs are now obligated to remove information or a communication link in relation to the **six prohibited categories of content** as and when a complaint arises. They **have to remove such information within 72 hours of the complaint being made.** Given the virality with which content spreads, this is an important step to contain the spread of the

content.

- **Establishment of Grievance Appellate Committee(s):**
 - Grievance Appellate Committee(s) will be **established to allow users to appeal against the inaction of, or decisions taken by intermediaries on user complaints.**
 - However, users will always have the right to approach courts for any remedy.
 - Further, the IT Rules, 2021 **do not provide any explicit power to the GAC to enforce its orders.** Lastly, if users can approach both the courts and the GAC parallelly, it could lead to conflicting decisions often undermining the impartiality and merit of one institution or the other.

What are the Key IT Rules, 2021?

- **Mandates Social Media to Exercise Greater Diligence:**
 - Broadly, the IT Rules (2021) mandate social media platforms to **exercise greater diligence with respect to the content on their platforms.**
- **Establish a Grievance Officer:**
 - They are required to establish a grievance redressal mechanism and remove unlawful and unfitting content within stipulated time frames.
 - The grievance officer of the platform's **redressal mechanism is responsible for receiving and resolving complaints of the users.**
- **Ensuring Online Safety and Dignity of Users:**
 - Intermediaries **shall remove or disable access within 24 hours of receipt of complaints of contents** that exposes the private areas of individuals, show such individuals in full or partial nudity or in sexual act or is in the nature of impersonation including morphed images etc.
- **Educating Users about the Privacy Policies:**
 - The privacy policies of the social media platforms **must ensure that users are educated about not circulating copyrighted material** and anything that can be construed as defamatory, racially or ethnically objectionable, paedophilic, threatening the unity, integrity, defence, security or sovereignty of India or friendly relations with foreign states, or violative of any contemporary law.

Why is there a Need for New IT Laws?

- **India Entering into Digital Age:** India is going to have a **trillion-dollar digital economy** in a few years, and a large number of businesses will be on the Indian Internet.
 - Therefore, an open & secure Internet becomes an important economic component of our country.
- **Rise of Splinternet:** The global internet as we know it is on the verge of splintering into smaller bubbles of national networks due to aggressive national policies, trade disputes, censorship, and dissatisfaction with big tech companies.
 - This will have **far-reaching consequences that impact international unions, data enterprises and individual consumers alike.**
 - Perhaps the most sophisticated instance of a splintered internet today would be China's Great Firewall'.
 - What are seen as essential services, like Google Search and Maps, Western social media, and so on – are **entirely banned and replaced by Chinese alternatives** like Weibo in the name of Cyber Sovereignty.
- **Majority of Cybercrimes in India are Bailable Offense:** A historical mistake was made when the **IT (Amendment) Act, 2008**, made almost all cybercrimes, barring a couple, bailable offences.
 - The focus was more on enhancing the quantum of civil liability and reducing the quantum of punishment, which explains the reason why the number of cybercrime convictions in the country is in single digits.
- **Restricted Cyber Security Remedy:** IT Act is effective in metropolitan cities like Mumbai, Delhi, Hyderabad, Bhopal, Bangalore, etc., but it is feeble in tier-two level cities as awareness of the law

by enforcement agencies remains a big challenge.

- The IT Act **does not cover most crimes committed through mobiles**. This needs to be rectified.

What are Present Government Initiatives for Cyber Security?

- [Cyber Surakshit Bharat Initiative.](#)
- [Cyber Swachhta Kendra.](#)
- [Online cybercrime reporting portal.](#)
- [Indian Cyber Crime Coordination Centre \(I4C\).](#)
- [National Critical Information Infrastructure Protection Centre \(NCIIPC\).](#)
- [Information Technology Act, 2000.](#)

What can be the Way Forward?

- The government is looking at a new legislative framework with the **new rulemaking capabilities** that deal with various issues related to digital space. This should include:
 - The majority of cybercrimes need to be made [non-bailable offences](#).
 - A comprehensive [data protection regime](#) needs to be incorporated in the law to make it more effective.
 - Cyber war as an offence needs to be covered under the IT Act.
 - Parts of [Section 66A of the IT Act](#) are beyond the reasonable restrictions on freedom of speech and expression under the Constitution of India. These need to be removed to make the provisions legally sustainable.
- Increasingly [bilateral or multilateral arrangements](#) **between countries** will have to evolve in such a way that nothing can be done in isolation from other countries.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

- (a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)