

**ADVANCED DIPLOMA IN MEDIA LAWS -2022-2023
PERSONAL CONTACT PROGRAMME- (Second Round)**

**DAY 2- Session 3-
Regulating Harmful Content under the
Information Technology Act, 2000 -
Administrative Structures and Substantive
Remedies**

**BY-
Pankhuri Agrawal
Doctoral Candidate, NALSAR University of Law Hyderabad
pankhuri11agrawal@nalsar.ac.in**



**REGULATING HARMFUL
CONTENT UNDER THE
INFORMATION
TECHNOLOGY ACT, 2000
- ADMINISTRATIVE
STRUCTURES AND
SUBSTANTIVE REMEDIES**



- Globalization and privatization - new regulation of e-commerce is necessitated
- UNCITRAL Model Law on Electronic Commerce, 1996
- Information Technology Act, 2000 -
Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures
3. Offenses and Contraventions
4. Justice Dispensation Systems for Cyber crimes -
- ITAA 2008 (Information Technology Amendment Act 2008) - Cyber Terrorism and Data Protection



Four Major Concerns:

Censorship - Art. 19(1)(a) and S. 69A, IT Act + Indian Telegraph Act

Surveillance - S. 69 and 69B, IT Act

Intermediary Liability- S. 79, IT Act

Cyber Security

Refer:

**[IT-Act-Amendment_Online-28-MAR-23.pdf](#)
[\(broadbandindiaforum.in\)](#)**

CENSORSHIP - S. 69A OF THE IT ACT

69A. Power to issue directions for blocking for public access of any information through any computer resource.—(1) Where the Central Government or any of its officers specially authorised by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.

(2) The procedure and safeguards subject to which such blocking for access by the public may be carried out, shall be such as may be prescribed.

(3) The intermediary who fails to comply with the direction issued under sub-section (1) shall be punished with an imprisonment for a term which may extend to seven years and also be liable to fine.

CENSORSHIP - S. 69A of the iT ACT

Processes and safeguards for the blocking of content are prescribed under the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (the "*Blocking Rules*").

Rule 3 - Central Government nominate a Joint Secretary as the "Designated Officer" to exercise the power of blocking online content.

Rules 4 and 6 - government agencies, central and state governments, and ministries may appoint "Nodal Officers" who are tasked with receiving a complaint from the public, assessing the need to take action under Section 69A, and further notifying the Designated Officer.

Rules 7 and 8 - Hereafter, each blocking request must be evaluated by a Committee of Examiners

On receiving a blocking request - Designated Officer make "all reasonable efforts" to identify the person or the intermediary who has hosted the impugned information online, - issue a notice to them to appear before the Committee and present their case opposing the proposed blocking.

The Committee examine the blocking request to determine whether it falls within the parameters of Section 69A(1) of the IT Act.

Designated Officer sends the Committee's recommendations to the Secretary of the Department of Information Technology, who takes the final decision regarding blocking.

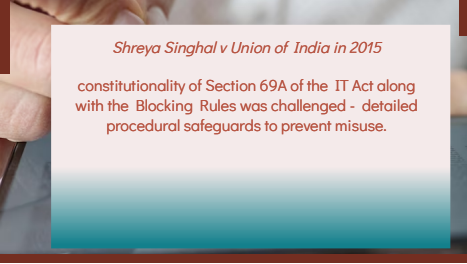
Upon approval, the Designated Officer directs the concerned government agency or intermediary to block the offending content.

Exception to prior notice:

Rule 9 - blocking content in cases of an emergency. However, such an action must be confirmed within 48 hours. (TikTok case)

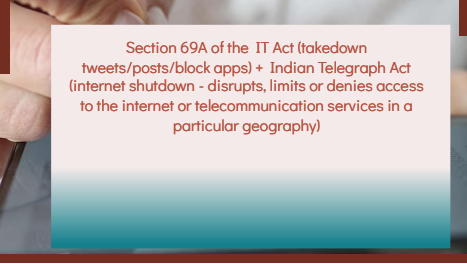
Rule 14 - a three member "Review Committee" (comprising of the three top bureaucrats) must meet once every two months to assess the compliance of the Committee's directions with Section 69A of the IT Act.

Rule 16, - strict confidentiality to be maintained regarding *"all the requests and complaints received and action taken thereof"*

A close-up photograph of a hand holding a pen, with the pen tip pointing towards the bottom left. The background is slightly blurred, showing what appears to be a document or a laptop keyboard.

Shreya Singhal v Union of India in 2015

constitutionality of Section 69A of the IT Act along with the Blocking Rules was challenged - detailed procedural safeguards to prevent misuse.



Section 69A of the IT Act (takedown tweets/posts/block apps) + Indian Telegraph Act (internet shutdown - disrupts, limits or denies access to the internet or telecommunication services in a particular geography)

Intermediary Liability

Due diligence clauses:

Section 79 of the Information Technology Act 2000 says that Intermediaries, like Google, Yahoo, Facebook, My Space etc are not liable for third party information if they observe due diligence while discharging their duties.

Private censorship through the use of intermediary liability frameworks

Section 79 of the IT Act and rules:

- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the “2021 IT Rules”) and
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 (“*2022 Amendment*”).

The due diligence standards - through these standards - and the proscription of obscenity, insults or harassment on the basis of gender, racially or ethnically objectionable - "that elements of decency and morality (which are not part of the Section 69A framework) are brought into censor content online." (BFI Report)

“ “due diligence” conditions (pre) + “actual knowledge” (post)

Initially, the actual knowledge standard was interpreted as a simple notice and take down framework. (over-compliance issues)

- Section 79(3)(b) - *Shreya Singhal v Union of India* - only after receiving a court order or based on notice from the government. (“*otherwise it would be very difficult for intermediaries like Google, Facebook etc. to act when millions of requests are made and the intermediary is then to judge as to which of such requests are legitimate and which are not.*”)

Information Technology ministry introduced the Information Technology(Intermediaries guidelines) Rules, 2011

- Emphasizes that the website hosts' obligations to perform "due diligence."
- Increase the responsibility of intermediaries in the pre-crime scenario, in terms of keeping a close watch over the kind of content that is put on the website by the end-user.
- Exempt intermediaries in post-crime scenario if steps are taken to curb the illegal activity of the end-user or disable access to the illegal content.

Concerns and Challenges:

- Non-involvement of civil society, media stake holders or people's representatives to voice their views
- 2021 IT Rules and the 2022 amendments provides broad obligations on intermediaries under the garb of "due diligence" guidelines
- Rule 3(1)(b) of the 2021 Rules - intermediaries to insert terms of use - that informs users that they must not publish or host any content that breaches a list of proscribed content. But the 2022 amendment require intermediaries to "make reasonable efforts" to prevent their users from publishing such content.

Concerns and Challenges:

- Rule 3(1)(j) - intermediaries to provide “information or assistance” to any government agency within 72 hours - (strictly governed by Section 69 of the IT Act 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (*“Surveillance Rules”*) notified thereunder.)
- The 2021 IT Rules - intermediaries to dispose off the complaint within 15 days. But 2022 amendment - removal request for certain specified types of content must be resolved within 72 hours
-

Concerns and Challenges:

Section 79 and the 2021 and 2022 IT Rules privatise censorship functions by passing the buck to intermediaries to serve as watchdogs over the content on their platform - made to police content - ten broadly worded subjective categories such as content that is - in the opinion of the user or an intermediary- "ethnically objectionable", "misleading in nature", "insulting other nation", "patently false and untrue" or "defamatory" (BIF Report)

-

Concerns and Challenges:

- Grievance Appellate Committee(s)" (GAC) : decide user appeals against the decision of social media intermediaries.
- The GAC is constituted of – *"a chairperson and two whole time members appointed by the Central Government, of which one shall be a member ex-officio and two shall be independent members."*
- Rule 4(2) - "significant social media intermediary" (which provides messaging services (such as WhatsApp) - identify the 'first originator' of messages based on a judicial order or order of a competent authority under Section 69 of the IT Act (concerning surveillance).

-

These rules require intermediaries to adopt terms of service that prohibit users from hosting, displaying, publishing, sending or sharing any proscribed content, including not just obscene or infringing content, but also any material that threatens national "unity" or "integrity," "public order," or is that "grossly offensive or menacing in nature," "disparaging," or "otherwise unlawful in any manner whatever." It is criticized that such a broad standard lacks clear limits on what kinds of content may be taken down and invites abuse.



The law thus imposes a duty that once an intermediary discovers, or is notified of proscribed content, it must "disable" the content within 36 hours. Under the rules, intermediaries are also authorized to immediately terminate access or usage rights. They must also preserve related user records for 90 days for investigatory purposes. This is not a flexible, discretionary standard: under the rules, intermediaries must "strictly follow the provisions of the Act or any other laws."

SURVEILLANCE- AUTHORITY TO INTERCEPT:

Section 69:

1. The Central Government/State Government/ its authorized agency can
2. intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource
3. if it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence or for investigation of any offence.

AUTHORITY TO INTERCEPT:

- Mumbai terrorist attacks of 2008, the Ministry of Home Affairs intercepted and documented mobile-phone communications between the gunmen and their Pakistan-based handlers.
- In May 2010, Outlook revealed transcripts of phone tapping that included politicians from the ruling party, which were captured using a GSM monitoring device.
- Nira Radia phone tapping case

AUTHORITY TO INTERCEPT:

Prosecution for Expression Crimes on Internet:

- Arrest of Lakshmana Kailash K for allegedly defaming an Indian historical figure Chatrapathi Shivajee online. (Google and a major ISP cooperated with a police investigation- later found wrong IP address)
- Arrest of two men for posting derogatory comments about Congress party Chief Sonia Gandhi on Orkut;
- Arrest of a magazine editor on defamation charge

AUTHORITY TO INTERCEPT:

Individual Freedom and State Power: Article 19 and 21

Freedom of speech and expression and Right to Privacy

In August 2010 it was reported that the Ministry of Home Affairs (MHA) had asked the Department of Telecommunications to suspend newly introduced 3G mobile service and halt providers' ongoing rollout of the technology, particularly in Jammu and Kashmir.

Expecting violence in Ayodhya in the wake of judgment on the dispute, the Government blocked mass text messages across India on September 23, 2010, which was later extended as the verdict was deferred.

By May 2007, Google had cooperated with the Mumbai police regarding online communities and comments directed against the Indian historical figure Shivaji, right-wing leader Bal Thackeray, and Father of the Indian Constitution Dr. B. R. Ambedkar.

CONCLUSION

Complying with the IT Act is essential for digital businesses operating in India. It ensures legal validity, security, and trust in electronic transactions. Businesses must stay updated with the Act's provisions and implement necessary measures to comply.

Indian Computer Emergency Response Team (CERT-IN) was created in 2003 within the MCIT's (Ministry of Communication and Information Technology's) Department of Information Technology.

CERT-IN serving as a nodal agency for accepting and reviewing requests from a designated pool of government officials to block access to specific websites.

When it decides to block a site, it directs the Department of Telecommunications to order all licensed Indian ISPs to comply with the decision.

No review or appeals are provided.

The Controller of Certifying Authorities (CCA), a government agency under the Department of Information Technology, is the agency that is entrusted under the IT Act with the power to block websites.



Criticism against making of the Rules

What is the remedy if some content is wrongfully removed? Such remedy was available under the rules of the 1998 United States' Digital Millennium Copyright Act (DMCA). It is criticized that the users in India do not have any recourse if their content is removed wrongfully. Nor are there any safeguards against abuse: the rules do not require that the party lodging the complaint have any rights or even have a good faith basis for believing that the content is illegal.

THANK YOU