

ADVANCED DIPLOMA IN MEDIA LAWS -2023-2024
PERSONAL CONTACT PROGRAMME- (SECOND ROUND)

DAY 1- SESSION 1-
REGULATING HARMFUL CONTENT UNDER THE
INFORMATION TECHNOLOGY ACT, 2000 -
ADMINISTRATIVE STRUCTURES AND SUBSTANTIVE
REMEDIES

BY
Pankhuri Agrawal
Assistant Professor, School of Law, BML Munjal University Gurgaon



**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 –

1. Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures
3. Offenses and Contraventions
4. Justice Dispensation Systems for Cyber crimes

-

- 1. Censorship - Art. 19(1)(a) and S. 69A, IT Act + Indian Telegraph Act**
- 2. Intermediary Liability- S. 79, IT Act**
- 3. Surveillance - S. 69 and 69B, IT Act**
- 4. Cyber Security**

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

Section 69

Power to issue directions for interception or monitoring or decryption of any information through any computer resource:

¹ [69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource.--(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that 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 relating to above or for investigation of any offence, it may subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.

...Section 69

Power to issue directions for interception or monitoring or decryption of any information through any computer resource:

(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to--

(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or

(b) intercept, monitor, or decrypt the information, as the case may be; or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.

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.

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, - Designated Officer make “all reasonable efforts” to identify the person or the intermediary who has each blocking request must be evaluated by a Committee of Examiners
On receiving a blocking request 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*”

Shreya Singhal v Union of India (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- S. 79, IT Act

- *Avnish Bajaj vs. State*
- ITAA 2008 (Information Technology Amendment Act 2008)-

Safe Harbour provision

2001-08- Narrow definition of intermediary and protection only for offences under IT Act

Post 2008 Amendment- Intermediary- *“any person, who on behalf of another person, receives, stores or transmits any particular electronic record or provides any service with respect to that record.”*

Section 79. Exemption from liability of intermediary in certain cases

¹[79. Exemption from liability of intermediary in certain cases.--(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him.

(3) The provisions of sub-section (1) shall not apply if--

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

The Information Technology (Intermediary Guidelines) Rules, 2011 ("**Intermediary Guidelines**") - primary guidelines which intermediaries need to observe to avail safe-harbour protection.

These guidelines list out the due diligence requirements that must be observed by intermediaries to avail the safe-harbour protection.

Actual knowledge by itself or by aggrieved + Due Diligence

Shreya Singh v. Union of India - to state that *actual knowledge* can be attributed to an intermediary only when there is a court order or notification from an appropriate government authority apprising the intermediary of unlawful content over its platform.

The 2021 Rules :

It supersede the 2011 guidelines for internet intermediaries.

Aim: Provide a robust complaint mechanism for social media and OTT platform users

The 2021 Rules classify the regulated entities into the following types:

Social media intermediary with less than 50 lakh registered Indian users;

Significant social media intermediary ("SSMI") with more than 50 lakh registered Indian users;

Publisher of news and current affairs_content including news aggregators,

Publisher of online curated content which covers all online streaming platforms including Over-the-Top ('OTT') platforms.

The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021: Focusing on The 2023 Amendment

PART II

DUE DILIGENCE BY INTERMEDIARIES AND GRIEVANCE REDRESSAL MECHANISM

- Rule 3(1)(b)(v) required intermediaries to make reasonable efforts not to host content that:

“deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any misinformation or information which is patently false and untrue or misleading in nature or, in respect of any business of the Central Government, is identified as fake or false or misleading by such fact check unit of the Central Government.”

Rule 7. Non-observance of Rules.—

Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

Also, Section 69A of the IT Act, 2000 elucidates the procedure to issue takedown orders, which these notified amendments could bypass.

Contrary to *Shreya Singhal vs Union of India* (2015), a verdict with clear guidelines for blocking content.

Equality and Due Process –Single authority to decide – CHILLING EFFECT - Article 19

No judicial oversight

Bombay HC's *Kunal Kamra v Union of India* judgment (2024)

- Division Bench (two Judges) - split verdict on the constitutionality of the 2023 amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (“**IT Rules**”).
- Justice Neela Gokhale upheld Rule 3(1)(b)(v) while Justice Gautam Patel struck it down.

J. Gokhale	J. Patel
After flagging of content by the FCU - the intermediary acts according to its “ <i>existing policy</i> ” and can either remove the content but also show a disclaimer or warning to users that the content is false	After flagging of content by the FCU - the intermediary will obviously remove the content (for safe harbour provision)
Loss of safe harbour -intermediary liable only when hosting unlawful speech, and the intermediary could always defend itself against such liability in court	Safe harbour provision protects free speech right

Surveillance - S. 69 and 69B, IT Act

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