INDIALAW

CYBER LAW

Intermediary Liability in the Digital Age: Judicial Enforcement and the Ramkumar Decision

AUTHOR Appurv Bhatia, Aditi Rana

PUBLISHED 23 July 2025

Introduction

As India's digital ecosystem rapidly expands, courts and regulators are increasingly confronted with the challenge of online harm, ranging from child sexual abuse material (CSAM) and non-consensual intimate imagery (NCII) to defamatory and unlawful content. Central to this challenge is the doctrine of intermediary liability: how far should digital platforms be held accountable for the content they host?

The recent decision of the Madras High Court in Ramkumar v. Union of India (2025) provides a critical perspective on the judicial expectations from intermediaries and the State in preventing access to content involving child sexual exploitation.

Legal Framework for Intermediary Liability

Under Indian law, the key provision governing intermediary liability is Section 79 of the Information Technology Act, 2000, which provides "safe harbour" to intermediaries, shielding them from liability for third-party content, provided they observe due diligence and act upon receiving actual knowledge of unlawful content.

This protection was clarified by the Supreme Court in Shreya Singhal v. Union of India[1], the Supreme Court clarified that intermediaries are required to take down content only upon receiving a court order or a notification from the appropriate government agency. The Court struck down Section 66A of the IT Act for being unconstitutional, and also read down Section 79(3)(b) of the IT Act and Rule 3(4) of the IT (Intermediaries Guidelines) Rules, 2011, holding that mere private complaints do not impose a legal obligation on intermediaries to act. Liability or takedown obligations arise only when the intermediary is notified by a competent authority."

To operationalize this, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, further mandate that intermediaries must:

- Publish clear grievance redressal mechanisms.
- Appoint compliance officers (for significant platforms).
- Remove notified content within 36 hours of receiving a government or judicial direction.

Ramkumar v. Union of India (Madras High Court, July 2025)

In Ramkumar[2], the petitioners approached the Madras High Court seeking removal of a film teaser allegedly depicting child pornography, hosted on YouTube and accessible via Google India. The teaser of the film "Bad Girl" was said to contain sexually explicit content involving schoolchildren, in alleged violation of the POCSO Act, IT Act, and constitutional protections under Article 21 and Article 39(f).

Although YouTube LLC was not impleaded, the Court held that the Ministry of Electronics and Information Technology (MeitY) had the authority and duty to issue appropriate directions to remove such content. Google India argued it had no role in content moderation, but the Court emphasized the social responsibility of intermediaries, noting that even procedural lapses (like non-impleadment) cannot outweigh the urgency of child protection.

The Court directed MeitY to ensure removal of the identified URLs within one month and instructed the National Commission for Protection of Child Rights and National Commission for Women to monitor and take further action. It refused to wait for impleadment of YouTube LLC, recognizing that the State has a continuing duty to act in cases of ongoing online harm.

Judicial Trends: Toward Proactive Accountability

While Ramkumar builds on the foundation laid in Shreya Singhal, it subtly marks a shift in judicial reasoning. Courts are increasingly prioritizing harm prevention over procedural technicalities in digital safety matters.

This trend is further reflected in the Supreme Court's order in X v. Union of India[3], where the Court dealt with the circulation of non-consensual intimate images (NCII) of a female advocate. The Supreme Court directed the Government to create a centralized takedown mechanism and emphasized the duty of intermediaries to implement global takedowns in such cases. While distinct from Ramkumar, the X ruling complements it by reinforcing that constitutional rights to privacy, dignity, and protection from digital abuse must shape the scope of intermediary responsibilities.

Conclusion

The jurisprudence on intermediary liability in India is increasingly shifting from a passive safe-harbour model toward a responsibility-driven framework. While statutory protections under Section 79 remain intact, courts are now interpreting them in light of fundamental rights, public interest, and platform capabilities.

The Ramkumar judgment affirms that intermediaries cannot remain neutral conduits when the content involves serious violations like child exploitation. At the same time, the judgment reinforces that government agencies cannot abdicate their duty to act merely because platforms are privately owned or located abroad.

As digital platforms continue to influence social norms and public safety, intermediary accountability will remain central to India's cyberlaw jurisprudence.

For more details, write to us at: contact@indialaw.in

1. (2015) 5 SCC 1 ??
2. Writ Petition No.5562 of 2025 ??
3. (WP No. 25017 of 2025) ??

Related Practice Areas

Cybersecurity and Incident Response | Information Technology