



Social Media Intermediary Liability in India: Balancing Freedom of Expression, Online Safety and Platform Accountability

Dr. Vishva Nath Sharma

Associate Professor, Department of Law, Invertis University, Bareilly

Article Info: (Received- 10/11/2025, Accept- 20/12/2025, Published- 06/01/2026)
DOI- [10.65919/ijahssc.2026.v2i1007](https://doi.org/10.65919/ijahssc.2026.v2i1007)

Abstract

Social media intermediaries have become central to contemporary communication, public debate, and the dissemination of information in India, creating complex questions concerning freedom of expression, online safety, and platform accountability. This paper examines the legal and constitutional framework governing intermediary liability in India, with particular emphasis on the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. It analyses the scope of safe-harbour protection under Section 79, due-diligence obligations, content moderation, grievance redressal mechanisms, and governmental powers relating to blocking and regulation of online content. The study further evaluates the constitutional relationship between freedom of speech under Article 19(1)(a), reasonable restrictions under Article 19(2), and privacy and personal liberty under Article 21. Important judicial decisions, including *Shreya Singhal v. Union of India*, *Anuradha Bhasin v. Union of India*, and *K.S. Puttaswamy v. Union of India*, are considered to understand evolving judicial approaches. The paper also discusses challenges involving misinformation, hate speech, algorithmic accountability, transparency, and global platform governance. It concludes that India requires a balanced regulatory framework that protects legitimate expression while ensuring effective accountability, procedural fairness, user safety, transparency, and meaningful institutional oversight.

Keywords: Social Media Intermediaries, Intermediary Liability, Freedom of Expression, Safe Harbour, Online Safety, Platform Accountability, Content Moderation.

1. Introduction

The Information Technology (IT) Act, 2000, introduced the first legal framework for the regulation of electronic commerce and cyber-related crimes in India. Recent amendments to the Act also contain provisions for regulating social media platforms operating in the country. The provisions on intermediaries are significant in this regard. They lend support to the balancing of freedom of expression with the need to counter harmful content online. The principle of balancing is important because on one hand,

India is a country with a vibrant social-media landscape where its citizens willingly use social media platforms to express their views and communicate with others. On the other, India also has the largest number of people in the world subjected to hateful and harassing forms of content. This challenges the demands of public order that form one of the permissible grounds for restricting freedom of expression under Article 19(2) of the Constitution of India. Three fundamental questions arise from the law regulating intermediaries: What must intermediaries do to receive safe-harbour immunity from liability for third-party content? What should intermediaries do to ensure the online safety of their users without unduly limiting their freedom of expression? What must be required of intermediaries to increase accountability for user-generated hateful, harassing, and obscene content while still enabling other forms of expression? The recent case law on these questions, especially the judgments of the Supreme Court and High Courts, illuminates the constitutional and legal position in India. It is also important to see how other jurisdictions, particularly in the US and the UK, have grappled with these difficult questions and the lessons to be drawn.

2. Legal Framework and Definitions

The Information Technology (IT) Act, 2000 establishes two broad categories of online intermediaries: access service providers and content intermediaries. Access service providers facilitate internet access to the public; content intermediaries offer services (such as hosting) that enable users to create, store, and share information. A third category—significant social media intermediaries (SSMIs)—is assigned additional responsibilities, due to their popularity and the volume of objectionable content they host. SSMIs play an essential role in the global distribution and dissemination of content but also face a plethora of harmful content, including misinformation and disinformation, hate speech, and child sexual exploitation and abuse. The extent of these harms has prompted increased scrutiny of and responsibility for SSMIs, both in India and overseas. The principle of constitutional balance plays a crucial role in promoting freedom of expression while ensuring online safety and security. At one end lies freedom of speech and expression under Article 19(1)(a); at the other lies the right to life and personal liberty under Article 21, which includes the right to privacy, the right to protection from hatred, and the right to protection from sexual abuse, especially for children. The wide range of content hosted by SSMIs also calls for attention, with these platforms acting as digital homes for both creative and legitimate expression and hateful, harassing, and obscene material. Balancing the constitutional imperatives of safety and freedom is, thus, fundamental to the governance of SSMIs.

2.1. Information Technology Act, 2000 and Amendments

The legal framework regulating social media intermediary liability is primarily established by the Information Technology Act 2000 and generally elaborated by the rules therein. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 elaborate the law further with respect to social media platforms as well as other news-related intermediary platforms, the former receiving more intensive regulation. Since the largest platforms including Facebook, Twitter, YouTube, and WhatsApp are U.S.-based, the laws they are subject to are not U.S. laws but Indian laws. The free speech protection framework in these jurisdictions is a function of judicial interpretation and application of civil society activism rather than law-making. The trade-off between individual freedom and state sovereignty remains.

2.2. Provisions Relevant to Intermediaries

Chapter II of the Information Technology Act deals with the cybersecurity of India. Section 69 provides the government with the authority to monitor and block any

information generated, transmitted, received, stored, or hosted in violation of law, sovereignty, dignity, or security, public order, or for reasons noted in the clause. Section 70 empowers the government to declare any computer resource as protected resource and give direction to certain agencies, which may be a violation of law or those who can monitor the information for the purpose of ensuring security. Under section 69E, any service provider shall provide information or assistance as required by entity, or as required. The government can also restrict by creating rules, any information from maintaining computers, or which can be used for monitoring, gathering.

Chapter III of the Act deals with the intermediary safeharbour provisions. Section 79 provides immunity to intermediaries from being held liable for any third-party information while acting as a mere conduit or those of which they are not aware or is not to their knowledge. Section 79A empowers the central government to make rules for instituting a cyber-ecology to enable safe and secure online interest for children and minors and also to issue directions when it is expressly provided to do so.

3. Constitutional and Fundamental Rights Context

Freedom of speech and expression is a fundamental right guaranteed under Article 19(1)(a) of the Constitution of India. It is also a right recognised under the International Covenant on Civil and Political Rights (ICCPR) to which India is a party. However, Article 19(2) allows the State to impose reasonable restrictions on freedom of speech and expression in the interests of, inter alia, public order. Reasonable restriction on the right to privacy is provided in Article 21 of the Constitution, which states that no person shall be deprived of his life or personal liberty save by procedure established by law. The recognition and emerging jurisprudence on the laws of privacy guarantee provided under Article 21 of the Constitution thus have a bearing on the manner in which the safety and security of users of public platforms, such as social media, both majorly and minors, ought to be treated.

Section 69A of the IT Act provides a mechanism and procedure for blocking of information generated, transmitted, received, or stored in any computer resource. Sub-section (1) of the provision enables the Central Government or any of its officers-specially designated to issue directions for blocking the access of the public to any information through any computer resource, if such information is 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 is inciting the commission of any cognizable offence relating to the above. Sub-section (2) provides that such blocking shall be in accordance with the procedure and safeguards prescribed by the Central Government.

3.1. Freedom of Speech and Expression under Article 19(1)(a)

Article 19(1)(a) of the Indian Constitution guarantees to all citizens the right to freedom of speech and expression. This essential right has been held by the Supreme Court to include the right to impart and receive information. Hence, the vast array of information that is available through social media is entitled to protection under Article 19(1)(a). However, it is also necessary to bear in mind that the right to free speech is not an absolute right and falls within the ambit of Article 19(2), which empowers the State to make laws that impose restrictions. The limitation must be consistent with a democratic society such as that envisaged by the Constitution of India. A well-structured balance between freedom of speech and expression and other competing societal interests is the hallmark of a civilized and cultured society.

Public order is one of the grounds available to the State for restricting the right to freedom of speech and, by necessary implication, the right to receive speech-related

content in the context of social media. Content that tends to undermine or disrupt public order can result in violence, damage to property, serious disruption to the level of public tranquility and safety, revolts against the State, disobedience of laws prescribed for the maintenance of public order, and riots. Social media platforms allow content users to share and receive a multitude of ideas, opinions, and information about events. However, the idiom and manner in which those ideas are expressed are not insulated from the restrictions outlined in Article 19(2).

3.2. Right to Privacy and Data Protection Considerations

The rapidly evolving information ecosystem, especially the development and large-scale deployment of digital information networks, presents new challenges to the protection of personal information. Information in digital form is easily susceptible to unauthorized collection, storage, mining and profiling, use, disclosure, and even destruction. With the exponential increase in data, a heightened awareness among the public regarding information security, coupled with a variety of technological advancements in the area of data surveillance and the focus on intellectual property and cyber laws, makes it imperative that a legal framework that ensures the protection of information is put in place.

The right to privacy has been recognised as a fundamental right. Furthermore, data protection is an important constituent of the right to privacy. Privacy has been recognized in many cases as one of the grounds for the reasonable restrictions under clause (2) of Article 19 and clause (1) of Article 21 specifically bars deprivation of life or personal liberty, except according to procedure established by law. With these aspects in mind, the advisory group has endeavoured to analyse the needs of data protection in the Indian context and emphasizes the need to develop a data protection regime that will be harmonized internationally while at the same time meeting the requirements of information and communication technology (ICT) sectors.

4. Balancing Mechanisms: Accountability, Safety, and Expression

The liability debate centres on user-generated content. Platforms are generally considered mere conduits—exempt from liability for content they do not create. Governments can impose few obligations on conduits. Intermediaries user-generated content share the conduit approach. A huge philosophy of Internet governance and regulation reasonably expects limited liability for intermediaries. The prospect of liability drives intermediaries to over-censor to avoid excessive risk. Emerging notions of digital sovereignty highlights the fundamental disruption of big technology companies' dominance platform Internet operations and space, violating sovereign governance and freedoms (Li, 2018).

Platforms have three options to moderate user-generated content. They may scramble, impose “friction” mechanisms—a cumbersome posting process to make participation more difficult, detrimental to users' ability to express themselves. Platforms might simultaneously oversee content compliance with domestic laws and international human rights principles to minimise arbitrary takedowns, as “rule of law” (Bayer, 2019). A balance opportunity affordable with well-resourced platforms developing innovative models.

4.1. Due Diligence and Compliance Obligations

The legal framework governing social media intermediaries imposes significant obligations to ensure the safety of users of these platforms. In the context of Section 79, a provider of an online computer resource is not liable to any person in respect of any third party information made available by them if it: (a) has taken reasonable steps to identify and remove such information as soon as it became aware of it. Such

due diligence constitutes an obligation under sub-rule (2) of Rule 3 of the 2021 Rules issued by the Ministry of Electronics and Information Technology (MeitY). The due diligence required to be observed by an intermediary is laid down therein and is exhaustive. It comprises 10 conditions covering aspects from registration of users to their verification, redressal of user complaints, removal of unlawful content, formulation of the privacy policy, and monitoring the activity of users. Formulation and publication of rules and regulations, and privacy policy for access or use of the computer resource by any person, clearly specifying the following: (i) the categories of information that will not be accepted. Further, upon receiving actual knowledge, or on being notified by the appropriate government or its agency, that any information under the preceding clause is being communicated, stored or hosted on its computer resource shall remove or disable access to such information. Such rules, privacy policy, and any other such document referred to in this sub-rule shall be published in the manner specified in sub-rule (1) and in case of a significant social media intermediary, in the regional languages where such computer resources are being accessed or used.

4.2. Content Moderation, Proactive Filtering, and Due Process

Content moderation practices adopted by significant social media intermediaries illustrate the tensions involved in balancing freedom of expression and online safety. In India, intermediaries have broadly interpreted the safe harbour provided under the Information Technology Act of 2000, exercising limited control over user-generated content. This legal shield, however, must be reconciled with the need for platforms to take additional due diligence measures against specific forms of unlawful content. Rule 3(2) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, obliges intermediaries to implement suitable content moderation policies, including proactive measures to identify and remove certain categories of harmful material, namely content that violates laws protecting the sovereignty, integrity, and security of India. The overlap between safe harbour provisions and content moderation obligations gives rise to a constitutional conundrum: proactive filtering constitutes moderation and is arguably not compatible with the role of a mere conduit for third-party information; yet if platforms wish to avoid liability for unlawful content, they must engage in such filtering.

4.3. User Rights, Redressal Mechanisms, and Appeals

The provisions of the IT Rules ensure that rights of users of the platform are protected while simultaneously establishing adequate redressal mechanisms within the platform to resolve any grievances that the users might face. Subsequent to the enactment of the IT Rules, it was held in *Anuradha Bhasin v. Union of India* that the Constitution requires the availability and use of an effective and swift remedy for all individuals or groups for alleged arbitrary and excessive restrictions on their rights and freedoms, as well as for loss of life, safety or limb or injury caused by arbitrariness. An adequate and effective remedy is the bedrock of the rule of law in a meaningful democracy, the foundation of which lies in India's constitutional philosophy. The nature of the remedy can and must be commensurate with the nature, gravity or magnitude of the alleged violation of constitutional rights arising from the arbitrary and excessive exercise of power to impose restrictions on the rights and freedoms guaranteed to citizens. These principles apply equally to people who experience a breach of fundamental freedoms because of any action or inaction on the part of a private entity. The IT Rules provide for these procedural safeguards to protect the rights of social media users.

4.4. Platform Responsibilities for Hateful, Harassing, and Obscene Content

Social media platforms in India play a pivotal role in facilitating a shared public

space by enabling users to exchange ideas, information, experiences, and opinions. However, concerns about the proliferation of hateful, harassing, and obscene content have prompted a demand for increased accountability. Internet users should not be subjected to hate speech or harassment, nor exposed to pornographic or obscene content, without their consent. Striking a balance between safety and freedom of expression requires consideration of three key questions: Do current content moderation rules for significant social media intermediaries go far enough in protecting users from hateful, harassing, and obscene content? Can the rules be followed without infringing user rights? Will the rules reduce hate speech and harassment or merely transfer them to less regulated spaces?

Under Rule 4 of the Intermediary Guidelines, a significant social media intermediary must make reasonable efforts to prevent the hosting of any information that constitutes hate speech, harassment or stalking, obscenity or sexually explicit material, or any act which is in violation of any law for the time being in force. While Rule 3(2)(a) requires these intermediaries to establish a grievance redressal mechanism, Rule 4(2) mandates that they “respect and honour users’ rights, dignity, and feelings.” Major and minor violations of these platform obligations have raised questions of efficacy, feasibility, and excessive gatekeeping. The United States Supreme Court is considering a case that examines whether Section 230(c) of the Communications Decency Act provides immunity from liability for a failure to enforce terms of service, including removal of content harmful to others.

5. Case Law and Judicial Trends

The Indian judiciary has regularly issued pronouncements that clarify the scope of intermediaries’ responsibilities and address the issue of removal of content from platforms. In the case of *Anuradha Bhasin v. Union of India*, the Supreme Court recognized that freedom of speech and expression, which includes the right to publish and communicate online, was being infringed as a result of the suspension of Internet access in Jammu and Kashmir. In another significant case, *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the Information Technology Act, which had provided for punishment for sending offensive messages through communication service, etc., on the ground that the provision was capable of abuse and had a chilling effect on free speech.

In *K.S. Puttaswamy v. Union of India*, the Supreme Court stated that the right to privacy is an intrinsic part of the right to life and personal liberty guaranteed by Article 21 of the Constitution and is also protected as an essential aspect of freedom of speech and expression under Article 19(1)(a) and as part of the guarantees in the Constitution governing association and marriage. Online speech must, therefore, be afforded the same safeguards as other forms of communication. The Supreme Court laid down that any restriction on freedom of speech through preventive detention must adhere to the principles of natural justice, which require that the executive must not act as judge in its own cause. In *Internet and Mobile Association of India v. Reserve Bank of India*, the Supreme Court held that measures which have a direct impact on the economy necessitate the highest degree of caution.

5.1. Notable Indian Supreme Court and High Court Judgments

Amendment 45 of the Indian Constitution makes it clear that the right to free speech can be limited by laws formulated in the interest of sovereignty and integrity of India, defence of India, security of the state, foreign relations, public order, decency, morality, contempt of court, defamation, incitement to an offence, and friendly relations with foreign states. The discourse regarding judicial decisions affecting the

constitutional right to free speech grew in intensity during the 2010s and eventually drew attention to the problem of balancing free speech and platform accountability. Notice-and-action provisions were introduced to enhance platform accountability. Notably, if a platform is unable to handle hateful, harassing, or obscene content, it does not mean that the platform does not have to attend to other aspects of user expression (Benge, 2019).

In 2021 alone, the Indian Supreme Court and high courts invoked and interpreted Article 19 in at least three decisions concerning online speech moderated on social media platforms (Sylvain, 2018). Though only a small selection of hearings, these judicial interventions highlight trends in the upper judiciary's approaches to free expression, platform accountability, and intervention in the online space and appetite for sustained engagement in these matters.

5.2. Comparative Perspectives from Global Jurisdictions

Social media platforms like Facebook, Twitter, and YouTube play a key role in online discourse. They are now the primary channels for public communication and debate and for mobilizing public opinion and collective action. An unambiguous settled understanding of their status, functions, and responsibilities is thus a prerequisite for balancing the competing demands of accountability, safety, and expression. The fact remains that private companies dominate the public square. Markets can no longer be relied upon to ensure an appropriate degree of openness: access to the public square is imperfectly regulated and frequently denied. Dominant platforms mediate access to participation and decide the issues, causes, and opinions that get heard. Platform responses to harmful content can impede freedom of speech and limit dissemination of important messages and facts. Comprehensive regulation is still imperfect and incomplete, and platform governance significantly differs from public governance.

5.3. Implications for Online Safety and Freedom of Expression

Recent judgments by the Indian Supreme Court and High Courts have underscored the inadequately addressed issues of online safety, intermediary accountability, and user privacy that arise from the current regime of safe harbours, content moderation, and compliance obligations for social media intermediaries.

The evidence presented to the Court and inherent contradictions in the very nature and functioning of social media raise serious concerns that require urgent consideration. On the one hand, social media platforms possess sweeping powers to moderate speech on their platforms, yet little oversight is placed on these powers through transparent processes and reasoned decision-making. On the other hand, the very nature of social media, in many cases, leads to the proliferation of false, hateful, and incendiary speech. The enormous economies of scale enjoyed by such platforms enable the effective weaponisation of such speech against crucial public interests—be it public order and communal harmony or free and fair democratic elections. Yet, the platforms operate with little responsibility towards mitigating such speech through a considered moderation policy—leaving users to contend with a spate of hateful, incendiary, harassing, and obscene content, and often returning empty-handed even after lawfully following the official takedown process.

6. Regulatory Landscape and Policy Debates

Intermediary liability is an important issue for social media platforms. Landmark legislative developments, including the enactment of the IT Act 2000, represent a significant shift in the legal environment governing online intermediaries in India. Chief among these developments is the introduction of civil and criminal liability for the dissemination of unlawful content. The urgency of the situation is underscored by

the growing use of social media in public discourse, marketing, political communication, and political mobilization, all of which have raised major concerns regarding the targeting of vulnerable individuals and minority groups (Li, 2018).

Legislation and the judiciary are moving in dual tracks, which raises the question of whether any changes made to a legal framework that is already under examination would require further amendments at a later stage. Certain existing provisions of the IT Act concerning online content have come to confer broad liability on intermediaries, depending on interpretations made by courts and enforcement agencies. Conversely, a robust statutory framework has been recommended (Bayer, 2019).

The safe harbour doctrine as a form of liability exemption and the regulations governing the procedures for taking down unlawful content transmitted by intermediaries must be defined. Clarifications are also needed with respect to the functions that can be compatibly performed by intermediaries without incurring liability and greater transparency regarding the identity of the parties making takedown requests (Benge, 2019). At present, the only formal procedure for taking down unlawful content is the Section 69A process, which applies to specific forms of content (technical assistance in drafting requests that comply with this regulation would be beneficial) and media of transmission (its considered application to content transmitted via a public library is debatable).

6.1. Safe Harbour Provisions and Their Scope

Safe harbour provisions insulate technology intermediaries from potential liability arising from third-party user-generated content if such intermediaries act in compliance with due diligence requirements laid out in the Information Technology (IT) Act, 2000 and applicable rules. These provisions are recognised globally and are key to developing countries seeking to ramp up their digital infrastructure. They foster various Internet businesses and innovative models that rely on user-generated content to offer information, products, and services. However, the relaxed treatment of technology intermediaries, especially social media intermediaries, has generated serious concerns among policymakers and regulators in India and internationally. Especially with the global expansion of social media and the rise of large platforms controlling significant — as defined by the IT Rules, 2021 — layers of the Internet for billions of users, the safeguards pervading the position of these platforms' have come under extensive scrutiny.

7. Challenges in Enforcement and Compliance

Treading the line between intermediary protection and criminal accountability is fraught with complexities; the deterrence of harm caused in the digital space suffers from the danger of intermediary apathy, while demands for the removal of immunities in the event of abuse are at constant risk of overreach. The measures outlined for the protection of users are often not implemented for technical or financial reasons. The four major international social-media platforms, operating under local law but bound by global governance structures, are in varying degrees of confrontation with the Indian government. The management of misinformation and disinformation especially in an atmosphere charged with sectarian tension—is all the more urgent given the approaching general election. No intermediary can remain apathetic to its core responsibility: to take down, with due diligence, content that is blatantly false or patently fake, that is obscene or pornographic, that spreads hatred or promotes enmity, and that incites violence or terrorism.

Determining when a piece of content can even be characterized as misinformation or disinformation poses a challenge for all platforms and requires the Indian

government to tread carefully. Therefore, although governments all over the world are implementing legal and regulatory measures to rein in the spread of harmful information within their jurisdictions, they would do well to remember that there is no definite formula for setting a limit on errors in public discourse. Excessive governmental control in this regard could well backfire and provoke backlash.

7.1. Technical Feasibility and Resource Implications

Thumbing an adroit balancing act, the intermediaries already face enormous pressures, managing the vast flows of information on their platforms while also ensuring compliance with a burgeoning range of governmental and non-governmental demands for removal. To comply with these demands, however, is often at odds with the principles of free speech. Moreover, many of the proposed measures not only violate the essence of freedom of speech but are also impractical or technically impossible: in effect, the regulation attempts too much. Instructions to block representation of particular religions, castes, races, and languages, or to ensure that content does not promote feelings of enmity and hatred, are feel-good measures with very real costs.

The content moderators employed by the large Indian intermediaries spend very little time making decisions, little more than 30 seconds per item. Content moderation is typically outsourced to low-cost destinations across Asia and Gen Z countries, where the emotional burden of performing such work (exposure to IS, child sexual abuse material, and other extreme content) is ignored or trivialised by companies over-eager to meet shareholder expectations. If content moderation was cost-free, accordingly, demands could, even if poorly, be implemented without undermining freedom of expression. Funds should also be made available to independent auditing of the platforms' operations.

7.2. Global Platform Governance vs. Local Regulation

Protocols of global platforms, driven by considerations spanning availability, business returns, user engagement, and revenue generation, do not guarantee local safety. A terrorist-inclined user may not actively precipitate a warrant, yet the knowledge of available content—and the option to act or not to act constitute a local threat. The spirit of the platform's responsiveness to local needs which separates personal liberty from security must properly activate; yet such foundation is fleeting, often oscillating. It calls into question the fundamental premise of both United States Communications Decency Act: Section 230 and the safe harbour provision in the Indian Information Technology Act: Section 79 reducing risk for such gatekeeping or filtering responsibility. Local regulation simply could not shoulder the responsibility; either platforms name their terms and conditions in ways that reflect local conditions, or the law provide for localised and more specific liability.

Possible alternatives to the excesses at the outer fringes of the debates related to the Web 2.0 environment could go as follows. The efforts of platforms to leverage local governance through elections and openness to scrutiny through a (government, civil-society, and industry-linked) oversight board offer: (a) viable and effective, albeit potential, structures for the future; and, (b) an obvious attempt by centres such as Facebook and Twitter—to take the power closer to the people and check the growing shrillness in the current discussion around the Internet.

8. Reform Proposals and Future Directions

Social media regulation remains a pressing challenge in India. The expanding user base has raised concerns about harmful communication, misinformation, disinformation, hate speech, and sexually explicit content; equally, users' individual boundaries with respect to freedom of speech, privacy, and security are increasingly

contested, particularly for young people. Despite high judiciary affirmations of freedom of expression as a fundamental right, the need for online safety has propelled regulation and restrictions. The legal framework provides security to intermediaries but compliance remains a significant challenge. The directive principles of state policy note the need to secure for citizens “an adequate means of livelihood, equal pay for equal work, participation of workers in the management of industries.” The Government of India has adopted the policy of a Digital India that The right to ask questions, explore alternative viewpoints and dissent must never be stifled.

8.1. Legal Reforms and Clarifications Needed

Legal reforms and clarifications are needed to narrow the scope of Section 79 so that it protects only genuine intermediaries by excluding those with actual knowledge of unlawful content but that do not take it down, as well as those that fail to act expeditiously to comply with government orders. The expansive interpretation of Section 79 by the Indian courts has resulted in the grant of liberty to platforms even where these provisions are not satisfied. The conditions can be made suitably stringent as per the requirements of the Indian legal landscape. Section 69A may also benefit from an addition of a transparent procedural framework. Protocols that govern and regulate platform content moderation policies can further aid judicial enforcement while preserving the industry’s internal self-regulatory autonomy. A clear set of laws governing platform behaviour and responsibility will aid in establishing a transparent framework for the proper operations of social media players.

8.2. Institutional Mechanisms for Oversight

In addition to proposed legislative reforms, institutional mechanisms may play a vital role in intermediary liability, expressed through the accountability of certain stakeholders. The challenge of misinformation, disinformation, and related threats to national security, public order, and public health should not rest solely on social media intermediaries, for the flaws of their global governing structures can also affect user communities in India. Given the speed at which harmful information propagates and the intensity of possible consequences, there is a need for a calibrated approach enabling all concerned parties government, intermediaries, and civil society—to work together to address such challenges. While the risk of bias in action or inaction cannot be disregarded, a stronger institutional presence from civil society may curb the overt or covert reluctance of social media platforms and help advance the principles contained in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

It has also been suggested that the Supreme Court of India should exercise its jurisdiction to lay down detailed guidelines for the blocking of access to information. Such continued gatekeeping of free speech and expression by private players, however, elevates the responsibility of social media intermediaries to act in a transparent, reasonable, and non-arbitrary manner. A further area requires reliable data, from online platforms, government security agencies, and other sources. Transparency in algorithmic design and the operational processes employed for decision-making, resource allocation, and user redress may enable better public understanding of why a digital platform decides to allow or disallow a certain product, service, or piece of information—a development crucial to establishing a mutually acceptable environment of trust wherein users can exercise their choice without fear of being misled or harmed.

9. Conclusion

India stands at a critical juncture in shaping the future of social media and online content, weighing platform accountability against free speech and public safety

concerns. Balancing these competing considerations is essential if India aims to harness the transformative potential of technology to advance prosperity, health, education, and civil liberty. Social media plays an important role in informing the public, facilitating dialogue, and enabling citizens to reach political representatives and advocate for change (Bayer, 2019). Too much regulation would encumber these benefits, while too little would expose users, especially women, to predation, hate speech, misinformation, and other harms (Sylvain, 2018). Global content dominate these risks and must be balanced with India's constitutional obligations. The French Council of State acknowledged the critical role of social media and other platforms in providing society with relevant information on matters of public concern that enable citizens to exercise their political and social rights (Li, 2018).

A cooperative governance model accounts for the unique characteristics of social media platforms and the broader political, economic, and regulatory objectives they serve. Currently, inadequate platform transparency permits domination by vested interests who weaponise disinformation and restrict users' rights to participate in public discourse. The same model seeks to moderate diverse political expression while encouraging mutual respect, equity, and dialogue across society. Brazil's differences in regulatory emphasis—for example, in focus on content or user rights—illustrate how platform classification affects accountability and that careful prioritisation may still serve inclusive dialogue, information access, and reasonable content protection. Such adjustments provide necessary or desirable furtherance of Indian objectives while permitting perspective beyond free-speech guarantees. Additional developments, expansion, or consideration of informational access—both domestic and international may enhance support for overcoming technical and resource constraints.

Author's Declaration-

I/We accept full responsibility, jointly and individually, for this article's content, views, analysis, conclusions, and any related errors, plagiarism, copyright, ethical, defamatory, or legal issues, now or in the future. The publisher, editors, and reviewers shall bear no liability. I/We declare no financial, personal, academic, or professional conflict of interest.

References:

1. Bengel, H. (2019). Who's liable? The Intersection of Free Speech and Content Regulation on Social Media Platforms.
2. Bayer, J. (2019). Between Anarchy and Censorship: Public discourse and the duties of social media. CEPS Paper in Liberty and Security in Europe No. 2019-03, May 2019.
3. Sylvain, O. (2018). Intermediary Design Duties.
4. Li, T. (2018). Beyond Intermediary Liability: The Future of Information Platforms - Workshop Report.
5. Gorwa, R. & Garton Ash, T. (2019). Democratic Transparency in the Platform Society. [osf.io](https://www.osf.io)

Disclaimer/Publisher's Note: The views, content, and claims expressed in this article are solely the responsibility of the author(s). The publisher and editors accept no legal liability for any errors, copyright infringement, or loss or damage arising from its use.

Cite this Article

"Sharma, V. N." (2026), "Social Media Intermediary Liability in India: Balancing Freedom of Expression, Online Safety and Platform Accountability", International Journal of Arts, Humanities, Social Sciences and Commerce, 2(1), 1–6. <https://doi.org/10.65919/ijahssc.2026.v2i1007>

"Copyright © 2026 The Author(s). This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License, permitting sharing and adaptation with appropriate attribution for non-commercial purposes".