Page 696 - 705 **DOI:** *https://doi.org/10.63108/IJLMH.13177*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

From Shreya Singhal to X Corp: The Evolution of Intermediary Accountability in Online Defamation Cases

DR. RAMESH SIROHI[*] AND VIJAY KUMAR[**]

ABSTRACT

The rapid digitization of public discourse in India has fundamentally transformed the dynamics of individual reputation and freedom of speech. While social media platforms serve as vital conduits for expression, they have simultaneously become prolific conduits for defamatory content. Central to this digital legal dilemma is the doctrine of 'Safe Harbour' codified under Section 79 of the Information Technology Act, 2000, which shields intermediaries from liability for third-party user content. This research paper critically examines the evolutionary trajectory of intermediary accountability in online defamation cases in India over the past decade. The study traces the legal jurisprudence originating from the landmark judgment in Shreya Singhal v. Union of India *(2015), which established the requirement of prior court orders or administrative notifications to trigger intermediary liability, to the heightened compliance regime introduced by the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Furthermore, it analyzes contemporary judicial friction, particularly highlighting the constitutional challenges and litigation involving X Corp (formerly Twitter) regarding state-mandated takedown orders, user privacy, and global injunctions. Incorporating the legislative transition towards the Bharatiya Nyaya Sanhita (BNS), 2023 and Bharatiya Sakshya Adhiniyam (BSA), 2023, this paper evaluates the delicate constitutional balance between safeguarding personal reputation under Article 21 and preserving freedom of expression under Article 19(1)(a) in cyberspace. The paper concludes by proposing a refined framework for intermediary accountability that mitigates administrative overreach while ensuring effective and swift remedies for victims of digital defamation.*

Keywords: *Cyber Defamation, Intermediary Liability, Safe Harbour, Section 79 IT Act, Shreya Singhal, X Corp, IT Rules 2021, Article 19(1)(a), Article 21, BNS 2023*

[*] Author is an Associate Professor at Institute of Law, Kurukshetra University, Kurukshetra, Haryana, India.
[**] Author is a Research Scholar at Department of Law, Kurukshetra University, Kurukshetra, Haryana, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

I. INTRODUCTION

The advent of the Internet and the proliferation of social media platforms have radically democratized communication, transforming every digital citizen into a publisher.[1] In India, home to one of the largest and most dynamic online populations globally, cyberspace has become the primary arena for public discourse, political debate, and social interaction.[2] However, this unprecedented democratisation of speech carries significant socio-legal vulnerabilities. The borderless, instantaneous, and frequently anonymous nature of online communication has accelerated the spread of injurious statements, leading to widespread cases of digital defamation, character assassination, and cyberbullying.[3]

Unlike traditional print or broadcast media, where editorial oversight filters potential tortious or criminal content, online platforms operate primarily as conduits for third-party user-generated content. This unique architecture introduces a complex legal conundrum: to what extent should technology platforms, designated as 'intermediaries' under Indian law, be held legally accountable for defamatory statements published by their users?[4]

Despite legislative updates, the mechanism for regulating online defamation remains fragmented between tort laws, criminal statutes, and intermediary rules. This paper analyzes the legal transformation of the 'Safe Harbour' principle from the *Shreya Singhal* judgment to contemporary judicial precedents, evaluates the impact of the IT Rules, 2021 on intermediary compliance and platform autonomy in handling defamatory content, and proposes a balanced reform framework that protects individual reputation under Article 21 without compromising digital speech under Article 19(1)(a). It employs a doctrinal and analytical method, relying on primary and secondary legal sources.

---

[1] *See Shreya Singhal v. Union of India*, (2015) 5 SCC 1, ¶ 98 (India) (recognizing "an intelligible differentia between speech on the internet and other mediums of communication").

[2] Ministry of Electronics & Information Technology, *Digital India: Power to Empower* (Gov't of India); *see also* Simon Kemp, *Digital 2024: India*, DATAREPORTAL (Feb. 21, 2024), https://datareportal.com/reports/digital-2024-india (reporting 751.5 million internet users in India at the start of 2024).

[3] The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860, §§ 499–500 (India) (defamation), replaced by The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, § 356 (India) [hereinafter BNS]; *see also* The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 66E, 67 (India) [hereinafter IT Act].

[4] IT Act, *supra* note 3, § 79; The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021) (India) [hereinafter IT Rules, 2021]; *see also Google India Private Ltd. v. Visaka Industries*, (2020) 4 SCC 162 (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

II. The conceptual framework of intermediary liability and 'Safe Harbour'

To foster technological innovation and protect digital platforms from being burdened with insurmountable litigation, legal regimes worldwide have established the doctrine of 'Safe Harbour'.[5]

Under Indian law, this principle is codified in Section 79 of the Information Technology Act, 2000 (IT Act). Section 79 provides conditional immunity to intermediaries, stipulating that a platform shall not be liable for any third-party information, data, or communication link made available or hosted by it, provided that:

1. the function of the intermediary is limited to providing access to a communication system; or
2. the intermediary does not initiate the transmission, select the receiver, or select or modify the information; and
3. the intermediary observes 'due diligence' as prescribed by the Central Government.[6]

However, this protection is not absolute. Under Section 79(3)(b), the safe harbour exemption is lost if the intermediary fails to expeditiously remove or disable access to defamatory or unlawful material upon receiving "actual knowledge" or on being notified by the appropriate Government or its agency.[7]

III. Legislative transition: the BNS and BSA regime

With the implementation of the Bharatiya Nyaya Sanhita (BNS), 2023, which replaced the Indian Penal Code, Section 356 now governs criminal defamation; it reaches any imputation that a person "makes or publishes in any manner", wording wide enough to cover electronic records and digital media.[8] Simultaneously, Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023 standardizes the admissibility of electronic evidence, directly affecting how digital defamation claims and intermediary logs are adjudicated in Indian courts.[9]

---

[5] *See, e.g.*, 47 U.S.C. § 230(c)(1); Directive 2000/31/EC, of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, art. 14, 2000 O.J. (L 178) 1 (now replaced by Regulation (EU) 2022/2065, art. 6, 2022 O.J. (L 277) 1).
[6] IT Act, *supra* note 3, § 79(2)(a)–(c).
[7] *Id.* § 79(3)(b).
[8] BNS, *supra* note 3, § 356(1).
[9] The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023, § 63 (India) [hereinafter BSA] (replacing Section 65B of The Indian Evidence Act, 1872, No. 1, Acts of Parliament, 1872 (India), for certificate-based proof of electronic records).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

IV. The regulatory shift: IT Rules, 2021

In recent years, the exponential rise of fake news, viral defamation, and online harassment prompted a regulatory recalibration. The government introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[10] These rules imposed stringent procedural requirements on intermediaries, and further obligations on Significant Social Media Intermediaries (SSMIs), including:

- strict timelines for content removal: thirty-six hours after a court order or government notification, and twenty-four hours after an individual's complaint about intimate images or impersonation;
- mandatory appointment of resident grievance officers; and
- an obligation on SSMIs to endeavour to deploy automated tools to identify certain categories of content proactively.[11]

V. The constitutional balance: Article 19(1)(a) vs. Article 21

At its core, the evolution of intermediary liability in digital defamation reflects a fundamental constitutional tug-of-war between the freedom of speech and expression under Article 19(1)(a) and the right to reputation and privacy under Article 21.

While the Right to Reputation is an intrinsic facet of the Right to Life and Personal Liberty under Article 21, as the Supreme Court held in *Subramanian Swamy v. Union of India*,[12] unreasonable restrictions or automated takedown mandates risk imposing a severe 'chilling effect' on free expression guaranteed under Article 19(1)(a).

VI. Jurisprudential analysis of key case laws

The jurisprudence surrounding online defamation and intermediary liability in India has evolved through a series of foundational judgments. Indian courts have continuously attempted to harmonise the constitutional tension between Free Speech under Article 19(1)(a) and the Right to Reputation under Article 21.

---

[10] IT Rules, 2021, *supra* note 4, rr. 3–4.

[11] *Id.* rr. 3(1)(d), 3(2)(b), 4(1)(c), 4(4) (as notified in 2021); *see also* Notification S.O. 942(E) (Feb. 25, 2021) (India) (fixing fifty lakh registered users in India as the threshold for a significant social media intermediary). The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India), in force from Feb. 20, 2026, shortened the thirty-six-hour and twenty-four-hour periods to three hours and two hours respectively, and replaced the duty to "endeavour to deploy" technology-based measures, including automated tools, with a duty to "deploy appropriate technical measures, including automated tools or other suitable mechanisms".

[12] *Subramanian Swamy v. Union of India*, (2016) 7 SCC 221, ¶ 139 (India) (holding that reputation is "an inextricable aspect of right to life under Article 21").

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

A. *Shreya Singhal v. Union of India*

The landmark case *Shreya Singhal v. Union of India* originated from the controversial arrest of two individuals under Section 66A of the IT Act, 2000, for posting comments on social media, and ultimately led to the fundamental restructuring of Section 79's Safe Harbour provisions and the accompanying Intermediary Guidelines Rules. Regarding intermediary accountability, the Supreme Court read down Section 79(3)(b) to protect platforms from being forced by private notices to judge the lawfulness of content, thereby preventing self-censorship and a chilling effect on free speech.[13] Furthermore, the Court strictly interpreted 'actual knowledge' under Section 79(3)(b) to mean knowledge derived from a court order or a notification by the appropriate Government or its agency, confined to the subjects listed in Article 19(2), rendering private takedown requests ineffective for stripping Safe Harbour protection. Conversely, a court order or government notification creates actual knowledge, and failure to act on it leads to the loss of safe harbour protection.[14]

Ultimately, *Shreya Singhal* established a high threshold for both state and private interference in digital speech, effectively insulating intermediaries from coercive private notices and preserving digital platforms as neutral public forums.

B. The Information Technology (Intermediaries Guidelines) Rules, 2011

Prior to this ruling, Rule 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011 required an intermediary to act within thirty-six hours once an affected person brought content to its actual knowledge in writing or by e-mail. Intermediaries were thus subjected to private notices from aggrieved individuals claiming that content was unlawful or defamatory, which pressed them to self-censor or take content down to avoid liability; the petitioners argued that the rule called on intermediaries to exercise their own judgment on such notices and then disable the information.[15] The Supreme Court upheld the 2011 Rules but read down Rule 3(4) in the same manner as Section 79(3)(b): the knowledge it speaks of must come only through a court order.[16]

C. *Subramanian Swamy v. Union of India*

In *Subramanian Swamy*, the petitioners challenged the constitutional validity of criminal defamation under Sections 499 and 500 of the Indian Penal Code (IPC), now governed by

[13] *Shreya Singhal*, *supra* note 1, ¶ 117.
[14] *Id.* ¶¶ 117, 119.
[15] *Id.* ¶¶ 113–114 (setting out Rule 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011 and the petitioners' challenge to it).
[16] *Id.* ¶¶ 118–119. The 2011 Rules were later superseded by the IT Rules, 2021. IT Rules, 2021, *supra* note 4, pmbl.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Section 356 of the Bharatiya Nyaya Sanhita, 2023, arguing that criminalizing speech violates Article 19(1)(a). The Supreme Court addressed this by recognizing that the Right to Reputation is an intrinsic element of the Right to Life and Personal Liberty under Article 21.[17] Rejecting the argument that free speech overrides reputation, the Court treated the case as one of balancing two fundamental rights, holding that one fundamental right cannot be allowed to destroy another,[18] and upheld criminal defamation as a 'reasonable restriction' under Article 19(2).[19]

By elevating reputation to a fundamental right under Article 21, *Subramanian Swamy* provided the constitutional foundation for victims of digital defamation to demand swift civil and criminal remedies against both individual tortfeasors and uncooperative platforms.

D. *Swami Ramdev v. Facebook, Inc.*

In *Swami Ramdev v. Facebook, Inc.*, the plaintiffs filed a suit before the Delhi High Court seeking an injunction against major social media platforms, such as Facebook, Twitter (now X), YouTube, and Google, to block and remove defamatory video content based on a book, bringing forth the central legal question of whether Indian courts possess the authority to issue a global injunction ordering worldwide content removal or whether orders must be restricted to users in India through geo-blocking. Resolving this issue, Justice Prathiba M. Singh held that content uploaded from IP addresses within India must be taken down on a global basis, while content uploaded from outside India may be geo-blocked so that users in India cannot access it.[20] The Court reasoned that geo-blocking alone is inadequate because users in India could still reach the content through Virtual Private Networks (VPNs) and other means, including the platforms' international websites,[21] and observed that, since the platforms themselves remove content globally when it breaches their own policies, there is no reason why court orders under Section 79 should not also operate globally.[22]

Ultimately, this decision, though expressed at the interim stage,[23] introduced global injunctions into Indian cyber jurisprudence, significantly expanding compliance burdens for multi-jurisdictional technology platforms involved in online defamation litigation.

[17] *Subramanian Swamy*, *supra* note 12, ¶ 139.
[18] *Id.* ¶¶ 131, 140.
[19] *Id.* ¶¶ 184, 199 (upholding Sections 499 and 500 of the IPC and Section 199 of the Code of Criminal Procedure).
[20] *Swami Ramdev v. Facebook, Inc.*, (2019) 263 DLT 689, ¶¶ 94, 96 (Del. HC) (India).
[21] *Id.* ¶ 92.
[22] *Id.* ¶¶ 87, 94.
[23] *Id.* ¶ 97 (disposing of I.A. 855/2019 and stating that the views expressed are *prima facie*).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

E. *X Corp v. Union of India*

In this dispute, X Corp (formerly Twitter) challenged multiple blocking orders issued by the Ministry of Electronics and Information Technology (MeitY) under Section 69A of the IT Act, several of which directed the platform to block entire user accounts rather than specific posts. X Corp argued that account-level blocking censors future speech that is yet to be posted and may be innocuous, invoked Article 19(1)(a), and objected that the account holders had been given no notice.[24] Section 69A permits blocking only in the interest of the sovereignty and integrity of India, the defence of India, the security of the State, friendly relations with foreign States or public order, or to prevent incitement to a cognizable offence relating to these grounds.[25] Defamation is not among them: a defamatory post is taken down not by a Section 69A blocking order but under Section 79(3)(b), on a court order or a government notification relatable to Article 19(2).[26]

In response, the State contended that it had resorted to blocking whole accounts only for a few users with a record of repetitive objectionable posting. On 30 June 2023, the Single Bench of the Karnataka High Court dismissed X Corp's petition. It accepted the State's explanation, noting that the tweets in question had "a great propensity to incite anti-national feelings"; held that X Corp, not being a citizen, could not claim the protection of Article 19(1)(a); held that the power under Section 69A extends to user accounts in their entirety and that notice under the Blocking Rules may be given to the intermediary rather than the user; and imposed exemplary costs of ₹50 lakh.[27] X Corp appealed, and in August 2023 a Division Bench stayed the order of costs on X Corp's depositing ₹25 lakh;[28] the intra-court appeal tests the limits of proportionality, procedural fairness, and account-level takedowns.

Ultimately, *X Corp* represents the modern frontier of intermediary liability, shifting the debate from whether platforms must remove specific defamatory posts to whether the State can compel platforms to silence digital entities and entire user channels.

---

[24] *X Corp. v. Union of India*, W.P. No. 13710 of 2022, slip op. at 17–18, 44–45, 79–80 (Kar. HC June 30, 2023) (India).
[25] IT Act, *supra* note 3, § 69A(1).
[26] *Shreya Singhal*, *supra* note 1, ¶¶ 117, 119; IT Rules, 2021, *supra* note 4, r. 3(1)(d) (listing defamation among the subjects on which an intermediary must act on actual knowledge).
[27] *X Corp.*, *supra* note 24, slip op. at 18, 61–63, 81–82, 109.
[28] Mustafa Plumber, *Account Blocking: Karnataka High Court Stays Payment of 'Exemplary' Cost by X Corp Subject to Depositing ₹25 Lakh*, LIVELAW (Aug. 10, 2023), https://www.livelaw.in/high-court/karnataka-high-court/karnataka-high-court-twitter-account-blocking-x-corp-appeal-meity-deposit-25-lakh-234879 (reporting the order in *X Corp. v. Union of India*, W.A. No. 895 of 2023 (Kar. HC 2023) (India)).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

VII. CRITICAL CHALLENGES IN MODERN CYBER DEFAMATION JURISPRUDENCE

Despite the progressive evolution of judicial precedents and legislative frameworks, the enforcement of online defamation laws in India faces several complex systemic hurdles.

A. The anonymity and pseudonymity conundrum

The proliferation of pseudonymous accounts, decentralized messaging apps, and burner profiles makes it extremely difficult to identify primary tortfeasors.[29] While platforms claim privacy protections under data security frameworks, victims are often left without a tangible defendant to sue, shifting undue pressure onto intermediaries.

B. Automated takedowns and the 'chilling effect'

Under intense pressure from the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which since February 2026 require removal within three hours of a court order or government notification and oblige SSMIs to deploy technical measures, including automated tools or other suitable mechanisms,[30] platforms are pushed towards automated algorithms and artificial intelligence filters. These algorithms can over-censor legitimate critical commentary, suppressing lawful public debate under Article 19(1)(a), a risk the Rules themselves recognize by requiring such measures to be proportionate to free speech and privacy and subject to human oversight.[31]

C. Jurisdictional conflicts and enforcement deficits

As highlighted in cross-border litigation, foreign-hosted platforms have at times delayed compliance with domestic orders; in *X Corp*, some blocking orders made in 2021 remained uncomplied with for more than a year.[32] Conversely, platforms resisting sweeping global injunctions point to conflicts of law, comity of courts, and the disparity between the defamation laws of different jurisdictions, raising questions of extraterritorial jurisdiction.[33]

D. Transition and interpretation challenges under new criminal laws

The introduction of the Bharatiya Nyaya Sanhita (BNS), 2023 (Section 356) and the Bharatiya Sakshya Adhiniyam (BSA), 2023 modernizes the law, and Section 63 of the BSA now governs the admissibility of electronic records.[34] However, law enforcement agencies and lower

[29] APARNA VISWANATHAN, CYBER LAW: INDIAN AND INTERNATIONAL PERSPECTIVES 142–145 (2012).
[30] IT Rules, 2021, *supra* note 4, rr. 3(1)(d), 4(4), *as amended by* The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E) (Feb. 10, 2026) (India).
[31] *Id.* r. 4(4) provisos (requiring that such measures be proportionate having regard to free speech and expression and the privacy of users, and subject to human oversight and periodic review).
[32] *X Corp.*, *supra* note 24, slip op. at 103–104, 106.
[33] *Swami Ramdev*, *supra* note 20, ¶¶ 90, 93.
[34] BSA, *supra* note 9, § 63.

judiciary units require standardized technical training to accurately authenticate volatile digital evidence such as metadata, IP logs, and server histories.

VIII. Policy recommendations and way forward

To achieve an equitable balance between individual reputation and digital free expression, the following legislative and administrative reforms are recommended.

A. Refinement of due diligence standards

The government and regulatory bodies should introduce graded due diligence standards that differentiate between small community forums and "Significant Social Media Intermediaries" (SSMIs), ensuring that automated filters are subject to human review.

B. Establishment of specialized cyber-defamation fast-track cells

Given the rapid virality of digital defamation, civil and criminal courts should establish dedicated fast-track adjudicatory mechanisms equipped with technical experts to handle urgent takedown injunctions within 48 to 72 hours.

C. Balancing traceability and privacy

While traceability of originators is crucial for curbing targeted smear campaigns, any mandate for message tracking must incorporate rigorous judicial oversight to prevent arbitrary state surveillance and protect user privacy under Article 21.

D. Enhanced judicial training on electronic evidence

Judicial academies must institutionalize specialised training modules regarding the evidentiary standards under Section 63 of the BSA, 2023, ensuring robust judicial evaluation of digital logs in online defamation trials.

IX. Conclusion

The evolutionary trajectory of intermediary accountability in India reflects a complex struggle to harmonize digital expression with individual rights. The journey from the protective shield of *Shreya Singhal*, which safeguarded free speech by narrowing "actual knowledge" to judicial or governmental orders, to the stringent regime of the IT Rules, 2021, demonstrates a distinct shift toward heightened regulatory scrutiny. While rapid digitization and viral character assassination necessitate robust mechanisms to protect personal reputation under Article 21, disproportionate takedown mandates, automated algorithmic censorship, and account-level blocking risk overreaching constitutional limits and chilling free speech guaranteed under Article 19(1)(a).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The legal transitions introduced by the Bharatiya Nyaya Sanhita (BNS), 2023, and Bharatiya Sakshya Adhiniyam (BSA), 2023, along with ongoing litigation like the *X Corp* cases, underline the urgent need for a recalibrated legal framework. To establish a resilient digital environment, India's cyber jurisprudence must move away from rigid binary choices between absolute immunity and aggressive censorship. By adopting fast-track adjudicatory mechanisms, graded due diligence standards, human oversight over automated filters, and procedural fairness in blocking orders, the legal framework can effectively protect individuals from digital defamation without compromising the core democratic principles of online discourse.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]