



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL**
**ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

REGULATION OF ONLINE OFFENCES IN INDIA: A CRITICAL ANALYSIS OF THE INFORMATION TECHNOLOGY ACT AND CRIMINAL LAW FRAMEWORK

AUTHORED BY - SAHIL SEHRAWAT

ABSTRACT

*The regulation of online offences in India rests on a composite and increasingly complex architecture combining substantive criminalisation under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, content-blocking powers under Section 69A of the IT Act, intermediary due-diligence obligations conditioning safe-harbour protection under Section 79, and an evidentiary framework governed by the Bharatiya Sakshya Adhiniyam, 2023. This paper undertakes a critical, doctrinal analysis of this composite regulatory architecture, examining how substantive offence provisions, content-blocking mechanisms, and intermediary regulation interact, and at times conflict, in governing online conduct in India. It traces the regulatory framework's evolution from the IT Act's original 2000 enactment through the 2008 amendment's expansion of both criminal offences and intermediary safe harbour, the Supreme Court's foundational 2015 ruling in *Shreya Singhal v. Union of India* striking down Section 66A while upholding Section 69A's blocking power subject to procedural safeguards, the progressive tightening of intermediary due-diligence obligations through the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 and its 2023 and 2025 amendments, and the still-unresolved 2025 Karnataka High Court litigation in *X Corp v. Union of India* concerning whether the government's Sahyog Portal, operating through Section 79(3)(b) read with Rule 3(1)(d), has created a parallel content-blocking channel that circumvents Section 69A's constitutionally mandated procedural safeguards. The paper critically examines the resulting regulatory fragmentation, including the coexistence of at least two distinct content-blocking pathways with materially different procedural protections, the tension between intermediary safe harbour and proactive content-moderation obligations, and the challenge of regulating artificial-intelligence-generated and synthetic content within a framework designed for a materially different technological era. Employing doctrinal legal research methodology, the paper argues that India's online-offence*

regulatory framework, while substantively comprehensive, suffers from a structural coherence deficit: overlapping and inconsistently safeguarded regulatory pathways create both enforcement unpredictability and constitutional vulnerability. The paper concludes with recommendations for procedural harmonisation across blocking pathways, clearer demarcation of intermediary due-diligence obligations, and legislative attention to emerging regulatory gaps in synthetic-media governance.

Keywords: *Information Technology Act, 2000; online offences; intermediary liability; Section 69A; content blocking; safe harbour; India.*

1. INTRODUCTION

The regulation of online conduct in India operates through a composite and, this paper argues, increasingly fragmented architecture rather than a single, integrated regulatory instrument. Four distinct but interlocking regulatory pillars govern online offences: substantive criminalisation, chiefly under the Information Technology Act, 2000 (“IT Act”) and the Bharatiya Nyaya Sanhita, 2023 (“BNS”); content-blocking powers vested in the Central Government under Section 69A of the IT Act; intermediary due-diligence obligations conditioning the availability of safe-harbour protection under Section 79; and an evidentiary and investigative framework now governed by the Bharatiya Nagarik Suraksha Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023.¹ This paper undertakes a critical, doctrinal examination of how these four pillars interact, and increasingly conflict, in the practical regulation of online offences in India, with particular attention to a live and unresolved doctrinal controversy: whether the government's 2025 deployment of the “Sahyog Portal” for content takedown, operating through Section 79(3)(b) of the IT Act read with Rule 3(1)(d) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, has created a parallel, materially less-safeguarded blocking pathway that circumvents the procedural protections the Supreme Court found constitutionally necessary for Section 69A blocking orders in *Shreya Singhal v. Union of India*.²

This inquiry carries substantial contemporary significance. Court filings in the X Corp litigation indicate that the platform received 29,118 government takedown requests in the first half of 2025 alone, complying with over ninety-one percent, with more than seventy percent of

¹Information Technology Act, 2000, ss. 66-67C, 69A, 79; Bharatiya Nyaya Sanhita, 2023.

²*Shreya Singhal v. Union of India*, (2015) 5 SCC 1; *X Corp v. Union of India*, W.P. No. 7405/2025, Karnataka High Court, order dated 24 September 2025.

orders reportedly issued through the Sahyog portal mechanism rather than the formally safeguarded Section 69A pathway.³ The scale of this activity, and the constitutional stakes attending the procedural adequacy of the mechanism through which it occurs, makes the regulation of online offences in India a matter of both doctrinal and practical urgency, extending well beyond any single platform dispute to the broader architecture governing how criminal and quasi-criminal online conduct is identified, addressed and adjudicated across India's digital ecosystem.

1.1 Statement of the Problem

India's regulatory framework for online offences has developed incrementally across substantive criminal law, content-blocking powers and intermediary regulation, each governed by distinct statutory provisions, procedural safeguards and judicial oversight mechanisms. This incremental development has produced a regulatory architecture whose constituent pillars do not operate with consistent procedural rigour, creating both enforcement unpredictability for regulated intermediaries and constitutional vulnerability for affected speakers and users, as the ongoing X Corp litigation starkly illustrates.

1.2 Objectives of the Study

- To map the composite regulatory architecture governing online offences in India across substantive criminalisation, content blocking, intermediary regulation and evidentiary frameworks.
- To critically analyse the doctrinal foundations and procedural safeguards attaching to each regulatory pillar, with particular reference to Section 69A and Section 79 of the IT Act.
- To examine the 2025-2026 X Corp v. Union of India litigation as a case study in regulatory fragmentation and its constitutional implications.
- To assess the adequacy of the current framework in addressing emerging online offence categories, including AI-generated and synthetic content.
- To recommend reforms promoting procedural coherence and constitutional robustness across India's online-offence regulatory architecture.

³“The Karnataka High Court on Content Blocking: What the X Corp Rulings Mean for Platform Accountability in India,” AMLegals (2025-26); CJP, “The Ghost of Shreya Singhal: Re-litigating Digital Free Speech” (2025).

1.3 Research Questions

- How do the substantive, content-blocking, intermediary-regulation and evidentiary pillars of India's online-offence framework interact, and where do they generate doctrinal inconsistency or conflict?
- Does the Sahyog Portal's operation through Section 79(3)(b) and Rule 3(1)(d) constitute a lawful, distinct efficiency mechanism, or does it functionally bypass the procedural safeguards the Supreme Court held constitutionally necessary for content blocking under Section 69A in *Shreya Singhal*?
- How adequately does the current regulatory framework address emerging online offence categories, including deepfake and AI-generated content?
- What legislative and institutional reforms would promote greater procedural coherence and constitutional robustness in India's online-offence regulatory architecture?

1.4 Research Methodology

This study adopts a doctrinal legal research methodology, involving critical analysis of the IT Act, the IT Rules and their amendments, the BNS, and judicial precedent, including the pending and recently decided *X Corp v. Union of India* litigation, supplemented by secondary literature and commentary. The analysis integrates statutory interpretation with constitutional analysis under Articles 19 and 21.

1.5 Scope and Limitations

The paper is confined to the regulation of online offences within India's domestic legal framework, with particular focus on the interaction between substantive criminal law, content blocking and intermediary regulation. It does not undertake detailed comparative analysis of foreign online-speech regulatory regimes, nor does it address the substantive content of the Digital Personal Data Protection Act, 2023 beyond its bearing on this analysis. The *X Corp* litigation remained subject to further appellate proceedings as of August 2026, and the analysis reflects the legal position as understood at that date.

2. LITERATURE REVIEW

2.1 The Foundational *Shreya Singhal* Framework

The doctrinal starting point for any analysis of online-offence regulation in India remains the Supreme Court's 2015 decision in *Shreya Singhal v. Union of India*, which considered the

constitutionality of three IT Act provisions: Section 66A (struck down for vagueness and overbreadth), Section 69A (upheld), and Section 79(3)(b) (read down).⁴ Critically, the Court characterised Section 79 as “an exemption provision” — a conditional safe-harbour mechanism protecting intermediaries from liability, rather than an independent source of government power to compel content removal — and held that intermediaries are required to remove or disable access to content only upon receiving actual knowledge in the form of a court order or a notification by an appropriate government agency acting under a law empowering such action, of which Section 69A (with its accompanying 2009 Blocking Rules) was the paradigmatic example.⁵ The Court upheld Section 69A specifically because it found it “a narrowly drawn provision with several safeguards” — including a written, reasoned order, a designated officer's review, and a committee examination process under the 2009 Blocking Rules — and its validation was explicitly contingent on strict governmental compliance with those procedural safeguards.⁶

2.2 The Evolution of Intermediary Regulation

Scholarship on intermediary liability traces the safe-harbour concept's origins to the 2008 amendment of the IT Act, prompted by a 2008 prosecution of a website officer under the Indian Penal Code for third-party obscene content, following which Section 79 was amended to exempt intermediaries functioning as mere conduits from liability under any law (not merely the IT Act itself), and the statutory definition of “intermediary” was broadened to include payment sites, search engines and internet service providers.⁷ The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 introduced substantially more detailed due-diligence conditions for retaining safe-harbour protection, including mandatory grievance-redressal mechanisms, a resident nodal and grievance officer requirement, and periodic compliance reporting.⁸ Comparative scholarship in Defeating Disinformation observes that these obligations are enforced “in a patchwork and inconsistent manner through courts,” while the government nonetheless retains powerful residual controls over platform behaviour through Section 69A's blocking power and the ability to impose

⁴Shreya Singhal v. Union of India, *supra* note 2.

⁵“Facilitating Digital Censorship – I: A Critique of the Karnataka High Court's Decision in X v Union of India,” Indian Constitutional Law and Philosophy Blog (2025), quoting Shreya Singhal, *supra* note 2.

⁶“Karnataka HC's Order in X Case Exemplifies Sheer Judicial Indiscipline,” The Leaflet (2025).

⁷“Safe Harbour Principle and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021),” Mondaq (2021).

⁸“Safe Harbour for Social Media,” Shankar IAS Current Affairs (2025).

personal liability on India-based platform employees.⁹ The 2023 amendment introduced a mechanism enabling loss of safe harbour for content flagged as “fake news” by the Press Information Bureau's Fact Check Unit, a mechanism itself subject to significant constitutional controversy regarding the delegation of content-veracity determination to an executive body without independent adjudicatory oversight.¹⁰

2.3 The 2025 Rule 3(1)(d) Amendment and AI-Generated Content

A 2025 amendment to Rule 3(1)(d) of the IT Rules, described in practitioner commentary as clarifying the scope of “actual knowledge” for safe-harbour purposes, is presented by the Government as strengthening intermediaries' safe-harbour defence by enabling more confident action upon receipt of reasoned, properly issued government intimations.¹¹ Parallel 2025-2026 regulatory developments extend intermediary due-diligence obligations to synthetically generated content: intermediaries enabling deepfake content creation must now inform users of potential criminal liability under the BNS, the Protection of Children from Sexual Offences Act, 2012, and the Representation of the People Act, 1951, and significant social media intermediaries are required to obtain user declarations on whether content is synthetically generated, implement technical verification measures, and prominently label verified synthetic content.¹² Commentary observes a structural tension in this expansion: the obligation of proactive monitoring for synthetic content risks transforming intermediaries from neutral conduits into “quasi-editorial gatekeepers,” a shift in character that sits uneasily with the safe-harbour framework's foundational premise of intermediary neutrality.¹³

2.4 X Corp v. Union of India: The Sahyog Portal Controversy

The most doctrinally significant recent development in this field is the ongoing litigation in X Corp v. Union of India before the Karnataka High Court. X Corp's petition, filed 5 March 2025, sought a declaration that Section 79(3)(b) does not confer an independent power to issue content-blocking orders, and that any such blocking action can be taken only through the constitutionally safeguarded Section 69A mechanism.¹⁴ The dispute arose from a 31 October

⁹“Safe Harbor and Content Moderation Regulation in India,” in *Defeating Disinformation* (Cambridge University Press, 2025).

¹⁰Shankar IAS, *supra* note 4.

¹¹“IT Rules 2025: New Intermediary Liability & Rule 3(1)(d),” Neeti Niyaman (2025), discussing *Sadhguru Jagadish Vasudev & Anr. v. Igor Isakov & Ors.*, 2024 SCC OnLine Del 3267.

¹²“India IT Rules 2021: Compliance Burdens, Speech and Privacy,” *Law.asia* (2026).

¹³*Id.*

¹⁴“X Relies on ‘Shreya Singhal’ in Arbitrary Content-Blocking Case in Karnataka HC,” *Supreme Court Observer* (2025).

2023 Office Memorandum issued by the Ministry of Electronics and Information Technology, which provided a “Template Blocking Order” for use by government authorities under Section 79(3)(b), and the subsequent operationalisation of the Sahyog Portal to route such notices at scale, which X Corp argued circumvented the Section 69A procedure and its accompanying safeguards.¹⁵ On 24 September 2025, the Karnataka High Court, in a judgment authored by Justice M. Nagaprasanna, upheld the government's authority to issue takedown orders under Section 79(3)(b) read with Rule 3(1)(d), holding that the Sahyog Portal merely improves administrative efficiency, ensuring notices reach appropriate officers with traceability, while the substantive power to block content remains exclusively vested in Section 69A and the 2009 Blocking Rules; the Court further held that Article 19(1)(a) protections extend only to citizens, such that X Corp, as a foreign corporate entity, could not itself invoke the fundamental right, though it acknowledged intervening Indian users' speech interests.¹⁶

2.5 Critical Commentary on the Karnataka High Court Ruling

The ruling has attracted substantial critical commentary. The Leaflet's analysis characterises the decision as reflecting “a conspicuous judicial attempt to dilute the settled precedent in *Shreya Singhal*,” privileging executive restriction over the enhancement of free expression that animated the 2015 ruling, and notes that the Court's characterisation of the 2011-era Blocking Rules addressed in *Shreya Singhal* as “now supplanted” by the 2021 Rules, requiring fresh interpretation, sidesteps rather than confronts the earlier decision's core structural holding that Section 79 is an exemption, not an empowering, provision.¹⁷ A guest analysis on the Indian Constitutional Law and Philosophy blog similarly argues that the *Shreya Singhal* ratio directly supports the petitioner's position: because Section 79 is an exemption provision “closely related to provisions which provide for offences including Section 69A,” there exist, under a faithful reading of *Shreya Singhal*, only two valid mechanisms for content takedown — a court order, or a government order issued specifically under Section 69A — rendering the Sahyog Portal's operation through Section 79(3)(b) alone constitutionally suspect.¹⁸ Supreme Court Observer's contemporaneous reporting on the case's earlier hearings notes that X Corp cited specific instances of takedown notices targeting satirical or politically critical content, news coverage of a public tragedy, and content related to an ongoing criminal matter, categories the petitioner

¹⁵Id.

¹⁶“An Exhaustive Takedown of Karnataka HC's Decision Upholding Sahyog Portal in *X Corp v. Union of India*,” The Leaflet (2025).

¹⁷The Leaflet, *supra* note 8; The Leaflet, *supra* note 6.

¹⁸“Facilitating Digital Censorship – I,” *supra* note 5.

argued may not meet the heightened substantive thresholds Section 69A itself imposes.¹⁹ A later report notes that the Section 69A blocking power is now also being deployed against unregulated digital lending applications, with the Ministry of State for Corporate Affairs informing the Lok Sabha in December 2025 that eighty-seven illegal loan applications had been blocked under Section 69A following the 2009 Blocking Rules procedure, illustrating the mechanism's expanding application beyond speech-related content to a broader category of online financial-offence regulation.²⁰

2.6 Research Gap

Existing literature substantially engages with either the historical Shreya Singhal framework, the evolving intermediary-regulation rules, or the X Corp litigation in isolation, without a systematic, integrated doctrinal account situating all three within a single analysis of India's composite online-offence regulatory architecture, read together with the substantive criminal law framework under the IT Act and BNS. This paper addresses that gap, offering an integrated, current (2026) account of how these regulatory pillars interact and where they generate coherence deficits.

3. ANALYSIS AND DISCUSSION

3.1 Mapping the Regulatory Architecture

As illustrated in Figure 1, the regulation of online offences in India rests on four interlocking pillars. Substantive criminalisation proceeds principally through the IT Act's Sections 66 to 67C (computer-related offences, identity theft, cheating by personation, privacy violation, cyber terrorism, obscene and sexually explicit content) and the BNS's general offence provisions (cheating, forgery, criminal intimidation, stalking, defamation), applied to online conduct through their technology-neutral drafting.²¹ Content-blocking operates through Section 69A of the IT Act, empowering the Central Government to direct blocking of public access to information on specified grounds including sovereignty, security, public order and prevention of incitement to a cognisable offence, subject to the procedural safeguards of the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.²² Intermediary regulation operates through Section 79's conditional safe-

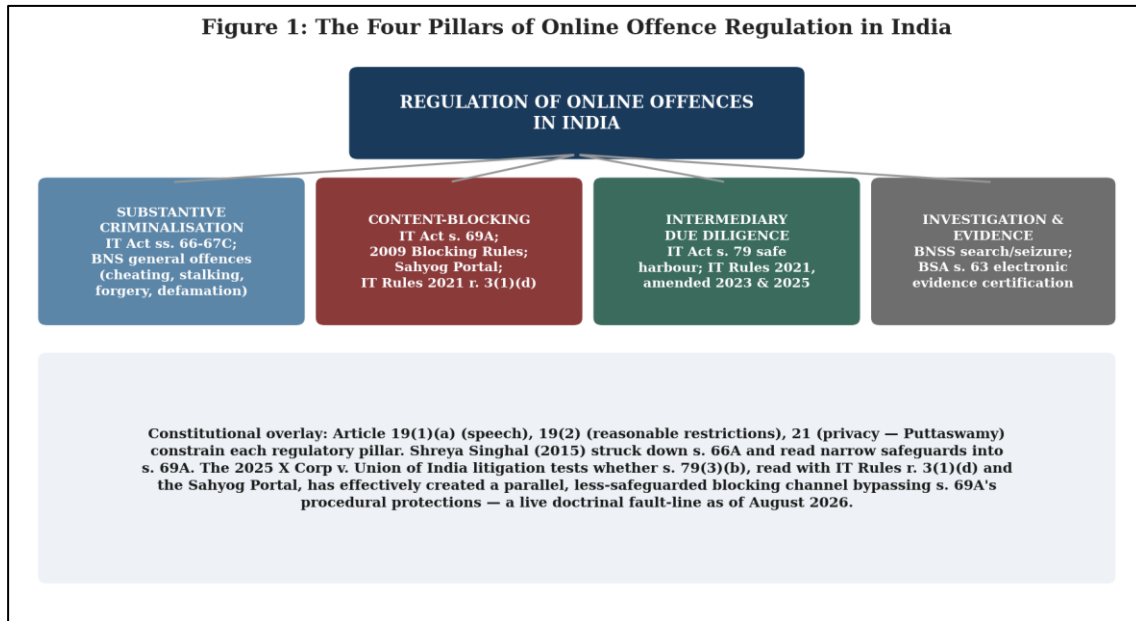
¹⁹CJP, *supra* note 3.

²⁰AMLegals, *supra* note 3.

²¹Information Technology Act, 2000, ss. 66-67C; Bharatiya Nyaya Sanhita, 2023.

²²Information Technology Act, 2000, s. 69A; Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

harbour protection, read with the IT Rules, 2021 and subsequent amendments, which impose due-diligence obligations as a precondition to retaining that protection.²³ The evidentiary and investigative pillar, governed by the BNSS and BSA, structures how conduct falling within the first three pillars is investigated and proved in criminal proceedings.



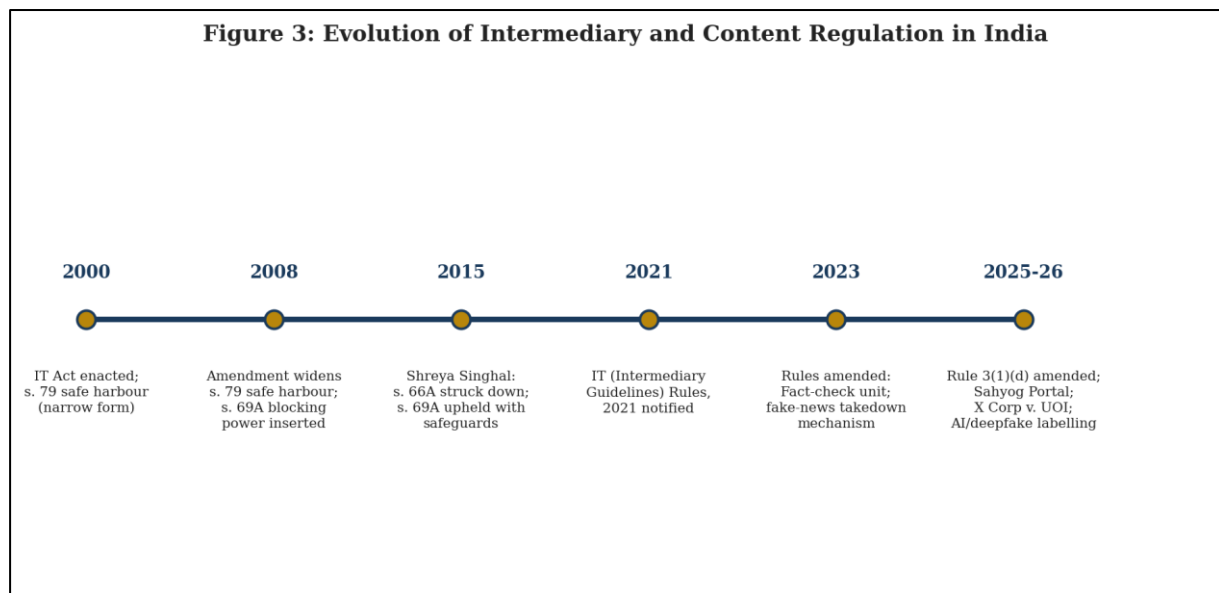
3.2 The Doctrinal Foundation: Shreya Singhal Revisited

Shreya Singhal's continuing doctrinal centrality lies in its structural characterisation of the relationship between Sections 69A and 79. The Court held that Section 79, as a conditional exemption provision, does not itself confer an independent power to compel content removal; rather, it defines the circumstances in which an intermediary's failure to act exposes it to a loss of immunity from liability that would otherwise attach under the general law.²⁴ Section 69A, by contrast, is an affirmatively empowering provision, vesting the Central Government with a positive power to direct blocking, but a power the Court found constitutionally sustainable only because of the procedural safeguards built into its accompanying 2009 Blocking Rules: a written, reasoned order requirement, review by a designated officer, and examination by a review committee before a blocking direction takes effect.²⁵ This structural distinction — an empowering provision with built-in safeguards, contrasted with an exemption provision without independent blocking authority — forms the doctrinal crux of the controversy examined in this Part.

²³Information Technology Act, 2000, s. 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

²⁴Shreya Singhal v. Union of India, *supra* note 2, at paras 117-122.

²⁵*Id.* at paras 99-109.



3.3 The Sahyog Portal Controversy: A Case Study in Regulatory Fragmentation

The Sahyog Portal, operationalised following the Ministry of Electronics and Information Technology's October 2023 Office Memorandum, routes government takedown notices to intermediaries under Section 79(3)(b) read with Rule 3(1)(d) of the IT Rules, 2021, using a standardised “Template Blocking Order” format.²⁶ As illustrated in Figure 2, this pathway differs materially from the Section 69A route in its procedural architecture: rather than requiring a written, reasoned order subject to designated-officer and committee review, Section 79(3)(b) conditions safe-harbour retention on the intermediary's response to a notice conveying “actual knowledge” of unlawful content, issued, on X Corp's account, by any authorised government officer without the independent multi-stage review Section 69A's 2009 Rules mandate.²⁷ The scale at which this pathway now operates — reportedly accounting for more than seventy percent of takedown notices received by X Corp in early 2025 — transforms what might otherwise be a narrow technical dispute over statutory interpretation into a matter of substantial practical consequence for the procedural rigour attending the overwhelming majority of India's online content regulation.²⁸

The Karnataka High Court's 24 September 2025 ruling in favour of the government's position rests on two principal holdings, each independently contestable on the critical commentary's account. First, the Court's characterisation of the Sahyog Portal as a mere administrative efficiency mechanism, rather than an independent exercise of blocking power, arguably

²⁶Supreme Court Observer, supra note 6.

²⁷Id.; The Leaflet, supra note 8.

²⁸AMLegals, supra note 3.

understates its practical effect: whatever its formal characterisation, a mechanism that results in the removal or disabling of access to content, without the reasoned-order, designated-officer and committee-review safeguards Shreya Singhal found constitutionally necessary, produces the same practical outcome as an unsafeguarded blocking order, regardless of its statutory label.²⁹ Second, the Court's holding that Article 19(1)(a) protections do not extend to a foreign corporate petitioner, while doctrinally defensible on the narrow question of X Corp's own standing, does not resolve the distinct and arguably more significant question of Indian users' speech interests, which the Court acknowledged only through intervening applicants rather than as a central element of its substantive reasoning.³⁰

3.4 Constitutional Analysis: Article 19 and the Proportionality of Regulatory Pathways

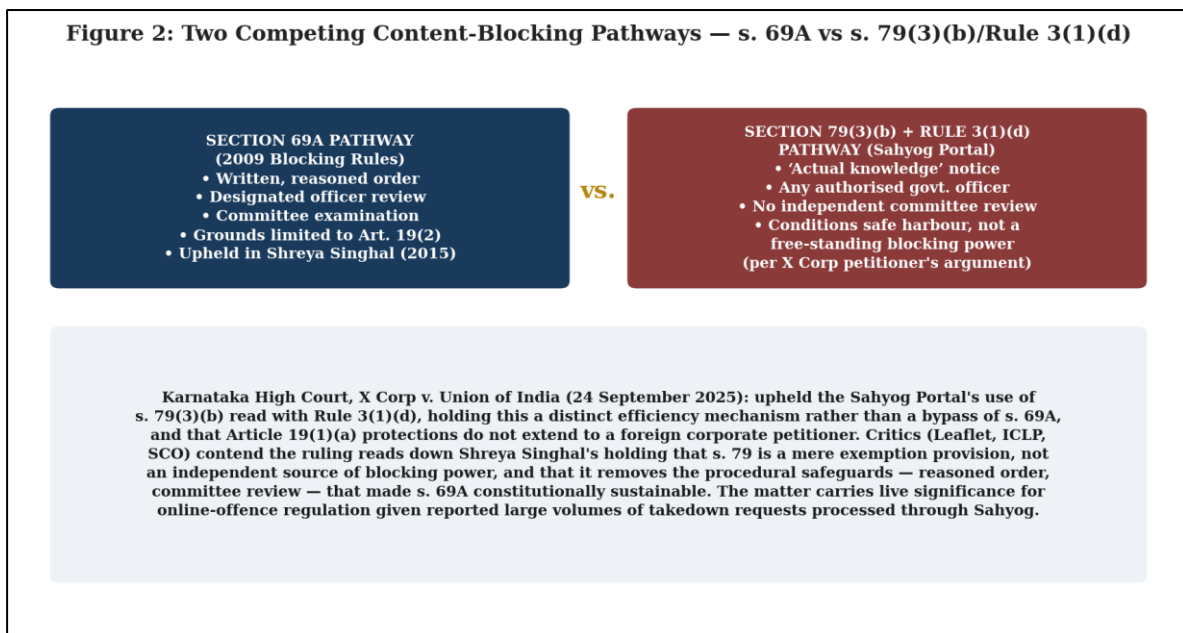
From a constitutional-doctrine perspective, the core difficulty with permitting two functionally equivalent but procedurally divergent content-blocking pathways to coexist is the risk of undermining the proportionality analysis Article 19(2) demands. Shreya Singhal's validation of Section 69A rested specifically on its narrow drafting and embedded procedural safeguards; a government able to achieve materially the same regulatory outcome through Section 79(3)(b), without equivalent safeguards, effectively permits the executive to select the less-constrained of two available pathways for content regulation, undermining the proportionality assessment that legitimised Section 69A in the first place.³¹ This concern is compounded by the practical reality, noted in X Corp's pleadings, that takedown notices routed through Sahyog have targeted categories of content — political satire, news coverage, content related to pending criminal matters — whose regulation implicates precisely the speech-protective concerns Shreya Singhal's safeguards were designed to police.³²

²⁹The Leaflet, supra note 8 (“an exhaustive takedown”).

³⁰CJP, supra note 3; Indian Constitutional Law and Philosophy Blog, supra note 5.

³¹Constitution of India, art. 19(1)(a), 19(2); Shreya Singhal, supra note 2.

³²CJP, supra note 3.



3.5 Intermediary Due Diligence and the Neutrality Paradox

Figure 3 traces the progressive tightening of intermediary due-diligence obligations from the IT Rules' 2021 notification through the 2023 fake-news mechanism and the 2025 Rule 3(1)(d) amendment and synthetic-content labelling requirements. This trajectory reveals a structural paradox at the heart of India's intermediary-regulation framework: safe harbour under Section 79 was conceived, and remains doctrinally justified, on the premise that intermediaries function as neutral conduits deserving immunity precisely because they do not exercise editorial control over user-generated content. Yet the cumulative effect of successive due-diligence obligations, including mandatory synthetic-content labelling, technical verification measures, and proactive monitoring expectations for AI-generated material, progressively pushes intermediaries towards precisely the editorial, content-evaluative posture the neutrality rationale was designed to avoid. Commentary describing this shift as transforming intermediaries into “quasi-editorial gatekeepers” captures a genuine doctrinal tension: the more due-diligence obligations require intermediaries to evaluate and act upon content substantively, the weaker the neutrality-based justification for the safe-harbour immunity those same obligations condition.

3.6 Emerging Regulatory Gaps: Synthetic and AI-Generated Content

Figure 4 illustrates the composition of online offences by primary regulatory mechanism, revealing that no single, clearly demarcated pathway currently governs the fastest-growing category of online-offence concern: artificial-intelligence-generated and synthetically manipulated content. The 2025-2026 regulatory response, requiring user declarations, technical

verification and content labelling, addresses disclosure and transparency but leaves the more fundamental question of substantive criminalisation largely unaddressed: no IT Act or BNS provision specifically defines the malicious creation of deepfake content as an offence, leaving prosecutors reliant on downstream harm-based provisions (identity theft, cheating by personation, defamation) triggered only once the synthetic content has been used to cause identifiable harm. This gap sits uneasily alongside the increasingly assertive content-blocking apparatus examined in Part 3.3, creating an asymmetric regulatory posture in which the state possesses substantial (and contested) power to block content after the fact, while lacking a clearly defined substantive offence addressing the underlying synthetic-media harm at its source.

3.7 The Overlap with Substantive Criminal Law: BNS and IT Act Concurrency

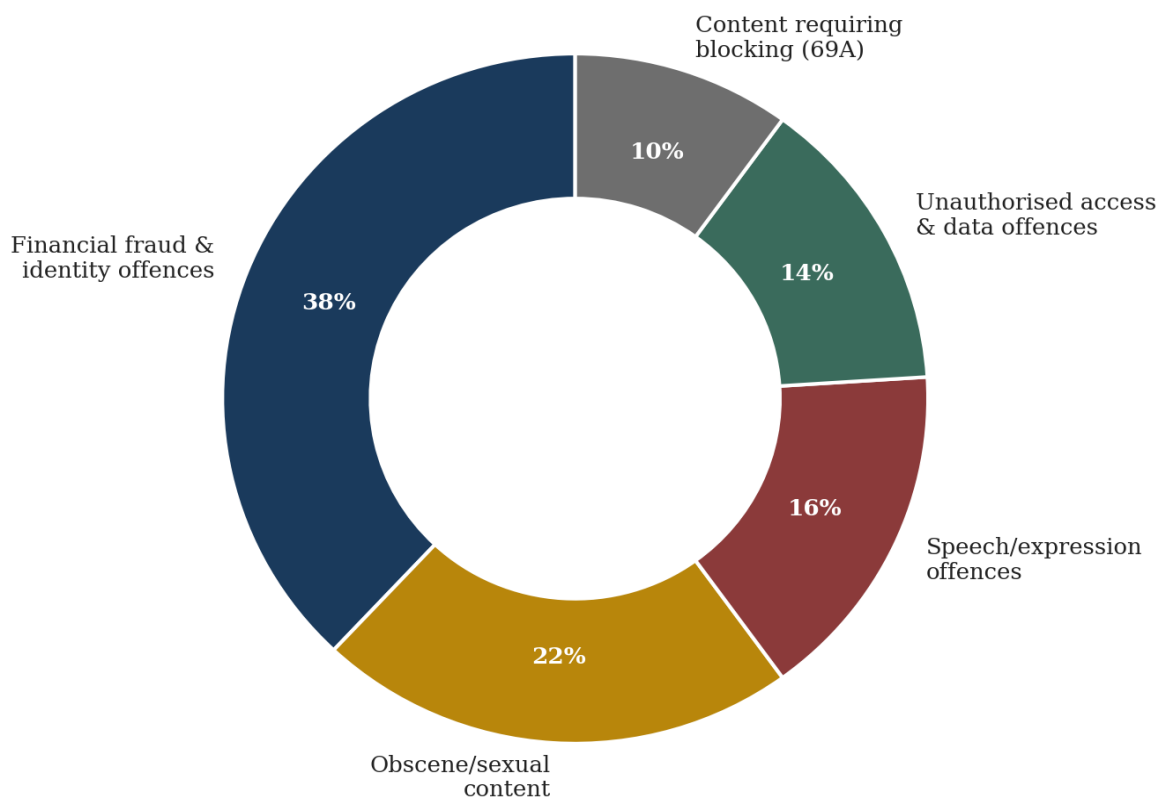
A further dimension of regulatory fragmentation, distinct from but related to the content-blocking controversy examined above, concerns the concurrent operation of the IT Act's technical offence provisions and the BNS's general criminal law provisions in addressing the same underlying online conduct. As with content blocking, this concurrency was not the product of a single coherent legislative design but accumulated incrementally: the IT Act's 2008 amendment introduced technically specific offences (identity theft, cheating by personation, privacy violation) without displacing the general criminal law's applicability to online conduct, while the BNS's 2023 drafting, in turn, extended established general offences (stalking, voyeurism, cheating, forgery) to electronic modality without attempting to consolidate or cross-reference the IT Act's parallel provisions. The consequence, examined in greater technical detail elsewhere in the broader literature on IT Act criminal liability, is that investigating officers and prosecutors must navigate two independently drafted, only loosely coordinated statutory schemes when framing charges for substantially identical online conduct — a practical complexity that compounds, rather than mitigates, the procedural fragmentation this paper identifies in the content-blocking context.

3.8 Institutional Coordination and the Absence of a Unified Regulator

A structural observation underlying much of this Part's analysis is the absence, within India's online-offence regulatory architecture, of a single institutional body with unified oversight across the four regulatory pillars identified in Figure 1. Content-blocking decisions under Section 69A are taken by designated officers within the Ministry of Electronics and Information Technology or, for certain categories, the Ministry of Information and

Broadcasting; intermediary due-diligence compliance is monitored through a combination of self-reporting and grievance-mechanism oversight; substantive criminal prosecution proceeds through state police forces and the Indian Cyber Crime Coordination Centre; and evidentiary questions are ultimately resolved by the ordinary criminal court system applying the BSA framework. This institutional dispersion means that no single body is positioned to identify, still less resolve, the kind of cross-pillar procedural inconsistency the X Corp litigation has exposed, leaving such inconsistencies to surface only through the comparatively slow and case-specific mechanism of individual litigation — a structural deficiency this paper's recommendations address in Part 5.

Figure 4: Illustrative Classification of Regulated Online Offences by Primary Regulatory Mechanism



Note: Illustrative classification synthesised from NCRB cybercrime case-category data and IT Act/BNS offence-provision mapping; categories are not mutually exclusive as conduct often triggers multiple mechanisms.

3.7 Comparative Snapshot: Regulatory Pathways for Online Content

Table 1 summarises the principal procedural characteristics of the two content-blocking pathways examined in this Part.

Feature	Section 69A + 2009 Blocking Rules	Section 79(3)(b) + Rule 3(1)(d) (Sahyog Portal)
Nature of provision	Affirmatively empowering (positive blocking power)	Conditional exemption provision (safe-harbour precondition), per Shreya Singhal
Order form	Written, reasoned order required	Notice conveying 'actual knowledge'; template order format
Review mechanism	Designated officer review + committee examination	No independent committee review identified in commentary
Issuing authority	Central Government (MeitY/MIB) under statutory procedure	Any authorised government officer via Sahyog Portal
Constitutional grounds	Confined to Article 19(2) grounds (sovereignty, security, public order, incitement)	Contested — X Corp alleges application beyond Article 19(2) thresholds
Judicial status (Aug. 2026)	Upheld with safeguards in Shreya Singhal (2015)	Upheld by Karnataka HC (Sept. 2025); subject to further appellate proceedings

Table 1: Comparative snapshot of the Section 69A and Section 79(3)(b)/Rule 3(1)(d) content-blocking pathways.

4. FINDINGS

- India's online-offence regulatory architecture comprises four interlocking but doctrinally distinct pillars — substantive criminalisation, content blocking, intermediary regulation and evidentiary/investigative process — whose independent development has produced significant procedural inconsistency rather than a coherent, integrated regulatory framework.
- *Shreya Singhal v. Union of India*'s structural characterisation of Section 79 as a conditional exemption provision, distinct from Section 69A's affirmatively empowering and procedurally safeguarded blocking power, remains the doctrinal foundation for assessing the constitutionality of content-regulation mechanisms, yet this foundation is under direct and unresolved challenge in the X Corp litigation.

- The Sahyog Portal's operation through Section 79(3)(b) read with Rule 3(1)(d), now reportedly accounting for the substantial majority of government takedown notices issued to at least one major platform, achieves outcomes functionally equivalent to Section 69A blocking without the reasoned-order, designated-officer and committee-review safeguards Shreya Singhal found constitutionally necessary for that power.
- The Karnataka High Court's September 2025 ruling upholding the Sahyog Portal's legality rests on a characterisation of the mechanism as administratively facilitative rather than independently empowering, a characterisation that critical commentary persuasively argues understates its practical speech-regulatory effect and does not adequately confront Shreya Singhal's structural holding on the relationship between Sections 69A and 79.
- Progressive tightening of intermediary due-diligence obligations, including 2025-2026 synthetic-content labelling and verification requirements, creates a structural tension with the neutrality-based rationale underlying Section 79 safe-harbour protection, pushing intermediaries towards an increasingly editorial, content-evaluative posture.
- No IT Act or BNS provision specifically criminalises the malicious creation of deepfake or AI-generated content, leaving a substantive regulatory gap that sits in tension with the state's increasingly assertive, and now procedurally contested, content-blocking capacity.
- The coexistence of procedurally divergent blocking pathways generates both enforcement unpredictability for regulated intermediaries and constitutional vulnerability for affected users and speakers, undermining the proportionality analysis that legitimised Section 69A's more assertive blocking power in the first place.

5. RECOMMENDATIONS

5.1 Legislative and Regulatory Reforms

- Amend the IT Rules to expressly confine Section 79(3)(b)/Rule 3(1)(d) notices to their safe-harbour-conditioning function, and require that any government-initiated content-blocking action proceed exclusively through the procedurally safeguarded Section 69A mechanism, restoring the structural distinction Shreya Singhal articulated.
- Introduce a specifically defined offence addressing the malicious creation and distribution of deepfake and AI-generated content within the BNS or IT Act, distinct from and prior to the existing disclosure and labelling obligations, to close the identified substantive regulatory gap.

- Clarify, through rule-making or authoritative guidance, the boundary between permissible intermediary due-diligence obligations and impermissible editorial control, to resolve the neutrality-safe-harbour tension identified in this paper.

5.2 Procedural and Institutional Reforms

- Extend committee-review-equivalent oversight to any high-volume government content-notice mechanism, including the Sahyog Portal, to ensure procedural safeguards commensurate with the practical speech-regulatory effect of the mechanism, regardless of its formal statutory characterisation.
- Establish an independent appellate or review mechanism accessible to affected users (not merely platforms) for content-blocking and takedown decisions, addressing the standing gap the Karnataka High Court's citizen-only Article 19(1)(a) holding leaves unresolved for non-citizen platforms acting on behalf of Indian users.
- Publish periodic, disaggregated transparency reporting distinguishing takedown volumes and grounds by regulatory pathway (Section 69A versus Section 79(3)(b)/Sahyog), to enable informed public and judicial scrutiny of the relative use of each mechanism.

5.3 Judicial and Doctrinal Development

- Encourage Supreme Court resolution of the Section 69A/Section 79(3)(b) structural question raised in the X Corp litigation, given its significance extending well beyond the immediate parties to the procedural integrity of India's online-content regulatory architecture as a whole.
- Develop clearer doctrinal guidance distinguishing genuine administrative-efficiency mechanisms from functionally equivalent but procedurally unsafeguarded exercises of blocking power, to prevent future erosion of Shreya Singhal's safeguards through mechanism relabelling.

5.4 Institutional Coordination Reforms

- Establish a coordinating body or inter-ministerial working group with cross-pillar oversight of online-offence regulation, spanning content blocking, intermediary compliance, substantive criminal enforcement and evidentiary practice, to identify and address the kind of procedural inconsistency the X Corp litigation has surfaced before it matures into full-scale litigation.

- Task this coordinating body with periodic public reporting on the comparative use, volume and outcomes of the Section 69A and Section 79(3)(b) pathways, supporting the transparency reform proposed in Section 5.2 above and enabling longitudinal assessment of whether procedural harmonisation reforms are achieving their intended effect.

6. CONCLUSION

India's regulation of online offences rests on a substantively comprehensive but structurally fragmented architecture, in which substantive criminalisation, content blocking, intermediary regulation and evidentiary process have each developed along largely independent doctrinal and procedural tracks. This analysis demonstrates that this fragmentation is not merely an academic concern: the ongoing *X Corp v. Union of India* litigation reveals, in stark and practically consequential terms, how the coexistence of procedurally divergent content-regulation pathways can produce outcomes that functionally circumvent the constitutional safeguards painstakingly established in *Shreya Singhal v. Union of India* a decade earlier. The Karnataka High Court's 2025 validation of the Sahyog Portal mechanism, whatever its administrative-efficiency justifications, leaves unresolved the deeper structural question of whether India's online-offence regulatory framework can sustain two materially different procedural standards for functionally equivalent content-regulation outcomes without undermining the very proportionality analysis that legitimises governmental power to restrict online speech and content. Beyond this immediate controversy, the framework's continuing silence on the substantive criminalisation of deepfake and AI-generated content, and the structural tension between intermediary neutrality and expanding due-diligence obligations, point to a regulatory architecture under genuine strain from technological change it was not originally designed to accommodate. Restoring doctrinal coherence will require deliberate legislative and judicial attention to harmonising procedural safeguards across regulatory pathways, closing substantive gaps in emerging offence categories, and ensuring that administrative convenience does not, in practice, erode the constitutional protections India's highest court found essential to a proportionate and legitimate system of online-content regulation.

REFERENCES

A. Statutes and Regulatory Instruments

1. *Information Technology Act, 2000 (Act No. 21 of 2000)*, ss. 66-67C, 69A, 79.
2. *Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009)*.
3. *Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009*.
4. *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023 and 2025*.
5. *Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)*.
6. *Bharatiya Nagarik Suraksha Sanhita, 2023; Bharatiya Sakshya Adhiniyam, 2023*.
7. *Digital Personal Data Protection Act, 2023*.
8. *Constitution of India*, arts. 19(1)(a), 19(2), 21.

B. Cases

9. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
10. *X Corp v. Union of India*, W.P. No. 7405/2025, Karnataka High Court, order dated 24 September 2025.
11. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
12. *Sadhguru Jagadish Vasudev & Anr. v. Igor Isakov & Ors.*, 2024 SCC OnLine Del 3267.

C. Journal Articles, Book Chapters and Commentary

13. "Safe Harbor and Content Moderation Regulation in India," in *Defeating Disinformation* (Cambridge University Press, 2025).
14. "Facilitating Digital Censorship – I: A Critique of the Karnataka High Court's Decision in *X v Union of India*," *Indian Constitutional Law and Philosophy Blog* (2025).
15. "Karnataka High Court Ruling on Content Blocking: A Setback for User Rights," *Indian Journal of Constitutional Law*, NALSAR (2025).

D. Web and Institutional Sources

16. "X Relies on 'Shreya Singhal' in Arbitrary Content-Blocking Case in Karnataka HC," *Supreme Court Observer* (2025), <https://www.scobserver.in>.

17. "Karnataka HC's Order in X Case Exemplifies Sheer Judicial Indiscipline," *The Leaflet* (2025), <https://theleaflet.in>.
18. "An Exhaustive Takedown of Karnataka HC's Decision Upholding Sahyog Portal in X Corp v. Union of India," *The Leaflet* (2025), <https://theleaflet.in>.
19. "The Ghost of Shreya Singhal: Re-litigating Digital Free Speech," *Citizens for Justice and Peace* (2025), <https://cjp.org.in>.
20. "India Dispatch: Social Media Platform X to Challenge Karnataka High Court Ruling over Free Speech Concerns," *JURIST* (2025).
21. "The Karnataka High Court on Content Blocking: What the X Corp Rulings Mean for Platform Accountability in India," *AMLegals* (2025-26), <https://amlegals.com>.
22. "India IT Rules 2021: Compliance Burdens, Speech and Privacy," *Law.asia* (2026), <https://law.asia>.
23. "Safe Harbour Principle and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules (2021)," *Mondaq* (2021).
24. "Safe Harbour for Social Media," *Shankar IAS Current Affairs* (2025), <https://www.shankariasparliament.com>.
25. "Revisions to the Information Technology Intermediary Rules (India)," *Lexology* (2026).
26. "IT Rules 2025: New Intermediary Liability & Rule 3(1)(d)," *Neeti Niyaman* (2025), <https://neetiniyaman.com>.
27. "Intermediary Liability & Data Protection Cyber Law," *Legal Blur* (2025), <https://legalblur.com>.

WHITE BLACK
LEGAL