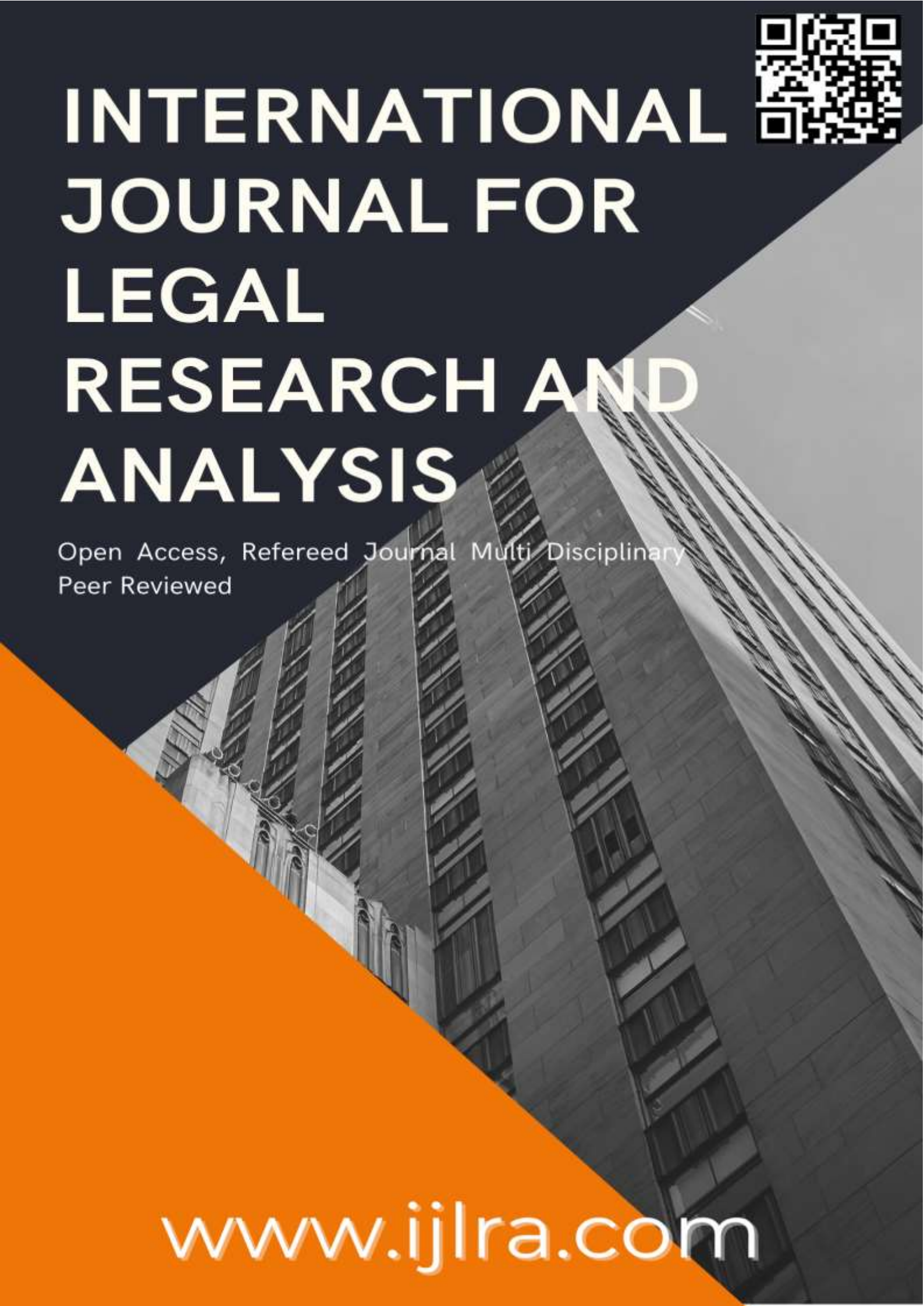
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

INTERMEDIARY LIABILITY AND E-COMMERCE JURISPRUDENCE IN INDIA: FROM SAFE HARBOUR TO EVOLVING STANDARDS OF ACCOUNTABILITY

AUTHORED BY - GUNJA DUBEY
(Research Scholar)
Nehru Gram Bharti (Deemed to be University, Prayagraj

CO-AUTHOR - DR. SUNIL KUMAR MISHRA
(Assistant Professor)
Nehru Gram Bharati (Deemed to be University), Prayagraj

Abstract

The rapid digitization of the Indian marketplace has necessitated a fundamental re-evaluation of the legal protections afforded to digital intermediaries. Traditionally, the "Safe Harbour" doctrine under Section 79 of the Information Technology Act, 2000, served as a blanket immunity, shielding platforms from liability for third-party content to foster technological innovation. However, as e-commerce entities evolved from passive conduits into active ecosystem orchestrators—engaging in inventory management, logistics, and algorithmic curation—the judicial and legislative stance has shifted toward "proactive accountability." This paper explores the transition from the "actual knowledge" standard established in *Shreya Singhal v. Union of India* to the stringent due diligence requirements mandated by the IT Rules, 2021, and the Consumer Protection (E-Commerce) Rules, 2020. By analyzing landmark precedents such as *Christian Louboutin v. Nakul Bajaj*, the study highlights the emergence of a "responsibility-based model." It concludes that while heightened standards protect consumer interests and national security, they pose significant challenges to the principles of data privacy and the operational autonomy of digital platforms in India's burgeoning digital economy.

Keywords: Safe Harbour, Intermediary Liability, Due Diligence, E-commerce Jurisprudence, IT Rules 2021.

ISSN: 2582-6433

1. Introduction

The digital revolution in India has transformed the internet from a mere repository of information into a sophisticated marketplace of ideas and commerce. At the heart of this transformation lies the 'intermediary'—an entity that facilitates the flow of data, goods, and services between third parties. Historically, the legal framework governing these entities was rooted in the "Safe Harbour" doctrine, which provided a protective shield against liability for third-party content. This immunity was considered a *sine qua non* for the growth of the early internet, ensuring that platforms were not stifled by the Herculean task of monitoring every byte of data transmitted through their systems.

The primary legislative instrument in this regard is **Section 79 of the Information Technology Act, 2000**,[1] which creates a "conditional immunity" for intermediaries[2]. However, the definition of an intermediary has undergone significant judicial expansion.[3] While early jurisprudence viewed platforms as "passive pipes," the contemporary e-commerce landscape sees them as active participants who curate, rank, and often influence consumer choice.[4] This evolution has led to a tension between the statutory protection of the "Safe Harbour" and the constitutional and consumer-centric need for accountability.

In recent years, the Indian judiciary and the executive have signalled a departure from the "hands-off" approach. The shift from "actual knowledge" as defined in the landmark *Shreya Singhal* case[5] to the "proactive due diligence" mandated by the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**[6], marks a watershed moment. This paper aims to analyse this jurisprudential shift, examining how e-commerce platforms are increasingly being held to higher standards of "duty of care" and "fallback liability," effectively narrowing the scope of the Safe Harbour in the interest of public order and consumer protection.

[1] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gaz. of India, Pt. II Sec. 3(i) (Feb. 25, 2021).
[2] Information Technology Act, 2000, s. 2(1)(w) defines an 'intermediary' as any person who on behalf of another person receives, stores or transmits that message or provides any service with respect to that message.
[3] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[4] Vakul Sharma, *Information Technology Law and Practice* 45 (LexisNexis, 7th edn., 2022).
[5] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[6] Consumer Protection (E-Commerce) Rules, 2020, r. 6.

ISSN: 2582-6433

2. The Statutory Framework and the Doctrine of Safe Harbour: The Digital "Umbrella"

To understand the current friction between Big Tech and the Indian State, we must look back at the turn of the millennium. When the **Information Technology Act, 2000** was first penned, the internet was a fragile frontier. Lawmakers realized that if a platform like an early search engine or a message board could be sued for every stray comment or copyright infringement committed by its users, the digital economy would collapse before it even began. This birthed the **"Safe Harbour"** doctrine—a legal pact that essentially says: *"Don't shoot the messenger."*[7] However, the original Act of 2000 was largely silent on the specifics of this immunity, leaving platforms in a state of legal limbo whenever a dispute arose.

It wasn't until the **Information Technology (Amendment) Act, 2008**[8] that India truly modernized its stance, moving away from a rudimentary exemption to a sophisticated, yet conditional, shield. This amendment was born out of necessity, following high-profile incidents where platform executives were arrested for content they didn't even know existed on their servers. The 2008 amendment introduced the current **Section 79**,[9] which acts as a "buffer zone" between the intermediary and the chaotic world of third-party content. It was designed to ensure that as long as a platform played by the rules, it wouldn't be held hostage by the illegal actions of its users.

2.1 The "Passive Pipe" Philosophy: Section 79(2)

The law operates on a fundamental assumption: the intermediary is a neutral conduit, a "digital pipe" that merely carries data without touching its substance. This philosophy suggests that just as a post office isn't responsible for the contents of a letter, a website shouldn't be responsible for the contents of a post. To stay under this protective umbrella, an entity must pass a "Triple Test" of neutrality:[10]

1. **Technical Passivity:** The platform's role must be strictly limited to providing the infrastructure—the wires, servers, and cloud space—that allow information to travel from Point A to Point B.

[7] N.S. Nappinai, *Cyber Laws* 625 (LexisNexis, 1st edn., 2017).
[8] The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
[9] The Information Technology Act, 2000 (Act 21 of 2000), s. 79(2).
[10] *Id.*, s. 79(2)(a).

ISSN: 2582-6433

2. **Zero Interference:** The intermediary must stay out of the editorial process. It cannot initiate the message, it cannot choose who receives it, and most importantly, it cannot "select or modify" the content.[11] If a platform edits a user's post, it effectively becomes an "editor" or "publisher," and the Safe Harbour evaporates instantly.
3. **The "Good Citizen" Requirement:** Protection is not a free pass. It is contingent on the intermediary following "due diligence" guidelines laid down by the government. This means maintaining a grievance officer and having a clear terms-of-service agreement. If a platform turns a blind eye to systemic abuse or fails to have a functioning complaint mechanism, the shield vanishes.[12]

This "neutrality" is the bedrock of the internet; without it, every social media comment section would be disabled, and every e-commerce listing would require a manual legal review before going live.

2.2 The Threshold of "Actual Knowledge" and the "Chilling Effect"

The most contentious part of this framework has always been the "Take-Down" mechanism under **Section 79(3)(b)**. The law states that once an intermediary has **"actual knowledge"** of an unlawful act, it must move with lightning speed to disable access to that content.[13] In the early years of the Act, the definition of "actual knowledge" was dangerously broad. It wasn't clear if a phone call, a tweet, or a legal notice from a private citizen constituted "knowledge." This ambiguity created a "Wild West" of legal notices. Platforms were flooded with "cease and desist" emails from private individuals who simply disliked certain content. Fearing criminal liability and the arrest of their local directors, platforms often deleted perfectly legal content just to be safe—a phenomenon known as the **"Chilling Effect."**[14] This era was defined by a nervous "delete first, ask questions later" mentality, where the intermediary was forced to act as a private judge, jury, and executioner over the digital town square, often sacrificing the user's right to free speech at the altar of corporate safety.[15] This period proved that without a clear judicial standard for "knowledge," the Safe Harbour was actually a tool for silencing dissent.

[11] *Id.*, s. 79(2)(b).
[12] Justice G.P. Singh, *Principles of Statutory Interpretation* 142 (LexisNexis, 14th edn., 2016).
[13] The Information Technology Act, 2000 (Act 21 of 2000), s. 79(3)(b)
[14] Apar Gupta, "Free Speech and Intermediary Liability", 49 *Econ. & Pol. Wkly.* 12 (2014).
[15] *Avnish Bajaj v. State (NCT) of Delhi*, (2005) 3 Comp LJ 364 (Del).

ISSN: 2582-6433

3. The Judicial Metamorphosis: From Passive Pipes to Active Policing

The real turning point for intermediary liability in India wasn't just a change in the text of the law, but a fundamental shift in how the courts began to interpret the "silence" of a platform. For years, digital entities lived in a state of perpetual legal anxiety: if a user complained about a post, should the platform delete it immediately to stay safe, or keep it up to protect free speech? This dilemma created a "trigger-happy" culture of private censorship where platforms, fearing criminal prosecution and the arrest of their directors, became the invisible censors of the Indian internet. The judiciary eventually realized that leaving the power of censorship in the hands of private corporations—who prioritize risk mitigation over constitutional rights—was a recipe for democratic decay. This led to a series of corrective judgments that moved the needle from "automatic liability" to "judicially overseen accountability."

3.1 The Shreya Singhal Revolution: Protecting the Digital Square

In 2015, the Supreme Court of India stepped in with the landmark **Shreya Singhal v. Union of India**[16] ruling, which effectively saved the Indian internet from becoming a sterile, over-moderated space. The Court astutely observed that if every disgruntled user's email or "notice" could force a platform to take down content under the threat of losing their Safe Harbour, the internet would lose its vibrancy and become a tool for the thin-skinned. By "reading down" Section 79(3)(b), the Court clarified that **"actual knowledge"** does not mean a random notification from a third party; instead, it requires a **court order** or a **government notification**.[17]

This shift was monumental because it outsourced the "judging" back to the State, ensuring that intermediaries were not forced to play judge and jury over complex constitutional questions of free speech. It allowed platforms to breathe, knowing they wouldn't be held in contempt for a user's tweet unless a magistrate or a designated government official explicitly said so.[18]This provided a much-needed period of "Digital Stability" where innovation could flourish without the constant shadow of frivolous litigation, firmly establishing that the intermediary is a facilitator of speech, not its regulator.

[16] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[17] *Id.*, at 1560.
[18] Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* 198 (Oxford University Press, 2016).

ISSN: 2582-6433

3.2 The "Active Participant" Exception: Christian Louboutin

However, the honeymoon period for e-commerce platforms ended when they started doing more than just "hosting" products for a fee. In the transformative case of **Christian Louboutin SAS v. Nakul Bajaj**,[19] the Delhi High Court drew a sharp, necessary line in the sand between a "marketplace" and a "seller." The defendant's website, Darveys.com, wasn't just a digital notice board; it actively curated luxury goods, used high-end brand trademarks to lure traffic, and managed the entire logistics chain from the overseas seller to the Indian doorstep. The Court held that when a platform crosses the line into **active participation**—by identifying sellers, promoting products as "authentic," or guaranteeing the quality of the goods—it sheds its skin as a neutral intermediary.[20]

The Court introduced a "list of factors" to identify an active participant, including whether the platform identifies the seller, provides transport, or uses the trademark in its meta-tags.[21]This ruling sent shockwaves through the e-commerce industry, signalling that "Safe Harbour" is not a get-out-of-jail-free card for business models designed to profit from the ambiguity of third-party listings. It effectively created a hybrid status: a platform could be an intermediary for some services but a "service provider" or "seller" for others, moving the legal needle from "blind immunity" to "commercial responsibility."[22] This ensured that luxury brands and consumers alike had a remedy against platforms that turned a blind eye to counterfeits while pocketing a commission from the sale.[23]

4. The 2021 IT Rules: The End of the "Hands-Off" Era

If the *Shreya Singhal* era was the high-water mark for platform protection, the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**[24] represent the tide pulling back with aggressive regulatory force. The government pivoted the legal burden from "wait for a court order" to "proactively police your own backyard." This shift acknowledges that in an era of viral misinformation, coordinated "cancel culture," and deepfakes, the passive model of 2000 is no longer sustainable for national security or social harmony. The 2021 Rules introduced a sophisticated, tiered system of compliance, recognizing that a small community blog shouldn't be governed by the same heavy-handed rules as a tech

[19] *Christian Louboutin SAS v. Nakul Bajaj*, (2018) 253 DLT 728
[20] *Id.*, at 745
[21] *Id.*, at 751
[22] Vakul Sharma, *Information Technology Law and Practice* 112 (LexisNexis, 7th edn., 2022).
[23] *Myspace Inc. v. Super Cassettes Industries Ltd.*, (2017) 236 DLT 478 (DB).
[24] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Gaz. of India, Pt. II Sec. 3(i) (Feb. 25, 2021).

ISSN: 2582-6433

giant with 500 million users. However, this nuance came with a heavy price: the requirement for "Significant Social Media Intermediaries" (SSMIs) to deploy automated filtering tools, which critics argue marks the return of algorithmic censorship.[25]

4.1 The New Compliance Straitjacket

Under these rules, "Safe Harbour" is no longer an inherent statutory right; it has been transformed into a **revocable privilege** contingent on meeting a gruelling checklist of "Due Diligence."[26] The 2021 Rules require platforms to move at a speed previously unseen in Indian law. For instance, any content involving non-consensual nudity or morphed images must be removed within **24 hours** of receiving a complaint.[27] This is a radical departure from the "actual knowledge" standard of 2015, as it forces platforms to act on private complaints without waiting for a judicial rubber stamp. By prioritizing victim safety over corporate convenience, the law has essentially ended the era of the "unregulated intermediary" in India, turning these digital giants into quasi-judicial entities that must resolve thousands of disputes daily.

4.2 Local Accountability and the Personal Liability Trap

Perhaps the most controversial aspect of the 2021 Rules[28] is the mandate for "local presence." Large platforms are now required to appoint a **Chief Compliance Officer**, a **Nodal Contact Person**, and a **Resident Grievance Officer**,[29] all of whom must be residents of India.[30] Crucially, the Chief Compliance Officer can be held **personally and criminally liable** if the company fails to follow a government take-down order or a law enforcement request. This "hostage-style" compliance model ensures that Silicon Valley giants cannot ignore Indian law from a distance. Furthermore, the "Traceability" mandate requires messaging platforms to identify the "first originator" of a message upon a legal order—a rule that has sparked a constitutional standoff.[31] Critics argue this shatters the "Privacy by Design" model of end-to-end encryption, while the State maintains it is a necessary tool to catch those inciting riots or spreading child sexual abuse material (CSAM).[32]

[25] Chinmayi Arun, "The 2021 IT Rules and the Future of the Indian Internet", 56 *Econ. & Pol. Wkly.* 15 (2021).
[26] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3.
[27] *Id.*, r. 3(2)(b).
[28] Ministry of Electronics and Information Technology (MeitY), *FAQs on Intermediary Guidelines and Digital Media Ethics Code Rules* (2021).
[29] *Facebook India Online Services Pvt. Ltd. v. Delhi Legislative Assembly*, (2021) SCC OnLine SC 448.
[30] *Id.*, r. 4(1).
[31] *WhatsApp LLC v. Union of India*, W.P.(C) 3959/2021 (Del).
[32] Abhinav Chandrachud, *Republic of Rhetoric: Free Speech and the Constitution of India* 215 (Penguin, 2017).

ISSN: 2582-6433

5. E-Commerce Accountability and Consumer Protection: Beyond the "Digital Notice Board"

The most profound evolution in intermediary jurisprudence has occurred within the e-commerce sector, which for years operated in a state of legal "exceptionalism." For over a decade, online marketplaces like Amazon, Flipkart, and Snapdeal functioned under the comfortable assumption that they were merely digital "notice boards" connecting buyers and sellers. However, as these platforms began to manage payments, handle returns, offer "guaranteed" delivery, and even launch their own private labels, the gap between their legal claims of being "neutral conduits" and their operational reality became a chasm too wide for the law to ignore. The transition from a "hands-off" marketplace to a deeply managed ecosystem has stripped away the traditional Safe Harbour, replacing it with a robust framework of **Consumer Protection** that prioritizes the buyer's trust over the platform's immunity.

5.1 The Death of the "Passive" Marketplace and Fallback Liability

The turning point for the industry came with the notification of the **Consumer Protection (E-Commerce) Rules, 2020**,[33] which finally synchronized the law with the modern shopping experience. These rules introduced the revolutionary concept of **"Fallback Liability."**[34]Historically, if a consumer bought a defective phone from a third-party seller on a large platform, the platform would simply point to its Terms of Service and tell the consumer to sue the seller—who was often untraceable or insolvent. Under the new regime, if a seller fails to deliver goods or services as promised, the e-commerce entity is held jointly liable if it has made any representation of authenticity or handled the fulfillment process.[35] This ensures that the platform, which pockets a commission from the transaction, also carries the risk of the transaction's failure.

This shift effectively turns the platform into a "guarantor" of the trade, forcing tech giants to move from a volume-based growth model to a quality-controlled governance model where every seller must be rigorously vetted.[36]

5.2 Algorithmic Accountability and the War on "Dark Patterns"

The modern e-commerce platform doesn't just host products; it uses complex, proprietary

[33] Consumer Protection (E-Commerce) Rules, 2020, Gaz. of India, Pt. II Sec. 3(i) (July 23, 2020).
[34] *Id.*, r. 6(4)
[35] *Amazon Seller Services Pvt. Ltd. v. Amway India Enterprises Pvt. Ltd.*, (2020) 267 DLT 228 (DB).
[36] Prateek Bhattacharya, "The Evolving Liability of E-commerce Intermediaries in India", 23 J. of World Intellect. Prop. 612 (2020).

ISSN: 2582-6433

algorithms to decide which products a consumer sees first. This "curation" is where the legal definition of an intermediary begins to crumble. When a platform ranks its own "house brands" higher than independent competitors, or uses **"Dark Patterns"**—deceptive user interfaces designed to trick users into buying insurance or adding items to their carts—it is no longer a neutral conduit.[37]The judiciary has signaled that if a platform's algorithm actively promotes infringing, deceptive, or biased content, the platform has "selected" that information under Section 79(2)(b) and thus forfeits its immunity.[38]

The 2020 Rules and subsequent guidelines now require platforms to be transparent about their "ranking parameters," ensuring that the "digital shelf" is not rigged against small-scale Indian sellers.[39] This marks a move toward **"Algorithmic Accountability,"** where the code itself—the invisible hand of the digital market—is subject to the rule of law and the principles of fair competition. By holding platforms accountable for how they direct consumer attention, the law is ensuring that the "Safe Harbour" does not become a sanctuary for anti-competitive behaviour or consumer exploitation.[40]

6. Conclusion: Toward a "Responsibility-Based" Digital Future

The trajectory of intermediary liability in India has come full circle—from the near-absolute immunity of the early 2000s to a contemporary era defined by "Conditional Accountability." We have transitioned from a legal regime where the "Messenger" was invisible and untouchable, to one where the Messenger is now the gatekeeper, the policeman, and the ultimate guarantor of the digital economy. This evolution reflects a global realization: as platforms grow to command more power than many nation-states, the "Safe Harbour" can no longer be an unconditional right. It must be a earned privilege, contingent upon a platform's commitment to user safety, transparency, and the rule of law.

The shift from the **Shreya Singhal** standard of "Judicial Knowledge" to the **IT Rules 2021** standard of "Proactive Diligence" represents a fundamental change in the social contract between the State and Big Tech. While the judiciary remains the ultimate guardian of free speech, the executive has stepped in to manage the darker side of the digital frontier—misinformation, non-consensual content, and anti-competitive e-commerce practices. The

[37] Ministry of Consumer Affairs, *Guidelines for Prevention and Regulation of Dark Patterns* (2023).
[38] Christian Louboutin SAS v. Nakul Bajaj, (2018) 253 DLT 728.
[39] Central Consumer Protection Authority (CCPA), *Advisory on Fair Trade Practices in E-Commerce* (2022).
[40] Justice Pratibha M. Singh, *Judicial Trends in Intellectual Property* 88 (Universal Law Publishing, 2021).

ISSN: 2582-6433

"Passive Pipe" model is officially dead; in its place is a hybrid system where liability is tied to the degree of control an entity exerts over its data and its users.

6.1 The Road to the Digital India Act

As India prepares to replace the aging IT Act with the proposed **Digital India Act**,[41] the focus is shifting toward "Algorithmic Accountability" and "Safe Harbour 2.0." This future framework is expected to formalize a "sliding scale" of liability: a simple ISP may retain broad immunity, while a "Gatekeeper" e-commerce platform or an AI-driven social media giant will carry a much heavier burden of care.[42] The message to digital platforms is clear: the era of the "unregulated intermediary" is over. To enjoy the protections of the Indian market, entities must adopt a "Compliance by Design" approach, ensuring that their business models do not profit from the erosion of consumer rights or public order. Ultimately, the goal of Indian jurisprudence is to create a "Trustworthy Internet"—one where innovation and accountability are not seen as opposing forces, but as two sides of the same coin.[43,44]

[41] Ministry of Electronics and Information Technology (MeitY), *Proposed Principles of Digital India Act* (2023).
[42] N.S. Nappinai, *Cyber Laws* 640 (LexisNexis, 1st edn., 2017).
[43] Abhinav Chandrachud, *Republic of Rhetoric: Free Speech and the Constitution of India* 215 (Penguin, 2017).
[44] *Facebook India Online Services Pvt. Ltd. v. Delhi Legislative Assembly*, (2021) SCC OnLine SC 448.