

# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary  
Peer Reviewed

[www.ijlra.com](http://www.ijlra.com)

## DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.  
All rights reserved.**

## 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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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.

## ***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.

## **APP-BASED DRUG TRAFFICKING IN INDIA: PLATFORM LIABILITY AND THE INDIVIDUAL CULPABILITY OF THE ACCUSED UNDER THE NDPS ACT.**

AUTHORED BY – SUMIT GURJAR<sup>1</sup>, VEDANT THAKUR<sup>2</sup>  
& SAMRIDDH SHARMA<sup>3</sup>

### **ABSTRACT**

The rapid digitization of the Indian economy has facilitated a fundamental shift in the architecture of organized crime, particularly within the illicit narcotics trade. The emergence of hyper local delivery services and gig-economy platforms has inadvertently supplied drug trafficking syndicates with a sophisticated, low-risk infrastructure for the domestic transportation of contraband, including high-potency synthetic substances such as methamphetamine, mephedrone, and LSD, alongside hydroponic cannabis. This transition from localized, physical hand-to-hand transactions to an app-mediated 'Drugs-as-a-Service' (DaaS) model, increasingly structured on a decentralized drop-shipping framework, presents profound challenges to the existing legal architecture. At the heart of this crisis sits a double friction: first, between the conditional immunity granted to digital intermediaries under the Information Technology (IT) Act, 2000, and the stringent, zero-tolerance mandates of the Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985; and second, within the NDPS framework itself, between the reverse-burden presumptions that make prosecution comparatively easy and the constitutional guarantee that no person may be punished without a fair opportunity to rebut the case against them.

This paper examines both halves of that friction. It begins with the platform-level question of intermediary liability that occupied the original literature on this subject, and then turns as its central concern to the liability of the individual drug accused within the app-based ecosystem: the kingpin who designs the operation, the financier who bankrolls it, the peddler who books the delivery, the gig-economy rider who unknowingly carries the parcel, and the end-consumer who receives it. Each of these actors occupies a different position on the NDPS Act's spectrum of culpability, and the reverse-burden presumptions of Sections 35 and 54, the bail bar under

---

<sup>1</sup> Fourth year B.sc L.Lb student at National law institute university ,Bhopal

<sup>2</sup> Fourth year B.sc L.Lb student at National law institute university ,Bhopal

<sup>3</sup> Fourth year B.A L.Lb student at National law institute university ,Bhopal

Section 37, and the confession jurisprudence following *Tofan Singh v State of Tamil Nadu* operate very differently depending on where an accused sits in that chain. Understanding this differentiated liability is essential to any coherent policy response to app-based trafficking, because a framework that treats the unwitting delivery rider and the syndicate financier identically is neither doctrinally sound nor likely to survive appellate scrutiny.

### **The Architecture of Intermediary Liability and the Safe Harbor Doctrine**

The legal status of delivery platforms such as Porter, Uber Connect, and Dunzo is primarily governed by Section 79 of the Information Technology Act, 2000. This provision establishes the “safe harbor” principle, which shields intermediaries from liability for third-party information, data, or communication links made available or hosted by them. However, the definition of an “intermediary” is not static. Under the IT Act, an intermediary is defined widely as any person who, on behalf of another person, receives, stores, or transmits an electronic record or provides any service with respect to that record. This definition extends to telecom service providers, network service providers, internet service providers, digital marketplaces, web-hosting service providers, search engines, online payment sites, online-auction sites, and online marketplaces.<sup>4</sup>

The immunity provided under Section 79(1) is conditional. To avail of safe harbor, an intermediary must satisfy the cumulative requirements set out in Section 79(2). First, the intermediary’s role must be limited to providing access to a communication system over which third-party information is transmitted, stored, or hosted. Second, the intermediary must not initiate the transmission, select the receiver of the transmission, or select or modify the information contained in the transmission. Third, and perhaps most critically in the contemporary regulatory climate, the intermediary must observe “due diligence” while discharging its duties under the Act and follow guidelines prescribed by the Central Government.<sup>5</sup>

The evolution of the “due diligence” requirement has seen a transition from a passive, hands-off approach to an increasingly proactive monitoring regime. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, mandate that intermediaries must publish their terms of service and privacy policy, explicitly prohibiting users from hosting or transmitting any information that violates any law for the time being in

<sup>4</sup> Information Technology Act 2000, s 2(1) (w).

<sup>5</sup> Information Technology Act 2000, s 79(2)(c).

force, which includes the NDPS Act. decentralized, platform-mediated narcotics supply chain that closely mirrors legitimate e-commerce distribution models.<sup>6</sup> Furthermore, Section 79(3) clarifies that safe harbor protection is lost if the intermediary has conspired, abetted, aided, or induced the commission of an unlawful act, or if it fails to expeditiously remove or disable access to unlawful material upon receiving “actual knowledge” of its existence.<sup>7</sup> This transformation reflects a broader shift toward a decentralized, platform-mediated narcotics supply chain that closely mirrors legitimate e-commerce distribution models

Retaining this safe harbor, however, is conditional on satisfying several cumulative requirements under Section 79. The intermediary must maintain limited functionality as a conduit under Section 79(2)(a), which is difficult to sustain when the app itself manages logistics and pricing. Section 79(2)(b) requires that the intermediary not select the receiver of a transmission or modify the data transmitted, a condition compromised by the algorithmic matching of riders to specific delivery targets. Section 79(2)(c) requires observance of prescribed “due diligence,” which in practice includes mandatory KYC checks and the reporting of suspicious items. Section 79(3)(a) requires the absence of abetment or inducement; profiting from drug-delivery commissions may itself be construed as abetment. Finally, Section 79(3)(b) requires the expeditious removal of unlawful material upon receiving “actual knowledge,” a standard whose meaning in physical logistics differs sharply from its meaning for purely digital content.

The interpretation of “actual knowledge” was fundamentally altered by the Supreme Court of India in the landmark case *Shreya Singhal v Union of India* (2015)<sup>8</sup>. The Court held that intermediaries are not required to act upon private complaints or their own discretion to determine the legality of content; instead, actual knowledge is strictly confined to the receipt of a court order or a directive from the appropriate government agency. While this interpretation safeguards free speech on digital content platforms, its transposition to physical logistics networks creates a significant enforcement vacuum. In the time required to secure a court order, a physical consignment containing narcotics may be delivered and dissipated before any regulatory intervention can be operationalized, leaving no physical evidence for law enforcement to seize.

---

<sup>6</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, r 3

<sup>7</sup> Information Technology Act 2000, s 79(3).

<sup>8</sup> *Shreya Singhal v Union of India* (2015) 5 SCC 1 [117]-[119] (Nariman J).

## **The Active Facilitator: Testing the Limits of Safe Harbor in Logistics**

The distinction between a “passive” intermediary and an “active” facilitator is the primary point of contention in litigation surrounding delivery and e-commerce platforms. The Delhi High Court has consistently tightened the safe harbor ambit for platforms that participate actively in the commercial lifecycle of a transaction. In *Christian Louboutin SAS v Nakul Bajaj* (2018), the Court identified several criteria to determine whether an e-commerce platform has crossed the line from hosting to facilitation, including exercising control over product listings, managing logistics, offering warranties, and handling customer engagement.<sup>9</sup>

When a platform like Porter or Uber Connect manages the entire delivery process assigning a specific rider, providing a real-time tracking interface, setting the price, and taking a commission on the transaction it ceases to function as a neutral conduit and assumes the role of an active participant in the transactional chain. The Court in the *Darveys.com* line of reasoning reinforced this, noting that a platform which guarantees authenticity or maintains close contractual relationships with sellers is a facilitator even if it complies with basic intermediary guidelines.<sup>10</sup> This “logistics paradox” suggests that the more efficient and integrated a delivery app becomes, the less likely it is to qualify for the Section 79 shield.

The doctrine of “constructive knowledge” further complicates the defense of delivery platforms. This legal theory posits that a platform is deemed to have knowledge of an activity if the tools to detect it are readily available and the platform chooses to ignore them a state of “willful blindness.” Given that these apps employ advanced behavioral analytics and route-optimization algorithms, the claim that such platforms are incapable of detecting patterns of suspicious delivery behavior, such as high-frequency short-distance bookings using pseudonyms in known narcotics hotspots, is increasingly untenable as a matter of law.

## **Algorithmic Negligence and the Duty of Care in the Gig Economy**

The integration of artificial intelligence and machine learning into hyper local logistics has birthed a new category of legal liability: algorithmic negligence. This concept centers on the failure of a platform to exercise reasonable care in the design and implementation of its decision-making systems.<sup>11</sup> In the context of drug trafficking, algorithmic negligence occurs

<sup>9</sup> *Christian Louboutin SAS v Nakul Bajaj* 2018 SCC OnLine Del 12215 [92] (Singh J).

<sup>10</sup> *Christian Louboutin SAS v Nakul Bajaj* 2018 SCC OnLine Del 12215 [84]–[90] (Singh J) (*Darveys.com* as defendant).

<sup>11</sup> cf Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015) ch 3.

when a platform's design priorities speed, cost-reduction, and "frictionless" user experience overtly ignore the foreseeable risk of its infrastructure being utilized for the movement of illicit substances.

Scholars describe this phenomenon as "algorithmic negligence by design," where the deliberate opacity of AI systems, often referred to as the "black box problem," allows platforms to evade responsibility. as an anonymous, unverified package delivery service it has breached its duty of care to the public.<sup>12</sup> By keeping the inner workings of their matching and risk-assessment algorithms proprietary and secret, platforms can claim that any criminal activity facilitated by their system was an unintended consequence that was not "foreseeable." However, the "tortification" of digital law argues that if a platform creates a system that makes a specific harm more likely such

The application of Bayesian–Neumann risk-mitigation theory in content and logistics liability suggests that platforms must move from a reactive "notice-and-takedown" model to a proactive "risk-mitigation" model. This involves shifting the burden of proof to the platform operator, who must present evidence of its efforts to detect and prevent illegal activities within its system.<sup>13</sup> For a delivery app, this would mean demonstrating that its algorithm includes anomaly-detection protocols designed to flag suspicious delivery patterns or "red flags" associated with drug peddling.

### **Indicators of Algorithmic Negligence in Delivery Systems**

- Failure to Implement Verified Identity: allowing senders to book deliveries using unverified accounts or burner phones, despite the availability of e-KYC (Know Your Customer) technology in India.
- Opacity of Matching Logic: lack of transparency in how riders are matched with consignments, potentially allowing a specific rider and peddler to "collude" through repeated manual selection or system manipulation.

---

<sup>12</sup> Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press 2015) <[https://tetrazolelover.at.ua/Frank\\_Pasquale-The\\_Black\\_Box\\_Society-The\\_Secret\\_Al.pdf](https://tetrazolelover.at.ua/Frank_Pasquale-The_Black_Box_Society-The_Secret_Al.pdf)> accessed 6 February 2026; Ilke Karatas, 'Negligent Algorithmic Discrimination' (2024) 4 *Studia Iuris* (KRE ÁJK) <[https://ajk.kre.hu/images/doc2024/studia\\_iuris/202414/ilke\\_karatas.pdf](https://ajk.kre.hu/images/doc2024/studia_iuris/202414/ilke_karatas.pdf)> accessed 6 February 2026.

<sup>13</sup> 'Algorithmic Negligence: Bayesian–Neumann Risk Mitigation in Content Liability' (2023) 8(2) *International Journal of Law Management & Humanities* <<https://ijlmh.com/publications/volume-viii-issue-ii/>> accessed 6 February 2026.

- **Prioritizing Speed Over Verification:** a user interface that does not require a declaration of package contents or a visual confirmation of the seal, purely to shave seconds off the booking process.
- **Ineffective Feedback Loops:** ignoring repeated reports from riders regarding suspicious odors (such as the pungent smell of marijuana) or suspicious behavior at pickup point

### **The NDPS Act and the Presumption of Culpability**

The Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985, is one of the most rigorous statutes in the Indian legal system. It was enacted to consolidate and amend the laws relating to narcotic drugs, to make stringent provisions for control and regulation, and to provide for the forfeiture of property derived from illicit traffic. Unlike ordinary criminal law, where the burden of proof rests squarely on the prosecution to prove the accuser's guilt beyond reasonable doubt, the NDPS Act under Sections 35 and 54 operates on a presumption of a "culpable mental state" and a "presumption of possession."<sup>14</sup> Once the prosecution establishes that the accused had physical possession of the contraband or controlled the premises or conveyance where it was found, the burden shifts to the accused to prove the absence of knowledge or intent.

For app-based logistics, Section 25 of the NDPS Act is the most potent tool available to law enforcement.<sup>15</sup> It prescribes punishment for any owner, occupier, or person having the control or use of any house, room, enclosure, space, place, animal, or conveyance who knowingly permits it to be used for the commission of an offense. While a platform like Uber or Porter does not own the vehicle used by a gig worker, it exercises near-absolute "control and use" over the digital coordination that brings the conveyance to the narcotics. If law enforcement can prove that a platform was aware of its services being used for trafficking perhaps through prior intelligence reports or a high volume of reported incidents and failed to implement preventive measures, the platform itself may be charged under Section 25.

Section 27A of the Act criminalizes the financing of illicit traffic and the harboring of offenders, carrying a mandatory minimum sentence of ten years and a maximum of twenty years, regardless of the quantity of drugs involved.<sup>16</sup> This section targets the organizers and "kingpins" of the drug trade. In the platform-liability context, if an app consistently profits from commissions on drug deliveries and provides a digital "harbor" for peddlers through

<sup>14</sup> Narcotic Drugs and Psychotropic Substances Act 1985, ss 35, 54.

<sup>15</sup> Narcotic Drugs and Psychotropic Substances Act 1985, s 25.

<sup>16</sup> Narcotic Drugs and Psychotropic Substances Act 1985, s 27A.

anonymity and unverified accounts, a legal argument can be constructed for indirect financing of illicit traffic.

The penalty structure under the NDPS Act, 1985, scales with both the substance and the quantity involved. For cannabis (ganja), punishment ranges from up to one year of rigorous imprisonment plus a fine for a small quantity, to up to ten years for an intermediate quantity, to ten to twenty years with a fine of ₹1-2 lakh for a commercial quantity. Cocaine and hydroponic marijuana carry an identical spectrum: up to one year for a small quantity, up to ten years for an intermediate quantity, and ten to twenty years with a ₹1-2 lakh fine for a commercial quantity. Financing or harboring under Section 27A carries a flat ten-to-twenty-year sentence with a ₹1–2 lakh fine regardless of quantity, since the offense is not quantity-graded. Allowing a conveyance to be used for trafficking under Section 25 is punished according to the underlying offense committed, at whatever quantity tier that offense falls into. A significant nuance involves the 2014 amendment to the NDPS Act. A drafting oversight re-lettered the catalogue of offenses from Section 2(viia) to Section 2(viib) to permit medical access to opioids such as morphine; the drafters, however, failed to update the corresponding reference in Section 27A, which continued to penalize the now-blank sub-clauses of 2(viia). In 2016 the Tripura High Court addressed this dissonance, holding that while the provision must be read in the spirit of the whole Act, criminal law cannot be amended retrospectively to the detriment of the accused.<sup>17</sup> This drafting error created a temporary window of legal uncertainty for those charged with financing, though most courts have since adopted a purposive interpretation to keep the provision operable.

### **Individual Liability of the Accused: Differentiating Culpability Within the App-Based Chain**

While platform-level liability under Section 79 and Section 25 has dominated recent scholarship, the more immediate and frequently litigated question in app-based trafficking cases is the liability of the individual accused—the person who is actually arrested, charged, and denied or granted bail. The NDPS Act does not treat all participants in a trafficking chain identically; rather, it calibrates culpability according to role, quantity of contraband, and the accused's proximity to knowledge of the offense. In the app-mediated ecosystem this chain typically comprises five distinguishable actors: the financier or kingpin who structures the

---

<sup>17</sup> Court on its Own Motion v Union of India Crl Ref No 1/2020, 4 June 2021 (Tripura HC) [11]–[14]; Constitution of India 1950, art 20(1).

operation; the local peddler or dispatcher who books deliveries and manages inventory; the gig-economy rider who physically transports the parcel; the receiving customer; and, occasionally, an intermediate “mule” whose bank account or identity is used to launder proceeds. Each occupies a materially different position under the Act’s presumptive and evidentiary framework.

### **The Reverse Burden: Sections 35 and 54**

Section 35 of the NDPS Act presumes the existence of a culpable mental state intention, knowledge, or a particular state of mind once the prosecution proves the foundational facts of the offense, and it is for the accused to prove the contrary beyond reasonable doubt. Section 54 goes further, presuming that the accused has committed the offense in respect of any narcotic drug or psychotropic substance for which he or she fails to satisfactorily account for possession. Together these provisions invert the ordinary criminal-law presumption of innocence for a discrete but consequential class of facts: once the prosecution shows possession or control, the accused bears the burden of displacing the presumption, typically by showing an absence of knowledge that the parcel contained a controlled substance.<sup>18</sup>

The Supreme Court upheld the constitutional validity of this reverse burden in *Noor Aga v State of Punjab* (2008), reasoning that a reverse onus clause is permissible provided the prosecution first establishes the “foundational facts” recovery, possession, and compliance with mandatory search and seizure procedure beyond reasonable doubt, and provided the accused is given a genuine and fair opportunity to rebut the presumption on the civil standard of preponderance of probability rather than the criminal standard.<sup>19</sup> This is the doctrinal hinge on which the liability of every app-based accused ultimately turns: the presumption operates only after the state has proved, procedurally and factually, that the accused was in conscious possession of the contraband.

### **Why Gig Workers Occupy a Structurally Weaker and Stronger Position**

For a delivery rider who unknowingly transported a parcel containing narcotics, Sections 35 and 54 create an immediate evidentiary difficulty: the mere physical possession of the package, even without knowledge of its contents, can trigger the presumption and place the rider in the position of having to prove a negative that he did not know what he was carrying. Indian courts

<sup>18</sup> Narcotic Drugs and Psychotropic Substances Act 1985, ss 35, 54.

<sup>19</sup> *Noor Aga v State of Punjab* (2008) 16 SCC 417 [58]–[60] (Sinha J).

have, however, increasingly recognized that “conscious possession” requires more than bare custody; it requires an element of knowledge and control over the contraband. Where a rider can show that the parcel was sealed, that the interface did not require or permit a declaration of contents, that his role was confined to point-to-point transport dictated entirely by the platform’s algorithm, and that he had no commercial stake beyond the delivery fee, courts have been willing to treat the presumption as rebutted at the bail stage and, in several instances, to discharge riders at the investigation or framing-of-charge stage. The Telangana Gig and Platform Workers’ Union has specifically petitioned for such riders to be treated as witnesses rather than accused where they self-report a suspicious parcel immediately upon discovery, a position that aligns with the “good faith” rebuttal contemplated by Noor Aga.

By contrast, the peddler or dispatcher who books the delivery, selects the concealment method, and communicates coordinates through encrypted channels is far less able to displace the presumption, because the very facts that establish possession—control over the packaging, the booking account, and the payment trail—also establish the knowledge element that Sections 35 and 54 presume. The financier or kingpin, in turn, is rarely found in physical possession at all, which historically made Section 27A the only viable charge against such individuals; but because Section 27A attaches a mandatory minimum of ten years regardless of quantity, once financing or harboring is established through financial records, call-detail records, or digital payment trails, the accused faces the most severe end of the NDPS penalty spectrum with comparatively little room for judicial discretion in sentencing.

### **Section 37 and the Bail Bar**

Beyond the reverse burden on guilt, Section 37 of the NDPS Act imposes an additional and largely independent hurdle at the bail stage for offenses involving commercial quantity. It requires the court to be satisfied, first, that there are reasonable grounds for believing the accused is not guilty of the offense, and second, that the accused is not likely to commit any offense while on bail—a conjunctive, twin-condition test that is considerably more demanding than the ordinary bail standard.<sup>20</sup> In several of the app-based cases discussed below, courts denied bail expressly on the ground that the use of a delivery platform to camouflage narcotics as legitimate e-commerce parcels demonstrated a level of planning and continuing risk that could not satisfy the second limb of Section 37. For an accused positioned as dispatcher or financier, the combination of the Section 35/54 presumption on merits and the Section 37 bail

---

<sup>20</sup> Narcotic Drugs and Psychotropic Substances Act 1985, s 37(1)(b)(ii).

bar means that pre-trial liberty is difficult to secure even where the trial itself may ultimately turn on rebuttable presumptions.

### **Tofan Singh and the Admissibility of Confessions**

A second major development bearing on individual liability is the Supreme Court's 2020 ruling in *Tofan Singh v State of Tamil Nadu*, which held that officers of the Narcotics Control Bureau and other authorities empowered under Section 53 of the NDPS Act are "police officers" for the purposes of Section 25 of the Indian Evidence Act, and that confessional statements recorded by them are therefore inadmissible as substantive evidence of guilt.<sup>21</sup> This ruling materially altered the liability calculus for accused persons across the trafficking chain, because a significant proportion of pre-Tofan Singh prosecutions, particularly against peddlers and mules, had relied heavily on statements recorded during NCB interrogation. Post-Tofan Singh, the prosecution must reconstruct its case for these actors from independent recovery evidence, digital records, call-detail records, and app-transaction logs sources of proof that are, in the app-based context, often more readily available than in conventional street-level trafficking, since every booking, payment, and delivery event leaves a time stamped, geolocated digital trail. Paradoxically, then, the same platform architecture that provides traffickers with operational cover also generates the forensic record that increasingly substitutes for the confessional evidence courts can no longer rely upon.

### **Procedural Safeguards: Sections 42 and 50**

The foundational facts that must precede any presumption under Sections 35 and 54 are themselves conditioned on strict compliance with the search and seizure procedure prescribed by Sections 42 and 50 of the Act. Section 42 requires an officer conducting a search without a warrant to record, in writing, the grounds of his belief and to forward that record to a superior officer within the prescribed time; Section 50 requires that a person about to be searched be informed of the right to be searched before a gazetted officer or a magistrate. The Supreme Court has repeatedly held, including in *State of Punjab v Baldev Singh*, that non-compliance with these provisions vitiates the trial and entitles the accused to acquittal irrespective of the presumption of possession, because the reverse burden can only operate once the underlying search was lawful.<sup>22</sup> In the app-based context, where recoveries frequently occur at transit

<sup>21</sup> *Tofan Singh v State of Tamil Nadu* (2021) 4 SCC 1 [159]–[160] (Nariman J); Indian Evidence Act 1872, s 25.

<sup>22</sup> *State of Punjab v Baldev Singh* (1999) 6 SCC 172 [57] (Pattanaik J).

points, delivery hubs, or during interception of a rider mid-delivery, procedural compliance is often the single most litigated issue at trial, and defense counsel routinely succeed in securing acquittals or bail on the ground that the search of a rider's vehicle or parcel did not conform to Section 50.

Liability differs sharply depending on where an individual sits in the app-based trafficking chain. The financier or kingpin typically faces a Section 27A charge for financing or harboring; the reverse presumption of possession is comparatively weak against this actor, since the case usually turns on proof via the financial trail, and the realistic defense posture is to contest that financial or harboring evidence directly, with the mandatory minimum sentence leaving little room for sentencing discretion. The local peddler or dispatcher is typically charged under Sections 8 and 21–23 and 29 for possession, sale, or conspiracy; here the reverse presumption is strong, since possession and knowledge are closely linked, and the defense realistically turns on rebutting knowledge on a preponderance standard or challenging compliance with Sections 42 and 50. The unwitting gig-economy rider, typically charged under Sections 8 and 21–23 for possession alone, faces a more contestable presumption, since possession here is not accompanied by proven knowledge, and the realistic defense rests on the absence of conscious possession, the algorithmic nature of the assignment, and immediate self-reporting where it occurred. The mule account holder, typically charged under Section 27A with a possible PMLA overlap, faces a moderate presumption that depends on proof of knowing participation, with identity theft or forged KYC and a genuine lack of knowledge of the underlying trade as the realistic defense. The end consumer, charged under Section 27 for consumption or simple possession for personal use, faces only a weak presumption in personal-quantity cases, and can typically rely on the small-quantity threshold and the possibility of rehabilitation in lieu of prosecution under Section 64A.

This differentiated map matters for both litigation strategy and policy design. A regulatory response that focuses exclusively on platform-level intermediary liability risks leaving the rider the most vulnerable and least culpable actor in the chain to bear the practical brunt of NDPS enforcement, simply because the rider is the person physically present at the point of interception. Conversely, a response that is too solicitous of riders risks under-punishing dispatchers who deliberately exploit the gig-economy interface's lack of content-declaration requirements. The doctrinally sound position, consistent with Noor Aga and the post-Tofan Singh evidentiary landscape, is to preserve the presumption as a tool against those with proven proximity to knowledge and control, while developing structured evidentiary thresholds of the kind proposed in the policy section below that allow courts to distinguish an unwitting mule

from a knowing participant at the earliest possible stage, ideally at the bail hearing rather than only after a full trial.

### **Case Studies in App-Based Marijuana Trafficking**

The Narcotics Control Bureau (NCB) and state police departments have documented a surge in cases where hyper local apps were used as the primary logistical layer for drug distribution. These cases reveal a highly organized modus operandi designed to exploit the “blind spots” of the gig economy, and each also illustrates the differentiated liability analysis set out above.

#### **The Noida NCR Syndicate: Deceptive Branding and Driver Diversion**

In November 2025, the Noida Sector-113 Police busted a major trafficking ring that utilized the Porter app to ship marijuana throughout the National Capital Region.<sup>23</sup> The gang, led by Yogendra Pratap Singh, sourced high-grade cannabis from Odisha, Andhra Pradesh, and Nepal. Their modus operandi involved three distinct layers of evasion. First, they targeted customers near colleges and corporate offices through offline scouting. Second, transactions and delivery coordinates were handled entirely through encrypted messaging and digital payment apps like PayTM. Third, the contraband was meticulously packaged to mimic legitimate shipments from Amazon or Flipkart, complete with branded boxes and logos. The use of a Porter rider ensured that if the delivery was intercepted, the driver would be the first point of investigation, providing the actual suppliers with a crucial window to escape and destroy evidence — a structural feature that, on the liability analysis above, deliberately positions the least culpable actor as the most exposed to arrest.

#### **Bangalore: The Essential Services Camouflage**

In Bangalore, the NCB unearthed a syndicate that leveraged the “essential services” status of delivery personnel during and after the pandemic. Seven individuals were arrested for using partners from Swiggy and Dunzo to deliver ganja in small packets of 10–50 grams to doorsteps.<sup>24</sup> The traffickers did not merely book riders but actively masqueraded as delivery personnel by wearing fake uniforms and carrying branded delivery boxes, moving 136 kg of

<sup>23</sup> Hindustan Times, “‘Ganja Home Delivery’: How Gang Busted in Noida Used Apps to Ship Its ‘Stuff’” Hindustan Times (New Delhi, 2025) <<https://www.hindustantimes.com/india-news/ganja-home-delivery-how-gang-busted-in-noida-used-apps-to-ship-its-stuff-101764498881540.html>> accessed 6 February 2026.

<sup>24</sup> The Hindu, ‘NCB Unearths Drug Racket That Provided Doorstep Delivery Using App Partners’ The Hindu (Bangalore) <<https://www.thehindu.com/news/cities/bangalore/ncb-unearths-drug-racket-that-provided-doorstep-delivery-using-app-partners/article36800268.ece>> accessed 6 February 2026.

ganja through the city with minimal police scrutiny. The High Court eventually denied bail to the accused, emphasizing that the use of online platforms and service providers for drug distribution constituted a serious offense; the denial turned squarely on the Section 37 twin-condition test, the court finding that the organized and repeated use of platform camouflage indicated an ongoing risk that satisfied the second limb of the bail bar.

### **Chennai: The Student Micro-Cell Network**

Greater Chennai Police have reported an alarming trend where 19-to-23-year-olds with clean police records use aggregator apps like Porter, Zepto, and Uber Courier to deliver illegal drugs to educational institutions.<sup>25</sup> This “student-run” model is particularly difficult to prosecute because it operates through decentralized micro-cells: one student handles the dark-web order and crypto currency payment, another receives the package via a third-party app, and a third manages redistribution. The use of common household items such as shampoo bottles or electronic devices for concealment means that delivery partners, often rushing to meet time targets, do not inspect the packages so long as they remain within weight limits. The compartmentalized structure of this network is itself a defense strategy: because no single micro-cell member has full knowledge of the chain, each can plausibly invoke the absence of a culpable mental state under Section 35, forcing the prosecution to rely more heavily on digital and financial trails than on any single individual’s admitted knowledge.

### **Transnational Hydroponic Routes: Thailand to Delhi**

The legalization of cannabis in Thailand has significantly impacted the Indian drug market. In October 2025, Delhi Police arrested a former Central Board of Indirect Taxes and Customs (CBIC) officer for smuggling 21 kg of “ocean-grown” hydroponic marijuana worth ₹27 crore from Thailand, laundered through hawala and cryptocurrency channels. Given the quantity involved, this case sits squarely at the commercial-quantity end of the penalty spectrum, and the accused’s prior position as a customs officer will likely be treated by courts as an aggravating factor bearing on both the Section 37 bail assessment and eventual sentencing, since it demonstrates specialized knowledge of exactly the interdiction points the syndicate

---

<sup>25</sup> Times of India, ‘Chennai Students Using Courier Apps for Drug Trafficking: A Growing Concern’ Times of India (Chennai, 2025) <<https://timesofindia.indiatimes.com/city/chennai/chennai-students-using-courier-apps-for-drug-trafficking-a-growing-concern/articleshow/123368923.cms>> accessed 6 February 2026.

sought to evade.<sup>26</sup> The syndicate used low-footfall airports such as Guwahati and domestic courier routes to move the contraband to Delhi. Once in the capital, the final leg of distribution was often handled via app-based delivery services to affluent users and party circles, with payments.

### Technical Vulnerabilities: The KYC and Verification Vacuum

The primary reason for the proliferation of app-based trafficking is the lack of robust Know Your Customer (KYC) and package-verification protocols within the gig economy. While the banking and financial services sector in India is subject to the stringent Master Direction on KYC (2016) and the Prevention of Money Laundering Act (PMLA), 2002, non-regulated entities like delivery apps prioritize speed and user experience over verification.<sup>27</sup>

In India, the threshold for identifying “beneficial ownership” has been lowered to 10 percent, requiring banks to perform thorough due diligence on all transactions. Conversely, a delivery-app user can often book a “package pickup” with just a mobile number and a digital wallet. This allows traffickers to use “mule accounts” bank accounts opened with stolen or forged identity documents to pay for delivery services and receive drug proceeds. In one operation by the “EAGLE” force in Telangana, investigators uncovered 59 mule accounts used by a Nigerian-led syndicate, with top accounts showing suspect transactions of nearly ₹7.9 crore.<sup>28</sup> For the mule-account holder, individual liability turns almost entirely on whether the prosecution can show knowing participation rather than mere identity theft; where the account was opened using forged documents without the named holder’s knowledge, that holder is properly a victim rather than an accused, and the evidentiary burden to establish otherwise rests with the prosecution notwithstanding the general reverse-burden architecture of the Act.

The Telangana Gig and Platform Workers’ Union (TGPWU) has raised concerns that the current model turns delivery workers into “unwilling drug mules.”<sup>29</sup> Without the right to inspect package contents or the infrastructure to verify the identity of the sender at the point of

<sup>26</sup> The Hindu, ‘Former CBIC Officer Held with ₹27 Crore “Hydroponic Marijuana”, Drug Cartel Busted: Police’ The Hindu (New Delhi, 2025) <<https://www.thehindu.com/news/cities/Delhi/former-cbic-officer-held-with-27-crore-hydroponic-marijuana-drug-cartel-busted-police/article70216579.ece>> accessed 6 February 2026.

<sup>27</sup> Reserve Bank of India, Master Direction — Know Your Customer (KYC) Directions 2016 (RBI, as amended) <<https://centralbankofindia.co.in/sites/default/files/2025-04/FINAL-KYCAML-Policy-2025-26-upto-06.11.2024.pdf>> accessed 6 February 2026; Prevention of Money Laundering Act 2002, s 12.

<sup>28</sup> The Hindu, ‘Major Multi-State Raids Disrupt Nationwide Drug Cartel Network Run by Nigerian Handlers in India’ The Hindu (2025) <<https://www.thehindu.com/news/national/telangana/major-multi-state-raids-disrupt-nationwide-drug-cartel-network-run-by-nigerian-handlers/article70334055.ece>> accessed 6 February 2026.

<sup>29</sup> The Hans India, ‘Using Courier Apps for Drug Trafficking a Growing Concern’ The Hans India (Hyderabad) <<https://www.thehansindia.com/telangana/using-courier-apps-for-drug-trafficking-a-growing-concern-1002515>> accessed 6 February 2026.

pickup, riders remain legally vulnerable notwithstanding the doctrinal arguments available to them at trial. The Hyderabad City Police have issued directives to app aggregators to record the sender's name and details more rigorously and to implement a declaration system for the contents of the parcel.

### **Algorithmic Matching as a Facilitation Tool**

The “black box” algorithms used by apps like Uber and Porter are designed to maximize efficiency through a process of “automated matching.” From a legal perspective, however, this matching process may disqualify a platform from safe harbor. Section 79(2)(b) specifically requires that the intermediary not “select the receiver of the transmission.”<sup>30</sup> In a logistics context, the “transmission” is the physical package, and the “receiver” is the rider. By using AI to determine which specific rider receives a booking request, the platform is arguably making a selection that voids its conduit status.

Furthermore, the real-time tracking feature of these apps provides traffickers with tactical information. If a delivery rider is delayed at a checkpoint, the sender and receiver can immediately see the disruption on the app and abort the transaction. This “tactical visibility” is a design feature that enhances user experience for legitimate customers but serves as an early-warning system for criminals. Legal scholars argue that the failure to implement “safety filters” for these high-visibility features, especially when they involve peer-to-peer delivery to high-risk zones, constitutes a breach of the duty of care, and also complicates the individual rider's defense, since prosecutors may argue that a rider who observed and did not report such a real-time abort pattern possessed at least constructive knowledge of the illicit nature of the transaction.

### **Policy Implications and Necessary Reforms**

Dismantling the app-based drug trafficking ecosystem requires a multi-pronged regulatory and technical response that addresses both platform-level immunity and the fairness of individual liability determinations. The current “one-size-fits-all” approach to intermediary immunity, and the corresponding absence of any structured mechanism for distinguishing among accused persons at the investigation stage, are both no longer sustainable.

---

<sup>30</sup> Information Technology Act 2000, s 79(2)(b).

### **Tiered Liability and KYBC Norms**

Legislators must recognize that a delivery app facilitating physical movement is fundamentally different from a social media app hosting a post. Legal experts propose a “tiered liability model” in which intermediaries are categorized based on their level of control over the transaction. Platforms that handle logistics, pricing, and payments should be subject to “Know Your Business Customer” (KYBC) norms, requiring commercial-grade identity verification for all senders.

### **Algorithmic Transparency and Reporting**

To combat algorithmic negligence, platforms must be required to disclose the risk parameters used by their safety algorithms to the NCB or local police. Furthermore, an “integrated reporting mechanism” should be established, linking delivery apps to the NCB’s “Manas” or “Sahyog” portals, allowing for the real-time flagging of suspicious booking patterns, such as multiple deliveries between a suspected darknet drop-point and university hostels.

### **Re-Evaluating the “Burden of Judgment”**

The Shreya Singhal requirement of a court order for “actual knowledge” must be modified for physical logistics, allowing them to report suspicious packages without fear of retaliation from the user or the platform. Platforms that receive repeated warnings from riders regarding a specific user account but fail to suspend that account should be held to a standard of “constructive knowledge” and should lose their immunity.<sup>31</sup> A “good faith” reporting system for delivery workers should be legally

### **A Statutory Presumption-Calibration Framework for the Accused**

Beyond platform reform, this paper argues that the NDPS framework itself would benefit from a codified set of evidentiary thresholds, applicable specifically to app-mediated deliveries, that calibrate how readily the Section 35/54 presumptions operate depending on the accused’s role. Concretely, this would involve: first, a rebuttable statutory inference that a gig-economy rider who immediately reports a suspicious parcel to the platform and to law enforcement is treated as a witness rather than an accused, formalizing the protection the TGPWU has sought administratively; second, a requirement that prosecutors seeking to rely on the presumption against a rider first demonstrate that the app’s interface permitted or required content

---

<sup>31</sup> Shreya Singhal v Union of India (2015) 5 SCC 1 [117]–[119] (Nariman J).

declaration, so that the presumption is not stretched to cover situations the platform's own design made detection impossible; and third, an explicit direction to trial courts that, post-Tofan Singh, digital transaction logs, geolocation data, and payment trails rather than any confessional statement recorded by NCB or police officers constitute the primary evidentiary foundation for establishing knowledge against dispatchers and financiers. Such a framework would preserve the deterrent force of the reverse burden against those genuinely embedded in the trafficking chain while reducing the risk that the Act's stringent presumptions fall disproportionately on the least culpable participants simply because they are the easiest to physically intercept.

### **Strengthening Gig Worker Protections**

The Telangana Gig and Platform Workers' Union has highlighted the lack of protection for drivers who discover narcotics. Law enforcement must establish clear standard operating procedures for "unwilling drug mules." If a rider discovers contraband, that rider should be treated as a witness rather than an accused, provided immediate reporting protocols are followed.

### **Conclusion: Toward a New Digital Accountability**

The intersection of India's gig economy and its drug-trafficking ecosystem has exposed the fragility of the current digital legal architecture on two distinct but related fronts. At the platform level, the safe harbor provision of Section 79, while essential for the early growth of the internet, has become a shield for "willful blindness" in the multi-billion-dollar logistics sector. At the level of the individual accused, the reverse-burden architecture of Sections 35, 37, and 54 designed for a world of street-level, hand-to-hand trafficking now operates within an app-mediated environment whose entire design compartmentalizes knowledge and diffuses culpability across financiers, dispatchers, riders, and mules who rarely share a common intent or awareness.

Deconstructing this crisis requires moving away from the binary logic of "conduit" versus "publisher" at the platform level, and equally away from a flattened, undifferentiated view of "the accused" at the individual level. The theory of algorithmic negligence provides a framework for holding platforms accountable for the physical consequences of their digital designs; the doctrine of graduated presumption, developed through Noor Aga, Baldev Singh, and Tofan Singh, provides the analogous framework for holding individuals accountable in

proportion to their actual proximity to knowledge and control. When an algorithm is designed to ignore the risk of narcotics movement in favor of speed and commission, the platform transitions from a neutral intermediary to an active, albeit automated, facilitator of illicit traffic and the individuals it recruits as unwitting couriers deserve a liability framework calibrated to that same reality, rather than one built for a pre-digital trafficking model that no longer describes how these networks actually operate.

The future of digital regulation in India, likely under the forthcoming Digital India Bill, must therefore pursue two reforms in tandem: strengthening KYC and algorithmic transparency obligations for gig-economy participants at the platform level, and codifying a role-sensitive presumption-calibration framework for individual accused persons at the enforcement level. Strengthening one without the other risks either leaving platforms structurally incentivized toward willful blindness, or leaving the most vulnerable and least culpable actors in the chain the delivery riders to absorb the practical weight of a statute designed for kingpins. The age of unconditional safe harbor is over, and the age of undifferentiated liability for the accused should be next.

