WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

Journal homepage: www.ijrpr.com ISSN 2582-7421

# Cyber-Facilitated Drug Trafficking and Legal Challenges under Indian Law

***Mumtaj[1], Dr. Radhika Dev Varma[2]***

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India.
[2]Professor, University Institute of Legal Studies, Chandigarh University, Mohali, Punjab, India

**Abstract**

The rapid spread of platform-based narcotics trade in India through darknet markets, encrypted social media channels and cryptocurrency payments has created a layered criminal economy that connects offshore vendors, Indian retail peddlers and youthful consumer cohorts in a manner that blurs conventional territorial lines. Press releases of the Narcotics Control Bureau in 2025 on Operation MELON, the takedown of the darknet vendor "Ketamelon" and interceptions of postal parcels show that traffickers are using Tor-based marketplaces, anonymous wallets and postal-courier drops to push LSD, MDMA, ketamine and designer pills into metropolitan and tier-two urban centres, while retaining command-and-control offshore or through hardened laptops running privacy operating systems.[1] The statutory frame that responds to this activity is still led by the "Narcotic Drugs and Psychotropic Substances Act, 1985" with its stringent offence design in "Sections 8, 20 to 29 and 37", but the enabling rails of the offence often fall outside NDPS and lie in the "Information Technology Act, 2000" and the "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021", which demand traceability, expedited takedown and preservation of traffic data from intermediaries, subject to ongoing constitutional contest around rule 4(2).[2] Crypto-financed trafficking further activates the "Prevention of Money Laundering Act, 2002" after the 7 March 2023 notification that made virtual digital asset service providers reporting entities under "Section 2(1)(wa)" read with accompanying obligations to register with FIU-IND, complete KYC and file suspicious transaction reports, creating a bridge between narcotics seizures and financial dissection of blockchain trails.[3] Admissibility of electronic proof is now governed by "Section 63 of the Bharatiya Sakshya Adhiniyam, 2023", which requires a structured certificate, device particulars and trusted hash values for chats, device images, e-mail headers or blockchain exports to be read in evidence, making cyber-narcotics probes document heavy and process dependent.[4] Enforcement experience shows that postal seizures or darknet arrests collapse in court when the certificate is absent or defective, or when the NDPS search safeguards framed for physical body search are mechanically applied to electronic contexts without adapting to online tip-offs, courier interceptions or controlled deliveries in digital form. Investigative trends, parliamentary answers in 2025 citing 1.09 lakh kg of seizures between 2020 and May 2025, and advisory material issued to upgrade cyber forensics reflect a state effort to move from seizure-led to network-led disruption of supply chains.[5] A reform path therefore needs to recalibrate NDPS procedure for digital-first operations, tighten intermediary liability without defeating privacy guarantees, link PMLA crypto compliance to narcotics FIRs through standard operating procedures, and harmonise "Section 63 BSA" with BNSS provisions on audio-video recorded search, so that electronic trails captured from darknet vendors, platform administrators and VDA wallets become courtroom proof and not investigative dead weight.

**Keywords:** NDPS Act; darknet; encrypted messaging; postal interdiction; cryptocurrency; PMLA; FIU-IND; IT Rules 2021; Rule 4(2) traceability; CERT-In directions.

## Introduction

Online marketplaces, encrypted messaging services and on-demand delivery systems have changed the topography of narcotics trafficking in India by allowing supply, payment and delivery to be separated in time, space and jurisdiction. Vendors operate from foreign or concealed locations on Tor or other anonymising networks, advertise LSD blotters, MDMA crystals, ketamine vials or high-grade cannabis in Indian rupees, but collect funds through cryptocurrency channels that are either mixed, privacy-enhanced or pushed through local P2P trades, after which delivery is arranged through national

[1] Press Release, *available at:* https://narcoticsindia.nic.in/pressrelease.php (last visited on November 3, 2025).
[2] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 6.4.2023], *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on November 2, 2025).
[3] Registration of Virtual Digital Asset Service Providers in FIU India as Reporting Entity-Reg., *available at:* https://fiuindia.gov.in/pdfs/downloads/VDASP04072023.pdf (last visited on November 1, 2025).
[4] The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 31, 2025).
[5] Lok Sabha Unstarred Question No. 4988: Steps to Check Drug Trafficking, *available at:* https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS01042025/4988.pdf (last visited on October 30, 2025).

postal systems or private courier franchises.[6] NCB communiqués from July 2025, followed by Parliament replies in early 2025, record interceptions of cocaine, LSD and psychotropics routed through foreign post offices, drop-off systems and dead-drop coordinates shared over encrypted apps, which shows that a substantial part of the retail narcotics market is now supported by digital communications and is not confined to traditional peddler networks.[7] This pattern challenges the controlling statute because the NDPS Act was drafted in 1985 with a clear focus on possession, transport and warehousing in the physical world, a presumption regime based on seizure and a bail standard in "Section 37" that hinges on recovery, quantity and reasonable grounds. When the contraband is never physically handled by the online controller, or when seizure is from a courier hub based on digital intelligence, the conventional evidentiary spine weakens, yet the punishment bands and bail restrictions stay in place and produce contested litigation. The problem deepens when encrypted platforms such as Telegram or WhatsApp are used, since service providers often sit outside India and claim inability to decrypt or identify the first originator, while Indian rules through "Rule 4(2) of the IT Rules, 2021" insist on traceability for serious offences and court-ordered disclosures. At the same time, the criminal procedure environment has itself changed because "Bharatiya Nagarik Suraksha Sanhita, 2023" now demands audio-video recording of search and seizure under "Section 105", and recognises cross-border electronic materials, which means NDPS field units have to reconcile special NDPS mandates in "Sections 42, 43 and 50" with the broader digital-friendly recordkeeping standard in the BNSS.[8] This legal research study therefore proceeds on the understanding that cyber-facilitated drug trafficking is not a separate offence cluster but a mode that sits at the intersection of NDPS, IT law, digital evidence law, money laundering law and data protection law, and that any doctrinal assessment must take into account parallel moves such as the "Digital Personal Data Protection Act, 2023" that allows processing of personal data for prevention, detection and investigation of offences in "Section 17", which can justify data sharing and decryption actions taken for narcotics cases.[9]

## Research Questions

The research questions of this study arise from the friction between technology enabled narcotics operations and the current shape of Indian criminal and data regimes. The first enquiry asks whether the combined text of the "NDPS Act, 1985", the "IT Act, 2000" with the 2021 Rules, the "BNSS, 2023", the "BSA, 2023" and the "DPDP Act, 2023" offers a coherent response to darknet markets, encrypted social media channels, courier-based deliveries and cryptocurrency-fuelled payments that are now visible in NCB seizures from 2023 to 2025.[10] The second enquiry tests whether the evidentiary standard for electronic records in "Section 63 BSA" and the search safeguards in "Sections 42, 43 and 50 NDPS Act" match the practical realities of cyber investigations where data is volatile, often stored abroad and sometimes captured without full device imaging, which later affects admissibility and bail.

## Problem Statement

NDPS procedure and rules of proof were designed for body search, house raid or vehicle intercept where contraband could be produced, weighed and sampled on site. Online drug trade profits from anonymity layers, foreign servers, non-custodial crypto wallets and courier drops, so officers often secure only chats or blockchain traces without immediate seizure. This mismatch produces disputes on compliance with "Sections 42, 50 and 52A NDPS Act", on the sufficiency of "Section 63 BSA" certificates, and on the very basis for applying the stringent "Section 37" bail bar when recovery is digital or derivative.

## Objectives of the Study

The study aims to map the live Indian legal framework that touches cyber-facilitated drug trafficking, capturing not only NDPS but also platform-governance rules, digital evidence mandates and financial intelligence duties triggered by crypto transactions. This mapping will then be used to show the points at which doctrine framed for physical contraband is burdening digital-first operations, especially in relation to courier seizures, postal monitoring and darknet vendor takedowns such as those recorded in Operation MELON. A further objective is to suggest integrated standards for preserving and certifying electronic records, for imposing time-bound cooperation on intermediaries under "Rule 3 and Rule 4 of the IT Rules, 2021", and for linking PMLA obligations of VDA entities back to NDPS investigations, so that parallel financial probes can be initiated early and assets linked to narcotics sales can be frozen or attached.

## Research Methodology

This study follows a doctrinal method by reading the text of the "NDPS Act, 1985", the "IT Act, 2000" and its 2021 Rules, the "Bharatiya Sakshya Adhiniyam, 2023", the "Bharatiya Nyaya Sanhita, 2023", the "Bharatiya Nagarik Suraksha Sanhita, 2023", the "DPDP Act, 2023", and the March 7,

[6] J. N. Barowalia & Abhishek Barowalia, *Commentary on the Narcotic Drugs and Psychotropic Substances Act* 168 (LexisNexis, New Delhi, 2nd edn., 2023).

[7] Dwaipayan Ghosh, "NCB Nabs 2 With Cocaine From Kenya", *available at:* https://timesofindia.indiatimes.com/city/kolkata/ncb-nabs-2-with-cocaine-from-kenya/articleshow/122580168.cms (last visited on October 29, 2025).

[8] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 28, 2025).

[9] The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 27, 2025).

[10] Spread of Illicit Drugs Through Dark Web, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/177/AU3691.pdf?source=pqals (last visited on October 26, 2025).

2023 PMLA notification on virtual digital assets, and placing them against NCB press material, Lok Sabha answers from 2025 and public advisories on cyber forensics, in order to produce a coherent legal reading of cyber-facilitated narcotics cases.[11]

## Statutory and Regulatory Framework

The Indian legal frame that engages cyber-facilitated drug trafficking is multilayered and rests on four pillars. The first pillar is the special criminal law in the "NDPS Act, 1985" which creates strict offences for production, possession, sale, purchase, transport, import inter-State, export inter-State, use and financing of narcotic drugs or psychotropic substances in "Sections 8, 20 to 29", imposes harsh minimums, and makes bail conditional and restrictive in "Section 37." The second pillar is procedure, now shared between the NDPS Act's own machinery provisions and the "Bharatiya Nagarik Suraksha Sanhita, 2023" which governs search, seizure, arrest, remand and recording of proceedings, including the new requirement of audio-video documentation in "Section 105 BNSS", which can secure the chain of custody when electronic devices or courier parcels are opened during search. The third pillar is cyber regulation under the "IT Act, 2000" and the 2021 Rules notified by MeitY which create a graded due-diligence architecture for intermediaries, insist on appointment of nodal officers and require significant social media intermediaries to enable identification of the first originator for serious offences, a clause that has direct relevance when a drug sale channel on Telegram or a broadcast group on WhatsApp is used to coordinate deliveries. The fourth pillar is financial surveillance through the "Prevention of Money Laundering Act, 2002" which, after the 2023 notification, brings virtual digital asset service providers, wallet custodians, exchanges and administrators into the reporting entity net, forcing them to identify Indian users, monitor wallet movements and provide data to FIU-IND, a model that can be directly applied to darknet vendors whose sales are settled in BTC, USDT or Monero through Indian-facing platforms. A supporting layer is the "Digital Personal Data Protection Act, 2023" which, by allowing processing of personal data for prevention, detection, investigation and prosecution of offences under "Section 17(2)(a)", gives legal cover to requests by NCB or state STF units to messaging platforms or VDA entities for subscriber and transactional data in narcotics probes.[12]

### *NDPS Act, 1985*

The NDPS Act criminalises every stage of narcotics commerce and therefore catches cyber-mediated conduct without needing new offence clauses. "Section 8" prohibits production, manufacture, possession, sale, purchase, transport, warehouse, use, consumption, import inter-State and export inter-State of narcotic drugs or psychotropic substances except for medical or scientific purposes and in the manner provided by the Act. "Sections 20, 21, 22, 23 and 24" fix punishment for cannabis, manufactured drugs, psychotropic substances, import-export offences and external dealings, while "Section 25" covers owners or occupiers who knowingly permit premises to be used for such activities, a provision that can be applied to co-working spaces or rented flats where darknet operators run TAILS-powered laptops. "Sections 27A and 29" deal with financing illicit traffic and abetment or criminal conspiracy, which means a person who hosts a mirror of a darknet market, encashes crypto for the main vendor or runs a consignee-address network for postal deliveries can be charged, even if physical possession is absent. Quantity thresholds and the mixture rule acquire enormous importance in online cases because LSD or MDMA ordered on the darknet is often in micro quantities per blot or pill but the total parcel may run into commercial quantity, triggering the embargo in "Section 37." After the Supreme Court decision in "*Hira Singh v. Union of India*[13] adjudication treats the entire mixture including neutral substances as the basis for determining small, intermediate or commercial quantity, which means that even granulated or diluted consignments intercepted by the foreign post office can place the accused in the non-bailable category. Table 1: NDPS provisions engaged in cyber-facilitated trafficking would therefore list "Sections 8, 20 to 24, 25, 27A, 29, 37, 53A (statements) and 68A to 68F (forfeiture)" as the core provisions that enforcement relies on when the acts are committed through digital means or culminate in courier-based deliveries.[14]

### *Procedural Safeguards under NDPS*

Procedure under the NDPS Act remains rigorous and continues to be a frequent ground for defence challenge in cyber cases. "Section 42" demands prior information to be taken down in writing and conveyed to superior officers when search is in a building, conveyance or enclosed place, while "Section 43" relaxes this for public places, which is relevant when a postal parcel is intercepted at a foreign post office or a courier hub because such facilities are generally treated as public areas, allowing immediate search. "Section 50" gives the person to be searched the option of being taken before a Gazetted Officer or Magistrate, and courts have repeatedly stated that this safeguard is confined to personal search, not to baggage or vehicle search, which means that in cyber cases where the contraband is in a courier envelope or in a serviceable parcel, strict "Section 50" compliance may not be insisted upon. "Section 52A" read with Standing Orders on sampling, sealing and disposal of seized narcotic drugs becomes extremely significant when seizures arise from digital tip-offs and are done in small postal packets, since prosecuting agencies must still draw representative samples, prepare a panchnama, record hash values if the packet is digitally imaged and prove an unbroken chain of custody. Postal or courier seizures based on darknet intelligence are often preceded by online surveillance, test purchases or controlled deliveries, so officers need to also respect the BNSS 2023 preference for audio-video recorded searches in "Section 105" and record such operations to preserve authenticity for later "Section 63 BSA" certificates. In many courier-based

[11] Notification S.O. 1072(E) Under the Prevention of Money-Laundering Act, 2002, *available at:* https://egazette.gov.in/WriteReadData/2023/244184.pdf (last visited on October 25, 2025).
[12] Stephen Mason & Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* 151 (Institute of Advanced Legal Studies, London, 5th edn., 2021).
[13] (2020) 20 SCC 272.
[14] Eric Jardine, "Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention", 46 *American Journal of Criminal Justice* 980 (2021).

cases, courts scrutinise whether the addressee had conscious possession, which makes it essential to match the packet with electronic communications, IP logs from the platform and crypto transaction records.[15]

***Intermediary Due Diligence under IT Act and Rules, 2021***

Digital drug markets cannot run without intermediaries, so the 2021 Rules become the connective tissue of enforcement. "Rule 3" obligates every intermediary to publish rules and regulations, privacy policy and user agreement and to remove unlawful content on receiving actual knowledge or on being notified by government agencies. For NDPS purposes, a channel that advertises LSD or offers delivery coordinates can be directed to be taken down, and non-compliance can expose the intermediary to loss of safe harbour under "Section 79 of the IT Act, 2000." "Rule 4(2)" goes a step further for significant social media intermediaries by requiring them to identify the first originator of a message related to offences involving the sovereignty or security of India, public order or rape and child sexual abuse, and the Union government has in several contexts argued that narcotics-related channels that fuel organised crime and cross-border terror financing fall within these serious categories, which would permit a traceability order. This clause is under constitutional challenge for allegedly infringing privacy and weakening end-to-end encryption, yet as long as it stays on the rulebook, narcotics investigators can approach platforms for originator information, subscriber details, IP logs and content preservation, subject to the DPDP Act's later framework on lawful processing. Table 2: Platform obligations relevant to NDPS investigations would identify content takedown, data retention for 180 days, naming of a grievance officer, appointment of a nodal contact person, disclosure of first originator, voluntary verification of users and deployment of automated tools to detect harmful content as the key hooks that agencies can rely on.[16] The point for doctrinal debate is whether non-compliance by an intermediary should in itself affect culpability of the individual trafficker, or whether it should only lead to regulatory action against the platform, a question that will gain weight when darknet vendors use mainstream platforms only for lead generation before moving to Tor.

***Electronic Evidence under Bharatiya Sakshya Adhiniyam, 2023***

The replacement of the Evidence Act, 1872 by the "Bharatiya Sakshya Adhiniyam, 2023" has direct impact on cyber-narcotics cases. "Section 63" of the BSA now governs admissibility of electronic records and demands a certificate that identifies the electronic record, describes the manner of production, provides device particulars, states that the computer or device was operating properly and includes a hash value or other technological means to establish integrity. The schedule-based format released by the Ministry of Home Affairs includes fields for messaging apps, email, CCTV, mobile phones and even blockchain outputs, which means that an investigator downloading darknet chat logs, Telegram order confirmations or crypto wallet CSV files has to secure a certificate either from the platform, from the officer who copied the data or from a notified cyber forensics laboratory.[17] In practice this creates friction because platforms abroad may not furnish certificates in the Indian format or may provide only a business record, which later leads to defence objections that the certificate is defective, that the person signing it did not have lawful control over the device, or that the hash does not match the exhibit produced in court. The BSA also interacts with BNSS 2023 because "Section 105 BNSS" expects search and seizure to be recorded in audio-video form, which can serve as foundational evidence showing that the device was sealed and that the data later produced under "Section 63" came from that device. For narcotics cases, this rigour is welcome because NDPS carries reverse burdens and severe sentences, so courts will demand strict authenticity of chat transcripts before inferring conspiracy or financing under "Sections 27A or 29 NDPS Act."

***Financial Trails and PMLA Coverage of Vdas***

Crypto payments have shifted narcotics profits away from cash couriers to wallets and P2P trades, which is why the March 7, 2023 notification under the PMLA is so significant. The notification brought under the PMLA umbrella entities that are involved in exchange between virtual digital assets and fiat currencies, exchange between one or more forms of virtual digital assets, transfer of virtual digital assets, safekeeping or administration of virtual digital assets and participation in financial services related to an issuer's offer and sale of a virtual digital asset. These entities must register with FIU-IND, maintain Know Your Customer records, conduct enhanced due diligence, file Suspicious Transaction Reports and make records available to enforcement agencies, a set of duties that mirrors those imposed on banks, money changers and payment system operators. When a darknet vendor is unmasked, investigators can now write to the Indian VDA exchange used for off-ramping to identify the account holder, freeze the wallet, secure IP and device fingerprints and even reconstruct the flow of funds across multiple tokens. FIU-IND in 2025 has also issued compliance actions against offshore VASPs offering services to Indian residents without registration, which gives teeth to requests arising from NDPS investigations. Table 3: Crypto compliance touchpoints for NDPS cases would map the stages at which narcotics information should be pushed into the AML system, starting from the NDPS FIR, to production of blockchain export, to requisition to the VDA exchange, to STR filing, to provisional attachment under "Sections 5 and 17 of the PMLA." When read with "Section 111 of the Bharatiya Nyaya Sanhita, 2023" on organised crime, this financial frame allows the state to target not just the courier who receives the parcel but the upstream international crypto-network behind the sale.[18]

---

[15] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* 212 (Academic Press, Waltham, MA, 3rd edn., 2011).

[16] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *available at:* https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (last visited on November 3, 2025).

[17] Ambu Raja, "Certificate Under 63(4) of Bharatiya Sakshya Adhiniyam", *available at:* https://www.scribd.com/document/837411615/Certificate-Under-63-4-of-BHARATIYA-SAKSHYA-ADHINIYAM (last visited on November 2, 2025).

[18] The Bharatiya Nyaya Sanhita, 2023, *available at:* https://prsindia.org/billtrack/the-bharatiya-nyaya-sanhita-2023 (last visited on November 1, 2025).

***Modus Operandi in Cyber-Facilitated Drug Trafficking***

Cyber-facilitated narcotics trafficking in India generally follows a modular path that starts with a darknet marketplace hosted on Tor or I2P, progresses through customer engagement on mainstream or encrypted platforms, moves value through cryptocurrency channels and ends with courier, postal or dead-drop delivery. Indian law enforcement has reported an increase in the use of vendor rating systems and escrow accounts on darknet markets, where buyers place orders for LSD or MDMA, make payment in BTC or stablecoins, and receive tracking numbers for parcels that originate from third countries or from Indian re-shippers, thereby reducing the exposure of the main vendor. Many of these vendors use privacy operating systems like TAILS, bridge connections and VPN chains to escape IP-based detection, while storing credentials and PGP keys in encrypted containers, which makes on-site seizure and forensic imaging very important. In several 2025 seizures, investigators found that vendors kept customer addresses in encrypted password managers and that the actual dispatch was outsourced to accomplices who mailed the packages from different Indian cities to avoid pattern recognition. Couriers and postal agencies play an unwitting role, which is why customs and postal monitoring has been identified in Lok Sabha answers as a priority for controlling dark web drugs.[19] The scene is completed by social media amplification, especially on Instagram-like platforms or on Telegram broadcast groups, where the darknet store's brand, menu, prices and delivery terms are advertised in plain language, after which the conversation is moved to a secure window with disappearing messages.

***Darknet Vendor Ecology in India***

Darknet vendor activity in India has shifted from occasional single-ship vendors to more professional, territory-aware sellers who target specific metro clusters and student populations. Operation MELON reported by NCB in July 2025 revealed a vendor operating under the alias "Ketamelon" who ran a multi-product catalogue of LSD, ketamine and MDMA, used TAILS OS for darknet access, accepted payments in crypto and relied on postal and dead-drop deliveries across Kochi and adjoining areas. The vendor also held cryptocurrency worth nearly Rs 70 lakh, which shows that narcotics proceeds are being stored digitally and can be attached under the PMLA once identified. The ecology is marked by consolidated vendors who buy in bulk from foreign suppliers, repackage into Indian-friendly denominations, and then sell on darknet markets while pushing Indian buyers to Telegram for real-time support. Postal routing is common because parcels of small size and legitimate appearance are less likely to be intercepted, and when seized, they create attribution problems because the parcel may be addressed to a rented address or to an unwitting person. Darknet vendors also invest in reputation management with customer reviews and refund policies, which increases demand and creates a consumer base that is difficult to disrupt by occasional seizures.[20]

***Encrypted Communications and Social Platforms***

Encrypted communications sit at the centre of cyber-facilitated drug trafficking because they allow real-time negotiation while preserving deniability. Telegram channels, WhatsApp business accounts, Signal groups and even lesser known apps like Zangi, as reported in Chennai's dead-drop cases, are used to share menus, QR codes, wallet addresses, GPS coordinates and pickup instructions, usually with disappearing messages and without full phone number visibility.[21] This practice brings the traceability rule in "Rule 4(2) of the IT Rules, 2021" into play because investigators often require identification of the first originator to connect a broadcast message advertising MDMA to the actual account holder who controlled the operation. The platforms have maintained that end-to-end encryption cannot be broken without weakening privacy for all users, leading to litigation and policy debate recorded in 2024 and 2025 commentaries.[22] Despite this, narcotics units can still demand basic subscriber information, IP logs, device identifiers and group metadata, especially when backed by "Section 17(2)(a) of the DPDP Act, 2023" which recognises processing of personal data for prevention, detection and investigation of offences.[23] The real challenge lies in evidentiary conversion, because chats exported from Telegram or WhatsApp must be supported by "Section 63 BSA" certificates, and if the platform does not issue such certificates, the officer must create one describing the process of extraction, the device used and the hash generated, failing which the defence may seek exclusion of the chats. The tension between privacy and traceability therefore plays out most sharply in narcotics cases, where the state interest in dismantling supply chains is very strong and the accused faces stringent bail conditions.

***Crypto Payments and Laundering Patterns***

Payment flows in cyber-narcotics cases usually begin with the buyer transferring BTC or another commonly listed token from a personal wallet or an Indian exchange to a wallet controlled by the vendor. Experienced vendors do not keep funds in that wallet but route them through exchange-hopping, chain-hopping or privacy coins such as Monero, after which they either cash out through Indian P2P markets or spend the crypto directly. The 2023 PMLA notification gives enforcement an entry point since every Indian-facing VDA exchange must collect KYC and report suspicious activity, so a narcotics FIR can be followed by a requisition to FIU-IND to identify which wallets or accounts received funds. Some 2025 actions against offshore

[19] Cases Under NDPS Act, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/185/AS131_rM5X7c.pdf?source=pqals (last visited on October 31, 2025).

[20] Julian Broséus, Damien Rhumorbarbe, Caro Mireault, Vincent Ouellette, Frank Crispino & David Décary-Hétu, "Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organisation from a Canadian Perspective", 264 *Forensic Science International* 7 (2016).

[21] Venkadesan S, "Traffickers Resort to 'Dead Drop' Method to Transit Drugs", *available at:* https://timesofindia.indiatimes.com/city/chennai/traffickers-resort-to-dead-drop-method-to-transit-drugs/articleshow/122393154.cms (last visited on October 30, 2025).

[22] Threats to Fundamental Rights in the Digital Era: Analysing Rule 4(2) of IT Rules 2021, *available at:* https://clsnluo.com/2025/02/13/threats-to-fundamental-rights-in-the-digital-era-analysing-rule-42-of-it-rules-2021/ (last visited on October 29, 2025).

[23] DPDPA Section 17: Exemptions, *available at:* https://dpdpa.com/dpdpa2023/chapter-4/section17.html (last visited on October 28, 2025).

VASPs, including notices and warnings, show that the government is now prepared to block or restrict overseas platforms that do not share data, which strengthens the hand of NDPS investigators.[24] Laundering patterns also include conversion of BTC to stablecoins like USDT, transfer to self-custody wallets, swap into privacy coins and then sale through local P2P dealers who pay in cash or bank transfers with innocuous descriptions. Each leg offers a point for legal control. Under NDPS, "Section 27A" can be invoked for financing illicit traffic. Under PMLA, the proceeds become property involved in money laundering and can be attached, and under the DPDP Act personal data related to these transactions can be processed for law enforcement. The challenge is to present blockchain analytics outputs in court with "Section 63 BSA" compliance, and to correlate them with device-level evidence seized from the accused.

***Youth Market and Synthetics***

A distinctive aspect of cyber-facilitated drug trafficking in India is the youth-focused market for synthetics and hallucinogens. NCB and parliamentary data between 2020 and 2025 point to rising seizures of LSD blotters, MDMA pills and designer party drugs that were ordered online by college students or young professionals and delivered through courier or collected from dead-drop locations shared via encrypted apps.[25] The appeal of darknet and social media channels for this demographic lies in the perception of anonymity, the absence of face-to-face contact, the ability to pay in small crypto amounts and the easy availability of micro quantities. For enforcement, such cases present legal dilemmas. Quantity may be small or intermediate but parcels may contain multiple hits, making application of the "Hira Singh" mixture rule potentially harsh when the blotter carriage material is counted. Search safeguards must be applied sensitively because many arrests follow digital surveillance and controlled deliveries rather than street-level interception, and strict "Section 37 NDPS Act" bail conditions can appear disproportionate for first-time youthful offenders caught in online stings. At the same time, courier-based LSD deliveries have shown links with larger darknet vendors operating across states, so investigative agencies must retain the power to map communications, demand traceability from platforms and invoke PMLA where crypto was used. In such cases, the data sharing clause in "Section 17 DPDP Act, 2023" and the recording provisions in "Section 105 BNSS" can be used to build a digital chain of evidence that traces the order from the encrypted chat to the wallet transfer, to the postal booking, to the parcel seizure, providing courts with a reliable basis to convict while still keeping space for prosecutorial discretion and policy reform on sentencing.

***Procedural and Evidentiary Hurdles***

Procedural compliance becomes the decisive filter through which cyber-facilitated drug trafficking cases under the "Narcotic Drugs and Psychotropic Substances Act, 1985" (NDPS Act) either survive or collapse at trial. Digital transactions, encrypted chats, cryptocurrency wallets, and deliveries routed through e-commerce logistics make the offence transnational in appearance but fragile in proof. Investigators must marry the rigid safeguards under "Sections 42, 50 and 52A of the NDPS Act" with newer methods such as device imaging, blockchain analytics and platform-based data extraction. Failure to record reasons of belief, to reduce telephonic intelligence into writing within the time stipulated, or to produce a tested and sealed sample before the court still leads to acquittal even when chat logs reveal active trafficking. The presence of the Bharatiya laws aggravates this tension, because the "Bharatiya Nagarik Suraksha Sanhita, 2023" now read with "Section 36A of the NDPS Act" demands a coherent chain of custody for extended remand, while the "Bharatiya Sakshya Adhiniyam, 2023" requires a certificate-driven regime for electronic records. Cyber seizures of phones, laptops, cold wallets or VPN-configured routers must therefore be preceded by correct search authorization, contemporaneous panchnama, videography of extraction, and exact matching of hash values to preserve integrity in court. Any gap between digital trail and statutory requirement benefits the accused, not because the court doubts the existence of a darknet marketplace, but because NDPS jurisprudence treats procedure as a substantive guarantee against misuse.[26]

***Section 50, 42 and 52A in Tech-Enabled Searches***

Electronic investigations do not dilute the personal search safeguards recognised by the Supreme Court. A cyber tip-off that an accused coordinates LSD deliveries over Telegram or Signal does not permit officers to skip the statutory choices embedded in "Section 50 of the NDPS Act" when the search ultimately turns on the person of the suspect. Remote surveillance, IP tracing and social media OSINT only justify reaching the physical search stage; they do not replace the duty to inform the accused of the right to be searched before a Gazetted Officer or a Magistrate. Digital-era searches must also differentiate between the person, the bag carrying a parcel booked on an e-commerce platform, and the digital device itself. The structure of "Section 42" continues to require prior recording of information and reporting to immediate superior officers, and in cyber-linked cases this extends to recording the tip received through Interpol I-24/7, the screenshot of the market listing, or the email from an intermediary that flagged suspicious consignments. When seized contraband is destroyed later, "Section 52A" directions on inventory, sampling and certification must be followed with scrupulous attention because cyber-facilitated consignments often involve small quantities concealed in diaries, books or electronics, making later reconstruction impossible.[27]

In the case of "*Vijaysinh Chandubha Jadeja v. State of Gujarat*[28], the Supreme Court addressed a prosecution under the NDPS Act where the core issue was whether the accused had been made aware of the exact right granted by "Section 50". The facts revealed that the search was preceded by an offer,

---

[24] Advisory to Virtual Digital Asset Service Providers for Registration With FIU-IND, *available at:* https://fiuindia.gov.in/pdfs/downloads/VDASP17102023.pdf (last visited on October 27, 2025).
[25] Lok Sabha Unstarred Question No. 328, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/185/AU328_XLmVB4.pdf?source=pqals (last visited on October 26, 2025).
[26] Eric Jardine, "Policing the Cybercrime Script of Darknet Drug Markets…", 46 *American Journal of Criminal Justice* 980 (2021).
[27] Eoghan Casey, *Digital Evidence and Computer Crime* 238 (Academic Press, Waltham, MA, 3rd edn., 2011).
[28] (2011) 1 SCC 609.

yet the offer was couched in general language and not in terms that conveyed an enforceable choice. The court noted that the person about to be searched must be told that he has a right, not a mere option, to be taken before a Gazetted Officer or a Magistrate, and this right must be conveyed in a manner that enables an individualised decision. The bench rejected the argument that substantial compliance would suffice, because the legislature had created "Section 50" as a safeguard in a statute that otherwise prescribes rigorous minimum sentences. The judgment held that non-communication of this right is not a curable irregularity and that the prosecution cannot draw support from the recovery itself to cure the illegality. The court underlined that the burden to prove a clear, conscious and informed waiver rests entirely on the prosecution and that a printed form, a joint notice for multiple accused, or an omnibus statement that the accused consented to a search cannot demonstrate compliance. It was also stressed that the court is not to presume knowledge of rights from the educational level or social status of the accused and that the officer must depose about the precise words spoken. On facts, the Supreme Court found that the notice served was not individualised, held the search to be vitiated, and acquitted the accused, reiterating that the gravity of the offence cannot dilute statutory safeguards.

The decision in "*State of Punjab v. Baldev Singh*[29] laid the constitutional foundation for the later ruling. The court recognised that NDPS offences often arise from sudden interception, secret information or chance recovery, yet it insisted that when the officer chooses to proceed under "Section 50" he must intimate the suspect that a search before a senior officer is available as of right. The court drew a careful distinction between searches of premises, vehicles or containers and the closer intrusion into the human body. It also clarified that failure to give this intimation does not automatically render the entire trial void, but the recovery made in violation of the mandate becomes suspect and can be excluded from consideration if it forms the sole incriminating material. In cyber-facilitated trafficking, where seizure of mobile phones and courier packets occurs simultaneously, this distinction serves to separate the validity of the device seizure from the validity of the personal search, preventing the prosecution from arguing that a clean personal search validates an improperly seized device.

The 6 October 2023 judgment of the Supreme Court in "*Ranjan Kumar Chadha v. State of Himachal Pradesh*[30] reaffirmed this line while dealing with a search where contraband was recovered from a bag carried on the shoulder. The court surveyed earlier decisions and repeated that "Section 50" applies to the person and not to baggage unless the baggage search is inseparable from a simultaneous personal search. The court observed that giving the accused a third option of being searched before a police officer vitiated compliance and that the High Court erred in treating the bag search as attracting "Section 50" when the person was not searched at all. The judgment is important for cyber-linked parcel cases because it recognises that a courier packet, a backpack containing 3D-printed concealment or a laptop bag is not automatically an extension of the body; only when the officer searches the body and the bag together will "Section 50" become mandatory, and even then the notice must speak of the statutory right and of nothing else. This clarification guides future trials where investigators rely on CCTV footage, call detail records and darknet chats to identify the suspect but must still defend the legality of the final physical search.

### *Confessional Statements and Section 67 NDPS*

Statements recorded by NDPS officers during digital-era investigations frequently narrate how the suspect ordered contraband from a darknet marketplace, paid through cryptocurrency, then used courier services to route the drugs to India. These statements are often extracted after sustained questioning, after devices have been seized, and before the accused has met counsel. The Supreme Court's approach has been to treat NDPS officers performing investigation as police officers for the purpose of confessional admissibility. The prosecution in cyber cases must therefore rely on electronic trails, platform responses, subscriber records, postal interceptions, and matched IP addresses rather than on statements recorded under "Section 67 of the NDPS Act". Where chats are in code or in regional languages, the prosecution must also produce translation certificates and independent witnesses to show that the accused actually controlled the account. Courts look for corroboration from digital footprints and will not accept bare admissions that the accused sold LSD blotters over Instagram.[31]

The Constitution Bench in "*Tofan Singh v. State of Tamil Nadu*[32], held that confessional statements made to officers invested with powers under the NDPS Act are inadmissible because such officers are police officers within the meaning of "Section 25 of the BSA" corresponding to the previous evidentiary bar. The court analysed the statutory scheme and noted that NDPS officers possess wide powers of search, seizure and arrest and can submit complaints directly before the Special Court, which places them on the same footing as traditional police for confessional purposes. The ruling declared that any admission of guilt recorded under "Section 67" cannot be used to convict an accused, although statements regarding discovery of material objects may still be saved. This position has sweeping consequences in cyber-facilitated cases where officers tend to write out long narratives containing usernames, wallet addresses and foreign collaborators based on the accused's oral disclosure. After "Tofan Singh", such narratives must be supported by call data from telecom service providers, server logs from platforms obtained under lawful orders, and certified extractions from devices, or else the prosecution case will fail for want of independent evidence.

### *Admissibility of Electronic Records*

The movement from the repealed "Section 65B of the Indian Evidence Act, 1872" to "Section 63 of the Bharatiya Sakshya Adhiniyam, 2023" retains the core logic that secondary electronic evidence requires a contemporaneous certificate that speaks to the manner of production, device in regular use, and

[29] (1999) 6 SCC 172.
[30] 2023 INSC 878.
1 [31] Thomas Joyce, " Following the (DNM) Bible? A crime script analysis of darknet drug vending", 80 *Crime, Law and Social Change* 419 (2023).
[32] (2021) 4 SCC 1.

integrity of the copy. The new law states that no electronic or digital record will be rejected purely because of its electronic character, but the party relying on it must still produce a certificate that identifies the electronic device, describes the process of conversion, and provides either a hash value or another reliable identifier. In cyber-facilitated drug prosecutions this means chat exports from WhatsApp, Telegram or Instagram, screenshots of darknet listings, blockchain transaction reports, e-commerce order histories and smartphone extraction reports must all carry a "Section 63 BSA" certificate from a responsible official or forensic analyst. Courts in India have become alert to the possibility of manipulation of screenshots and are likely to insist on production of the device or of a certified forensic image if the defence challenges authenticity.[33]

In "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[34], the Supreme Court restored the mandatory nature of the certificate requirement and said that a party wishing to rely on secondary electronic evidence must file the certificate at the time of tendering the evidence, except in narrowly defined situations where the device is out of reach or is held by an adversary public authority. The court rejected the practice of permitting oral evidence of authenticity in place of the certificate and clarified that an appellate or revisional court cannot ordinarily cure the absence of a certificate by invoking inherent powers. This principle travels intact into the BSA era and obliges drug law enforcement agencies to procure certificates from telecom providers, payment gateways, courier companies and social media intermediaries before filing the complaint. Failure to do so cannot be glossed over later by claiming that the material was downloaded from a secure government device because the certificate is the statutory bridge between digital environment and courtroom.

The judgment in "*Anvar P.V. v. P.K. Basheer*[35], supplied the baseline proposition that electronic records are on par with documentary evidence only when the conditions in the special provision are fulfilled. The court rejected admission of un-certified CDs and held that secondary electronic evidence without certificate is inadmissible. This became the fountainhead for later rulings and is still relevant because several state NDPS units continue to annex printed chat transcripts without certificate. For cyber-facilitated drug trafficking, forensic SOPs should capture the scene on video, note IMEI numbers, collect cloud credentials, create a write-blocked image, compute MD5/SHA-256 hashes, and record the person generating the certificate. To anchor these practices, an internal format may be evolved titled "Table 4: Digital seizure checklist and certificate contents under BSA" listing date and time of seizure, device details, operating system, extraction tool, hash values, location of original storage, name and designation of certifying officer, and reference to the investigating officer's case diary entry. Courts are more comfortable with blockchain analytics reports or darknet scraping outputs when accompanied by such structured certification because it signals that the data has not been altered after seizure.

***Quantity, Sampling and Mixtures***

Cyber trafficking often relies on micro-quantities engineered to pass unnoticed through postal systems. LSD blotters, MDMA crystals concealed in earphones, or designer drugs concealed in protein powders raise questions on whether the entire mixture is to be considered for quantity determination or only the active drug. The Supreme Court had previously seen conflicting views, but the practical problems became stark once e-commerce parcels began carrying small but pure consignments. Investigators sometimes sample only the blotter without testing the carrier paper or weigh only the dry powder without the packaging, leading to disputes during trial. When the parcel is intercepted after a controlled delivery, the entire process must be videographed and a part of the material must be sent promptly to the Forensic Science Laboratory with intact seals to guard against defence claims of planting.[36]

In "*Hira Singh v. Union of India*[37], the Supreme Court resolved the issue by holding that when a narcotic drug or psychotropic substance is mixed with one or more neutral substances, the quantity of the entire mixture is to be considered for determining whether the quantity is small, intermediate or commercial. The court gave primacy to the legislative intent behind the NDPS Act to deter trafficking and rejected arguments that only the pure drug content should count. This ruling has direct consequences for cyber-facilitated trafficking because contraband arriving in India through courier networks is often diluted or packed with adulterants to evade detection. If the entire parcel containing LSD impregnated paper, chocolate, or herbal mixtures is treated as the drug for quantity purposes, the accused will find it harder to secure bail or to argue that the offence is minor. Investigators must therefore record weights at each stage, preserve the packing, and refer to the standing orders on sampling so that the defence cannot argue that the parcel was weighed along with extraneous material such as bubble wrap or cardboard.

***Bail in NDPS and Cyber Cases***

Bail remains the arena where cyber evidence is most aggressively contested. "Section 37 of the NDPS Act" imposes twin conditions for offences involving commercial quantity: the court must hear the Public Prosecutor, and it must be satisfied that there are reasonable grounds to believe that the accused is not guilty and will not commit an offence if released. Digital trails obtained from chats or crypto wallets make it easier to attribute knowledge, so accused persons seek to puncture the admissibility of this material to show absence of reasonable grounds. The BNSS provisions that correspond to the old "Section 167(2) CrPC" continue to give an accused the right to default bail if investigation is not completed within the stipulated period and charge-sheet

[33] James Martin, *Drugs on the Dark Net* 126 (Palgrave Macmillan, London, 1st edn., 2014).
[34] (2020) 7 SCC 1.
[35] (2014) 10 SCC 473.
[36] Chan Wing Cheong, "Culpability in the Misuse of Drugs Act", 25 *Singapore Academy of Law Journal* 110 (2013).
[37] *Supra* note 13.

is not filed, yet in NDPS cases "Section 36A(4)" allows extension up to one year on a proper report. Courts therefore read BNSS timelines together with NDPS special provisions, leading to disputes on when the right to default bail actually arises.[38]

In "*State of Kerala v. Rajesh*[39], the Supreme Court emphasised that satisfaction under "Section 37" is not a mere formality. The court reversed a High Court order granting bail on lenient reasoning and held that positive satisfaction of the twin conditions is a sine qua non. The court pointed out that the quantity involved, the manner of concealment and the possibility of tampering with evidence must be assessed. This decision is frequently cited in cyber-linked prosecutions where the accused claims to be only the holder of a mobile phone or only a payment facilitator. The court's insistence on a rigorous approach means that even when electronic evidence is still under certification, the court may deny bail if prima facie material connects the accused with organised trafficking.

The ruling in "*Narcotics Control Bureau v. Mohit Aggarwal*[40], showed the court's approach to chat-based incrimination. The accused argued that WhatsApp chats without certificate could not form the basis for refusal of bail. The Supreme Court accepted that uncertified electronic transcripts may not ultimately be admissible, yet it stated that at the bail stage the court can look at the totality of materials, including call records, seizure memos and statements of co-accused, to decide whether "Section 37" is satisfied. The judgment therefore signals that defects in "Section 63 BSA" certification will not automatically open the door to bail in NDPS cases, particularly when other incriminating circumstances exist. Cyber traffickers using VPNs, foreign exchanges and drop addresses cannot bank solely on technicalities to secure release.

Recent orders of the Supreme Court and High Courts show a continued preference for the rigour of "Section 37" even after the coming into force of the BNSS, and courts have clarified that resort to further investigation under "Section 193(9) BNSS" will not defeat an already-accrued right to default bail, echoing what the Delhi High Court said while upholding BNSS safeguards.[41] For practical handling, investigators and prosecutors can adopt an internal narrative labelled "Table 5: Bail decision tree for NDPS cyber cases" describing sequential questions such as nature of quantity, presence of commercial features like multiple wallets or darknet orders, completion of "Section 63 BSA" certification, status of device forensic reports, and whether the statutory period has expired. Such a structured presentation helps courts see that the case is not based only on chats but on a holistic digital and physical trail.

***Intermediary Liability and Traceability***

Online platforms are now unavoidable intermediaries in cyber-facilitated drug trafficking. Offenders use messaging services, e-commerce storefronts, payment wallets, VPNs and cloud-based email to arrange supply chains. Indian law grants conditional safe harbour to such intermediaries under "Section 79 of the Information Technology Act, 2000" but attaches it to due diligence, prompt takedown and cooperation with lawful orders. The 2021 rules and subsequent amendments of 2022 and 2023 sharpened these conditions, partly to deal with online betting and deepfake problems, and partly to make intermediaries responsive to law enforcement seeking data about organised drug networks. The DPDP Act, 2023 operates in the background by permitting retention of personal data when required by law or by an investigating agency, so a platform can lawfully preserve transaction data or IP logs when served with an order concerning NDPS trafficking. Cyber-enabled drug cases therefore test the balance between user privacy and statutory obligations to assist the State.[42]

***IT Rules, 2021 and 2022 – 2023 Amendments***

The "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" introduced layered due diligence duties: publication of rules, appointment of grievance redressal officers, compliance with takedown orders within 24 hours for certain content categories, and the creation of nodal contacts for law enforcement. The 2022–2023 amendments, as reflected in the consolidated government version, underline that intermediaries must make reasonable efforts to prevent users from hosting or sharing content that promotes or encourages money laundering, terrorism or offences relating to narcotic drugs. A platform that receives a lawful request for subscriber details or message-related metadata in an NDPS probe must respond expeditiously or it risks losing safe harbour. Since many drug deals are brokered through closed groups, law enforcement frequently asks intermediaries to disable groups, preserve chats and share device registration data. The BNSS and the DPDP Act permit such disclosure subject to process, so intermediaries cannot plead privacy to refuse cooperation in a live NDPS case so long as the request is properly authorised.[43]

***Rule 4(2) Traceability Litigation***

Rule 4(2) of the 2021 Rules requires significant social media intermediaries providing messaging to enable identification of the first originator of information when ordered by a court or by a competent authority for specified offences. WhatsApp and its parent company challenged this requirement before the Delhi High Court, arguing that traceability will break end-to-end encryption and violate the right to privacy laid down in "*K.S. Puttaswamy v. Union of India*[44]. The petitions are still pending and the Union of India continues to defend traceability as a necessary tool for serious offences, including

[38] Sidney N. Lederman, *Michelle K. Fuerst & Hamish C. Stewart, Sopinka, Lederman & Bryant: The Law of Evidence in Canada* 192 (LexisNexis Canada, Toronto, 6th edn., 2022).
[39] (2020) 12 SCC 122.
[40] 2022 SCC OnLine SC 891.
[41] Adequate Safeguards in Law for Bail: Court, *available at:* https://timesofindia.indiatimes.com/city/delhi/adequate-safeguards-in-law-for-bail-court/articleshow/123569781.cms (last visited on October 25, 2025).
[42] Julian Broséus et al., "Studying Illicit Drug Trafficking on Darknet Markets…", 264 *Forensic Science International* 7 (2016).
[43] J. N. Barowalia & Abhishek Barowalia, *Commentary on the NDPS Act* 158 (LexisNexis, New Delhi, 2nd edn., 2023).
[44] (2017) 10 SCC 1.

NDPS offences with cyber features.[45] For investigators this litigation creates an operational gap: they can obtain subscriber information, IP logs and login history, but they cannot, in the absence of a final ruling, always insist on disclosure of the first originator for every narcotics message. Where end-to-end encryption is involved, feasibility itself becomes doubtful because tracing a broadcast message to the exact sender may require breaking encryption for all users, which the court may later disallow. Cyber NDPS investigations therefore tend to rely on endpoint forensics, carrier-level data and financial trails rather than on the contested traceability mandate.

***CERT-In 2022 Directions***

The directions issued by CERT-In on 28 April 2022 under "Section 70B(6) of the IT Act" require entities to log ICT system data, synchronise time with government network time protocol servers, and report specified cyber incidents within six hours of noticing them.[46] These directions matter for NDPS cyber cases because drug traffickers often use VPNs, hosting services and cloud infrastructure located abroad to mask their location. Service providers in India must maintain logs of customers and VPN sessions for at least five years, which enables law enforcement to attribute darknet buying and selling to identifiable persons even when they try to disappear after a single transaction. VPN and cloud providers who fail to maintain logs can be compelled by MeitY to comply or face blocking, creating leverage for investigators to demand data that corroborates seized devices. The time-synchronisation requirement also improves the evidentiary value of access logs because it allows hash-matched device timestamps to be placed alongside network logs in court.

***Crypto, Money Trails and PMLA Convergence***

Cyber-facilitated drug trafficking often ends in cryptocurrency settlements, particularly where buyers pay in USDT, Bitcoin or privacy coins and vendors later cash out through offshore exchanges. Once such funds pass through Indian accounts, the Prevention of Money Laundering Act, 2002 (PMLA) is attracted because NDPS offences are in the Schedule. The Enforcement Directorate has, in recent years, treated virtual digital asset (VDA) transactions connected with fraud and narcotics as proceeds of crime and has used PMLA search and seizure powers to freeze or take over wallets.[47] The convergence of NDPS and PMLA gives investigators wider room to target not just the courier who delivered the parcel but also the exchanger, the mule account holder and the VDA service provider who processed the withdrawal. This approach is consistent with government statements that VDA platforms operating in India or targeting Indian users must comply with PMLA reporting obligations.[48]

***Vda Sps as Reporting Entities***

On 4 July 2023, the FIU-IND issued guidance stating that virtual digital asset service providers must register and report suspicious transactions, placing them in the same category as banks, payment intermediaries and securities market entities. Non-compliant offshore exchanges received show-cause notices in December 2023 and again in 2025, signalling that the government expects KYC, record-keeping, IP logging and prompt furnishing of information when Indian agencies investigate trafficking or money laundering.[49] For NDPS cyber cases, this means investigators can ask FIU-IND for STRs filed by exchanges, match wallet addresses with KYC data, and move the Special Court to freeze balances pending trial. An internal working format captioned "Table 6: PMLA reporting and freezing toolkit for VDA-linked NDPS cases" can list steps such as identifying exchange, sending Section 50 PMLA summons, obtaining KYC and transaction history, requesting blockchain analytics for mixing services, issuing freezing orders to custodial wallets, and filing a provisional attachment before the Adjudicating Authority. This financial trail often supplies the independent corroboration that "Tofan Singh" now demands.

***Seizure and Freezing of Crypto Assets***

Seizing crypto assets is procedurally complex because the asset is intangible and control lies with whoever holds the private key or seed phrase. Investigators must therefore, at the time of arrest or device seizure, record the exact wallet applications installed, compel the accused to disclose seed phrases where law permits, and create on-the-spot hash-verified screenshots of wallet balances. When records are exported from exchanges, the prosecution must secure "Section 63 BSA" certificates from the compliance officer of the exchange so that transaction histories, IP logs and KYC documents can be read in evidence. Chain analytics tools can de-anonymise transactions passing through major blockchains, but their reports must also be certified. Postal and courier interdictions sometimes reveal paper backups of seed phrases or hardware wallets, and these must be seized and sealed

[45] Editor, "Del HC | WhatsApp Challenges Intermediary Rules, Says Traceability Will Break End-To-End Encryption, Breach Privacy; Union of India Says No Fundamental Right Is Absolute", *available at:* https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/ (last visited on November 3, 2025).

[46] Directions Under Section 70B of the Information Technology Act, 2000 (Dated 28.04.2022), *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on November 2, 2025).

[47] Press Release: Search in BitConnect Case, 15.02.2025, *available at:* https://enforcementdirectorate.gov.in/sites/default/files/latestnews/Press%20Release-Search-%20Bitconnect-15.02.2025.pdf (last visited on November 1, 2025).

[48] Jaspreet Kalra, "Binance Registers With India's Financial Watchdog as It Seeks to Resume Operations", *available at:* https://www.reuters.com/business/finance/binance-registers-with-indias-financial-watchdog-it-seeks-resume-operations-2024-05-10/ (last visited on October 31, 2025).

[49] Financial Intelligence Unit India (FIU-IND) Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs), *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372 (last visited on October 30, 2025).

like any other document. The freezing of assets under PMLA can then be tied back to the NDPS complaint to show that the funds are proceeds of drug trafficking.[50]

***International Cooperation and Jurisdiction***

Cyber-facilitated drug trafficking thrives on cross-border elements. Darknet markets are hosted on servers in Europe, buyers are in India, sellers may be in Southeast Asia, and payments flow through global exchanges. Indian agencies must therefore resort to mutual legal assistance treaties (MLATs), letters rogatory and 24x7 points of contact to secure server logs, subscriber details and content records. The Ministry of Home Affairs has issued detailed MLAT guidelines that require requests for electronic evidence to specify IP addresses, time zones, user identifiers and the precise offences invoked.[51] Delays in receiving data sometimes affect NDPS timelines for filing complaints, making early preservation letters and domestic orders under the IT Act critical. Jurisdictionally, Indian courts have accepted that when part of the conspiracy or delivery occurs in India, they can try the offence even if the server is abroad, especially when the evidence shows that the drugs were meant for consumption or distribution in India.

***India's Non-Accession to Budapest Convention***

India has still not acceded to the Council of Europe's Convention on Cybercrime, widely known as the Budapest Convention.[52] Despite this, India participates in the G7/GLACY+ style 24x7 network and pursues cooperation through bilateral and multilateral MLATs. The reluctance to join stems from concerns over sovereignty, data localisation and the asymmetry of obligations, especially when several source countries for cybercrime are themselves not parties. For NDPS cyber cases this means Indian investigators cannot rely on the expedited data preservation and direct cooperation channels that Budapest parties enjoy, so they must lean on domestic powers under the IT Act, NDPS Act and PMLA to secure data from Indian intermediaries before it is lost. The non-accession also means that India often negotiates access to foreign-held data on a case-by-case basis, which works when the foreign platform has a presence in India but becomes slow when only the US-based CLOUD Act route is available.

***U.N. Cybercrime Convention, 2024 Adoption***

The United Nations Convention against Cybercrime was adopted by the UN General Assembly in December 2024 to create a global framework for preventing and combating cybercrime and for sharing electronic evidence.[53] The treaty opened for signature in 2025, with many states signalling support, though civil society raised concerns about surveillance and human rights. India has taken a cautious line, participating in negotiations but insisting on safeguards for data sovereignty and privacy. For NDPS cyber investigations, this treaty promises faster access to cross-border data and more predictable timelines for executing requests, which would help in cases where drugs are ordered from servers located in non-traditional jurisdictions. At the same time, the treaty's final shape will determine whether India can insist on dual criminality for narcotics offences linked to encrypted platforms.

***Comparative Note***

A short comparison shows that the European Union, through instruments like the e-evidence Regulation, and the United States, through the CLOUD Act and strict VDA AML rules, have created faster and more direct channels for obtaining electronic evidence and for regulating platforms than India presently has. The Indian model relies on "Section 79 IT Act", the 2021 Rules, CERT-In directions and the DPDP Act to impose due diligence, but continues to route most cross-border requests through MLATs.[54] In the crypto AML space, the US and EU require VASPs to travel rule data and to register nationally, while India has achieved functional parity by designating VDA SPs as reporting entities and by blocking non-compliant offshore exchanges. This position can be captured in a narrative titled "Table 7: Comparative cooperation mechanisms and e-evidence standards", listing EU's direct cooperation orders, US's CLOUD Act and FinCEN rules, and India's MLAT-based but widening domestic compulsion framework. Such a comparative lens helps explain why cyber-facilitated drug trafficking cases in India face longer evidentiary timelines and why courts insist so strongly on strict NDPS procedural compliance to offset these structural delays.

## Conclusion

The analysis demonstrates that cyber-facilitated trafficking is not a new crime but a new *mode* that reroutes the classic NDPS triad-supply, payment, delivery-through infrastructures the 1985 statute never contemplated. Doctrinally, NDPS captures the conduct (Sections 8, 20–29) and preserves a stringent bail regime (Section 37), yet prosecution quality now pivots on how well investigators translate digital intelligence into admissible exhibits. Three levers emerge as decisive. First, procedure: BNSS Section 105 mandates audio-video recording of search and seizure; when used at courier hubs

[50] *Supra* note 31.
[51] ISII Comprehensive Guidelines (17.12.2019), *available at:* https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines_17122019%5B1%5D.pdf (last visited on October 29, 2025).
[52] India: Country Page on Cybercrime, *available at:* https://www.coe.int/en/web/octopus/-/india (last visited on October 28, 2025).
[53] Cybercrime Convention — Home, *available at:* https://www.unodc.org/unodc/cybercrime/convention/home.html (last visited on October 27, 2025).
[54] The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=105 (last visited on October 26, 2025).

and controlled deliveries, it anchors chain-of-custody and complements NDPS Sections 42/43/52A in a technology-neutral way.[55] Second, proof: BSA Section 63 shifts electronic material from "printout" culture to a certificate-and-hash regime; failures here-missing device particulars, inconsistent hashes, or the wrong signatory-regularly sink cases.[56] Third, financial convergence: the March 7, 2023 notification pulls VDA service providers into PMLA, enabling KYC, STRs and freezes that stitch blockchain trails to real-world identities; when activated early, it generates corroboration that *Tofan Singh* now demands beyond inadmissible Section 67 narratives. Enforcement experience (e.g., Operation MELON) shows that when these levers are used together-videographed openings of parcels, contemporaneous device imaging, Section 63 certificates for chat exports and wallet statements, and timely FIU-IND engagement-courts are more willing to treat encrypted communications and crypto flows as reliable circumstantial proof.[57]

At the same time, the jurisprudential guardrails remain exacting. The Supreme Court's mixture rule in *Hira Singh* heightens stakes at the threshold-especially for micro-dose LSD or adulterated consignments-by tying bail and punishment bands to total mixture weight, although the Court has recently agreed to revisit the logic, reflecting concerns about proportionality.[58] Bail continues to be filtered through the rigorous twin conditions under Section 37, with *State of Kerala v. Rajesh*[59] and *NCB v. Mohit Aggarwal*[60] signalling that even at the bail stage, a holistic prima facie picture (beyond uncertified chats alone) can justify custody.[61] Privacy-traceability tensions also persist: Rule 4(2)'s "first originator" mandate is under constitutional challenge, pushing agencies toward endpoint forensics, carrier-level logs and PMLA data rather than universal decryption.[62] Complementary cyber-policy requirements-CERT-In's 28 April 2022 directions on time-sync and log retention-quietly underwrite attribution in VPN/cloud contexts and should be woven into NDPS playbooks. Finally, cross-border latency remains a bottleneck; the UN Cybercrime Convention adopted in December 2024 (now open for signature) may shorten e-evidence timelines once operational, but until then, India must rely on domestic compulsion and MLATs while hardening its evidentiary processes at home.

## Suggestions

Against the backdrop of this article's focus, the following targeted measures are proposed to convert volatile cyber trails into court-worthy evidence without diluting rights:[63]

- BNSS-first search discipline at courier hubs. Mandate A/V recording for all NDPS searches of postal/courier facilities, using a standard capture protocol that logs GPS, timestamps (NTP-synced), and witness sign-offs. Require immediate upload to the court-facing repository specified by BNSS Section 105 and local SOPs. Link each video to a seizure memo QR so exhibits and footage reconcile at filing.
- Section 63 BSA "one-page" certificate kit. Issue a national template pack for chats, email headers, device images and blockchain CSVs with fields for device particulars, tools used, and SHA-256 values. Make the IO and a lab analyst co-sign where the platform declines to certify. Build a pre-filing checklist that rejects chargesheets lacking hashes or proper signatories. Train prosecutors to object to defence "printout" attempts to keep parity.
- Early PMLA docking for VDA flows. Within 72 hours of registering an NDPS FIR involving crypto, require: (a) wallet triage and on-chain tracing; (b) STR/CTR pulls from FIU-IND; and (c) provisional freezes at custodial VASPs. Publish a model "NDPS↔PMLA bridge" SOP that maps summons formats and timelines for exchanges. Track hits in a dashboard to drive parallel attachment under Sections 5/17 PMLA.
- CERT-In logging as evidentiary spine. Direct all district cyber cells to issue preservation letters that cite the April 28, 2022 CERT-In directions (log retention, NTP sync, PoC) when approaching ISPs/VPNs/clouds. Add a form paragraph in requests specifying the UTC offset and hash targets to ease later matching. Build a local "log map" so investigators know which providers keep which artefacts for how long. Audit compliance semi-annually with spot checks.
- Intermediary cooperation timers + escalation. For takedown, subscriber data, and metadata, set internal clocks (e.g., 24h preservation, 72h production) consistent with the IT Rules; record delays and escalate through nodal contacts to MeitY. Where Rule 4(2) traceability is invoked, ensure orders are tightly scoped to the offence and timeframe to withstand scrutiny. If originator data is unavailable, pivot to endpoint forensics and carrier CDR/IPDRs to avoid stall. Publish quarterly scorecards of platform responsiveness.
- Controlled-delivery playbook for digital tips. When darknet intelligence triggers a postal intercept, pre-authorise controlled delivery with

---

[55] The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nagarik_Suraksha_Sanhita%2C_2023.pdf (last visited on October 25, 2025).

[56] Certificate for Electronic Evidence as per Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://lawgic.info/wp-content/uploads/2024/06/Certificate-for-Electronic-Evidence-as-per-section-634c-of-the-Bharatiya-Sakshya-Adhiniyam-2023-1.pdf (last visited on November 3, 2025).

[57] Press Release: Darknet Case — Cochin (01.07.2025), *available at:* https://narcoticsindia.nic.in/pressrelease/01_07_25_hq_cochin_darknet.pdf (last visited on November 2, 2025).

[58] Hira Singh v. Union of India — Judgment (22 April 2020), *available at:* https://narcoticsindia.nic.in/Judgments/Hira_Singh_vs_Uoi_on_22_April_2020.pdf (last visited on November 1, 2025).

[59] *Supra* note 39.

[60] 2022 LiveLaw (SC) 613.

[61] State of Kerala v. Rajesh — Judgment (24 January 2020), *available at:* https://narcoticsindia.nic.in/Judgments/State_Of_Kerala_vs_Rajesh_on_24_January_2020.pdf (last visited on October 31, 2025).

[62] Prashant Jha, "Breaking Encryption Will End WhatsApp: Delhi High Court Told in Challenge to IT Rules", *available at:* https://www.barandbench.com/news/breaking-encryption-whatsapp-delhi-high-court-challenge-it-rules (last visited on October 30, 2025).

[63] J. Sasikumar, " Dark Net Drug Transactions (DNDT): An Emerging Crypto- Trends in Drug Trafficking", 49 *Indian Journal of Criminology* 88 (2021).

embedded videography, live hash of packaging, and staged sampling under Section 52A. Script roles: a parcel-handler, an A/V officer, a sampler, and a documentation lead. On breach, capture the first-touch A/V plus fingerprints to establish conscious possession. Pair with contemporaneous extraction of the consignee's device for chat-wallet correlation.

- Mixture-rule proportionality buffers. Pending the Supreme Court's re-examination of *Hira Singh*, instruct FSLs and IOs to record gross, net, and carrier weights separately, and to preserve representative samples of carrier media (e.g., LSD blotter paper) with video documentation. Require prosecutors to explain quantity calculations in bail oppositions with FSL notes attached. Train investigators to avoid weighing extraneous packaging (bubble wrap, cardboard) to reduce challenge risks. Maintain a "quantity worksheet" in every case.
- Youth-market diversion protocol. For first-time, small-quantity online buyers with no network role, build a diversion track: rapid forensic triage to exclude upstream roles, counselling referral, and tightly supervised probation, while reserving full NDPS rigour for suppliers/financiers. Codify objective screens (no bulk orders, no reseller evidence, no crypto off-ramp history) to avoid arbitrariness. This preserves prosecutorial bandwidth for darknet vendOrs Publish anonymised outcomes to build legitimacy.
- Court-ready exhibits by design. Require that every digital exhibit (chat PDF, wallet CSV, scraping output) is stamped with a unique Exhibit ID, file hash, and device/location provenance. Keep immutable originals and produce redacted working copies to the defence with an integrity statement. Standardise exhibit bundles so judges see a consistent order: A/V search, seizure memo, forensic image hashes, Section 63 certificate, platform response, blockchain trace, and PMLA linkage. Run pre-trial "mock admissibility" reviews to catch defects early.
- International evidence fast-lane. Until the UN Cybercrime Convention mechanisms mature, maintain a 24×7 e-evidence team to draft MLAT/letters rogatory with precise time-zones, IPs, and retention asks; send same-day preservation to platforms with India footprint. Map which providers accept domestic process versus treaty requests and keep templates ready. Track turnaround KPIs and escalate stale requests through diplomatic channels. Once available, pilot Convention channels on a small docket and publish timelines for practitioner guidance.

**Bibliography**

**Books:**

- Eoghan Casey, *Digital Evidence and Computer Crime* (Academic Press, Waltham, MA, 3rd edn., 2011).
- Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (Academic Press, Waltham, MA, 3rd edn., 2011).
- J. N. Barowalia & Abhishek Barowalia, *Commentary on the Narcotic Drugs and Psychotropic Substances Act* (LexisNexis, New Delhi, 2nd edn., 2023).
- J. N. Barowalia & Abhishek Barowalia, *Commentary on the NDPS Act* (LexisNexis, New Delhi, 2nd edn., 2023).
- James Martin, *Drugs on the Dark Net* (Palgrave Macmillan, London, 1st edn., 2014).
- Sidney N. Lederman, *Michelle K. Fuerst & Hamish C. Stewart, Sopinka, Lederman & Bryant: The Law of Evidence in Canada* (LexisNexis Canada, Toronto, 6th edn., 2022).
- Stephen Mason & Daniel Seng (eds.), *Electronic Evidence and Electronic Signatures* (Institute of Advanced Legal Studies, London, 5th edn., 2021).

**Statutes:**

- The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 47 of 2023)
- The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023)
- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 46 of 2023)
- The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (GSR 139(E) of 2021)
- The Information Technology Act, 2000 (Act No. 21 of 2000)
- The Narcotic Drugs and Psychotropic Substances Act, 1985 (Act No. 61 of 1985)
- The Prevention of Money Laundering Act, 2002 (Act No. 15 of 2003)

**Articles:**

- Chan Wing Cheong, "Culpability in the Misuse of Drugs Act", 25 *Singapore Academy of Law Journal* 110 (2013).
- Eric Jardine, "Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention", 46 *American Journal of Criminal Justice* 980 (2021).

- Eric Jardine, "Policing the Cybercrime Script of Darknet Drug Markets…", 46 *American Journal of Criminal Justice* 980 (2021).
- J. Sasikumar, "Dark Net Drug Transactions (DNDT): An Emerging Crypto- Trends in Drug Trafficking", 49 *Indian Journal of Criminology* 88 (2021).
- Julian Broséus et al., "Studying Illicit Drug Trafficking on Darknet Markets…", 264 *Forensic Science International* 7 (2016).
- Julian Broséus, Damien Rhumorbarbe, Caro Mireault, Vincent Ouellette, Frank Crispino & David Décary-Hétu, "Studying Illicit Drug Trafficking on Darknet Markets: Structure and Organisation from a Canadian Perspective", 264 *Forensic Science International* 7 (2016).
- Thomas Joyce, " Following the (DNM) Bible? A crime script analysis of darknet drug vending", 80 *Crime, Law and Social Change* 419 (2023).

**Websites:**

- Adequate Safeguards in Law for Bail: Court, *available at:* https://timesofindia.indiatimes.com/city/delhi/adequate-safeguards-in-law-for-bail-court/articleshow/123569781.cms (last visited on October 25, 2025).
- Advisory to Virtual Digital Asset Service Providers for Registration With FIU-IND, *available at:* https://fiuindia.gov.in/pdfs/downloads/VDASP17102023.pdf (last visited on October 27, 2025).
- Ambu Raja, "Certificate Under 63(4) of Bharatiya Sakshya Adhiniyam", *available at:* https://www.scribd.com/document/837411615/Certificate-Under-63-4-of-BHARATIYA-SAKSHYA-ADHINIYAM (last visited on November 2, 2025).
- Cases Under NDPS Act, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/185/AS131_rM5X7c.pdf?source=pqals (last visited on October 31, 2025).
- Certificate for Electronic Evidence as per Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://lawgic.info/wp-content/uploads/2024/06/Certificate-for-Electronic-Evidence-as-per-section-634c-of-the-Bharatiya-Sakshya-Adhiniyam-2023-1.pdf (last visited on November 3, 2025).
- Cybercrime Convention - Home, *available at:* https://www.unodc.org/unodc/cybercrime/convention/home.html (last visited on October 27, 2025).
- Directions Under Section 70B of the Information Technology Act, 2000 (Dated 28.04.2022), *available at:* https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on November 2, 2025).
- DPDPA Section 17: Exemptions, *available at:* https://dpdpa.com/dpdpa2023/chapter-4/section17.html (last visited on October 28, 2025).
- Dwaipayan Ghosh, "NCB Nabs 2 With Cocaine From Kenya", *available at:* https://timesofindia.indiatimes.com/city/kolkata/ncb-nabs-2-with-cocaine-from-kenya/articleshow/122580168.cms (last visited on October 29, 2025).
- Editor, "Del HC | WhatsApp Challenges Intermediary Rules, Says Traceability Will Break End-To-End Encryption, Breach Privacy; Union of India Says No Fundamental Right Is Absolute", *available at:* https://www.scconline.com/blog/post/2021/05/27/del-hc-whatsapp-challenges-intermediary-rules-says-traceability-will-break-end-to-end-encryption-breach-privacy-union-of-india-says-no-fundamental-right-is-absolute/ (last visited on November 3, 2025).
- Financial Intelligence Unit India (FIU-IND) Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers (VDA SPs), *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372 (last visited on October 30, 2025).
- Hira Singh v. Union of India - Judgment (22 April 2020), *available at:* https://narcoticsindia.nic.in/Judgments/Hira_Singh_vs_Uoi_on_22_April_2020.pdf (last visited on November 1, 2025).
- India: Country Page on Cybercrime, *available at:* https://www.coe.int/en/web/octopus/-/india (last visited on October 28, 2025).
- ISII Comprehensive Guidelines (17.12.2019), *available at:* https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines_17122019%5B1%5D.pdf (last visited on October 29, 2025).
- Jaspreet Kalra, "Binance Registers With India's Financial Watchdog as It Seeks to Resume Operations", *available at:* https://www.reuters.com/business/finance/binance-registers-with-indias-financial-watchdog-it-seeks-resume-operations-2024-05-10/ (last visited on October 31, 2025).
- Lok Sabha Unstarred Question No. 328, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/185/AU328_XLmVB4.pdf?source=pqals (last visited on October 26, 2025).
- Lok Sabha Unstarred Question No. 4988: Steps to Check Drug Trafficking, *available at:* https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS01042025/4988.pdf (last visited on October 30, 2025).
- Notification S.O. 1072(E) Under the Prevention of Money-Laundering Act, 2002, *available at:* https://egazette.gov.in/WriteReadData/2023/

244184.pdf (last visited on October 25, 2025).

- Prashant Jha, "Breaking Encryption Will End WhatsApp: Delhi High Court Told in Challenge to IT Rules", *available at:* https://www.barandbench.com/news/breaking-encryption-whatsapp-delhi-high-court-challenge-it-rules (last visited on October 30, 2025).
- Press Release, *available at:* https://narcoticsindia.nic.in/pressrelease.php (last visited on November 3, 2025).
- Press Release: Darknet Case - Cochin (01.07.2025), *available at:* https://narcoticsindia.nic.in/pressrelease/01_07_25_hq_cochin_darknet.pdf (last visited on November 2, 2025).
- Press Release: Search in BitConnect Case, 15.02.2025, *available at:* https://enforcementdirectorate.gov.in/sites/default/files/latestnews/Press%20Release-Search-%20Bitconnect-15.02.2025.pdf (last visited on November 1, 2025).
- Registration of Virtual Digital Asset Service Providers in FIU India as Reporting Entity-Reg., *available at:* https://fiuindia.gov.in/pdfs/downloads/VDASP04072023.pdf (last visited on November 1, 2025).
- Spread of Illicit Drugs Through Dark Web, *available at:* https://sansad.in/getFile/loksabhaquestions/annex/177/AU3691.pdf?source=pqals (last visited on October 26, 2025).
- State of Kerala v. Rajesh - Judgment (24 January 2020), *available at:* https://narcoticsindia.nic.in/Judgments/State_Of_Kerala_vs_Rajesh_on_24_January_2020.pdf (last visited on October 31, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://prsindia.org/files/bills_acts/bills_parliament/2023/Bharatiya_Nagarik_Suraksha_Sanhita%2C_2023.pdf (last visited on October 25, 2025).
- The Bharatiya Nagarik Suraksha Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/21544/1/the_bharatiya_nagarik_suraksha_sanhita%2C_2023.pdf (last visited on October 28, 2025).
- The Bharatiya Nyaya Sanhita, 2023, *available at:* https://prsindia.org/billtrack/the-bharatiya-nyaya-sanhita-2023 (last visited on November 1, 2025).
- The Bharatiya Sakshya Adhiniyam, 2023, *available at:* https://www.mha.gov.in/sites/default/files/2024-04/250882_english_01042024_0.pdf (last visited on October 31, 2025).
- The Digital Personal Data Protection Act, 2023, *available at:* https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last visited on October 27, 2025).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 [Updated as on 6.4.2023], *available at:* https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (last visited on November 2, 2025).
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, *available at:* https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021 (last visited on November 3, 2025).
- The Information Technology Act, 2000, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=105 (last visited on October 26, 2025).
- Threats to Fundamental Rights in the Digital Era: Analysing Rule 4(2) of IT Rules 2021, *available at:* https://clsnluo.com/2025/02/13/threats-to-fundamental-rights-in-the-digital-era-analysing-rule-42-of-it-rules-2021/ (last visited on October 29, 2025).
- Venkadesan S, "Traffickers Resort to ‘Dead Drop' Method to Transit Drugs", *available at:* https://timesofindia.indiatimes.com/city/chennai/traffickers-resort-to-dead-drop-method-to-transit-drugs/articleshow/122393154.cms (last visited on October 30, 2025).