WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Dark Web, Digital Assets, and Criminal Liability: The Emerging Nexus between Cryptocurrency and Organized Crime

Simratpal Kaur[1], Dr. Harshita Thalwal[2]

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

ABSTRACT :

The article interrogates the convergence of dark web markets, virtual digital assets, and organized criminality, and it does so through a doctrinal lens grounded in Indian public law and criminal procedure. The core problem lies in attributing culpability where anonymity, pseudo-anonymous wallet infrastructure, and cross-border routing frustrate traditional evidentiary and jurisdictional methods. The analysis maps how "virtual digital assets" gained a determinate meaning in Indian tax law through "Section 2(47A) of the Income-tax Act" and how "Section 115BBH" and "Section 194S" now structure reporting and revenue collection. The inquiry then situates the March 7, 2023 expansion of "reporting entities" under the "PMLA" to include VDA-facing services, which generates obligations for exchanges, custodial wallets, and related actors, supported by updated PML Rules and FIU-India guidance. The piece also examines the "CERT-In Directions of April 28, 2022", which impose logging, incident reporting, and KYC-style validation touching VASPs, VPS, and VPN providers relevant to crypto compliance pipelines. Within the substantive criminal law, the "BNS" adds a consolidated "organized crime" offence with application to cyber-enabled syndicates, while the "NDPS Act" has already intersected with crypto tracing in darknet narcotics matters such as NCB's Operation Melon. Finally, "UAPA" standards on terror financing frame the residual high-risk perimeter where stablecoins and cross-chain obfuscation raise attribution hurdles. The doctrinal method reads text, rules, and judgments against actual enforcement arc, including FIU-India actions against offshore exchanges and the penalty and registration pathway for global platforms seeking re-entry. Key findings indicate that Indian law now supplies clear AML anchors for VASPs, retains high tax frictions that curb retail laundering channels, and preserves evidentiary continuity through the "BSA" certificate lineage. Reform proposals stress calibrated travel-rule implementation, exchange-mixer liability tests aligned with knowledge standards, streamlined wallet-freezing templates under "PMLA" and "BNSS", and MLAT practices adapted to non-Budapest cooperation realities.

Keywords: Cryptocurrency, Dark web, Virtual digital assets, PMLA, BNS, NDPS, FIU India, FATF, Evidence law, Cybercrime

Introduction

The past half-decade has seen virtual digital assets grow from speculative curiosities into settlement media for cyber-enabled crime, with darknet markets and illicit service economies using pseudo-anonymous payment rails, escrow practices, and laundering stacks that challenge routine policing. India's response has moved from observation to active supervision. Tax law now frames VDAs through "Section 2(47A)" of the Income-tax Act, with a 30 percent rate under "Section 115BBH" and a 1 percent withholding under "Section 194S" for transfers above specified thresholds.[1] Anti-money laundering law widened on 7 March 2023, when the Ministry of Finance brought VDA-related services into the "PMLA" reporting perimeter, pulling exchanges, transfer facilitators, and custodial services into FIU-India's orbit. Technical regulation matured in parallel, as CERT-In's 2022 Directions mandated near-real-time incident reporting, system log retention, and subscriber validation duties for a broad set of intermediaries, including virtual asset service providers. Enforcement then followed policy: FIU-India issued show-cause notices to offshore exchanges, sought URL blocking for non-compliance, required registration, and imposed penalties, while certain platforms completed FIU registration and settled monetary sanctions. Against this domestic backdrop, international practice illuminates recurrent crime patterns, notably the Hydra and AlphaBay takedowns that exposed mixers, dead drops, and sophisticated cash-out loops that moved illicit proceeds through layered crypto stacks. The Indian framework also added an "organized crime" offence in the "BNS", while the "NDPS Act" has provided predicate pathways where darknet narcotics cases use blockchain analytics to link trafficking to wallets and exchange accounts. The article's doctrinal lens reads statutory text and rules in light of recent operations to test how the elements of offence, mental states, attribution to platforms, and extraterritorial reach meet the specific risks of VDA-mediated wrongdoing.[2]

Research Questions

The research questions for the study are as follows: -

[1] Updated Guidance: FATF Recommendation 15 — Virtual Assets, *available at:* https://www.fatf-gafi.org/en/publications/Guidance/Guidance-va-vaps.html (last visited on October 23, 2025).
[2] The Income-Tax Act, 1961, *available at:* https://incometaxindia.gov.in/Acts/Income-tax Act%2C 1961/2024_1/102120000000081156.htm (last visited on October 27, 2025).

- To delineate how Indian statutes allocate actus reus and mens rea elements to VDA-linked laundering, drug trafficking, terror financing, and tax offences across "PMLA", "BNS", "NDPS", "UAPA", and the Income-tax Act.
- To evaluate when platforms and intermediaries incur liability under "PMLA" and "BNS", and whether procedural powers under "BNSS" and evidentiary rules under "BSA" are sufficient to secure convictions in cross-border, pseudo-anonymous crypto contexts.

Problem Statement

Attribution falters when services fragment across wallets, custodians, mixers, and privacy-preserving networks, while jurisdiction splinters as nodes, data, and suspects sit abroad. Indian criminal law must map liability to conduct that occurs through VDAs without misfitting legacy constructs. The challenge is to reconcile "PMLA" obligations, high-friction VDA taxation, CERT-In technical duties, and "BNS" organized crime coverage with workable seizure, freezing, and evidentiary routes that withstand judicial scrutiny despite anonymization and multi-country routing.

Objectives of the Study

The objectives of the study are as follows: -

- To construct a doctrinal map of offence clusters that identifies conduct, knowledge standards, and attribution rules for VDA-enabled organized crime.
- To propose calibrated procedural and compliance reforms that improve freezing, evidence capture, and cross-border cooperation while preserving due process under "BNSS" and admissibility under "BSA."

Research Methodology

The method is doctrinal and black-letter. Statutes, delegated rules, official notifications, FIU-India and CERT-In instruments, and Supreme Court judgments are read against public enforcement outputs and select international comparators such as FATF Recommendation 15 updates and darknet market takedowns. The approach is India-centred, using foreign materials for illumination rather than authority, with emphasis on statutory text, schedules, and certificates under "BSA", and procedural pivots under "BNSS."

Concepts and Typologies

The conceptual baseline starts with the legal meaning of "virtual digital asset", which anchors taxation and AML coverage, and then moves to empirical crime patterns on the dark web. Marketplace structures, escrow logic, reputational systems, and vendor discipline shape how tokens circulate and are laundered, while service layers such as mixers and cross-chain bridges mediate proceeds. On the domestic criminal side, organized crime's statutory elements under the "BNS" supply a gate to capture syndicate behaviour where the wrong involves coordinated, continuing illegal activity with economic advantage, overlapping cyber and physical acts. This section brings the categories together to show which Indian statutes and agencies are typically implicated and where evidentiary and procedural frictions emerge.[3]

Virtual Digital Assets

Indian tax law defines VDA expansively through the 2022 amendments, with "Section 2(47A)" capturing any digital representation of value generated through cryptographic or other means that can be transferred, stored, or traded electronically, and expressly including NFTs subject to notified exclusions. Income from transfers is taxed at a flat rate under "Section 115BBH", with no deduction except cost of acquisition and no set-off of losses; "Section 194S" imposes a 1 percent TDS on consideration for transfers subject to thresholds and payer categories. CBDT's notification architecture clarifies the NFT perimeter. This definition is distinct from proposed central bank digital currency, which is state money, and from securities, though overlap questions arise for tokenized instruments and schemes. As construed for AML, "PMLA" now ties VASP status to activities relating to exchange, transfers, safekeeping, and sale participation.[4]

Dark Web and Crypto Crime Patterns

Darknet markets, such as AlphaBay and Hydra, demonstrated how cryptocurrencies, escrow, vendor ratings, and off-market laundering combined to scale distribution of narcotics, data, and illicit services, often with mixers and nested exchange accounts assisting cash-out. Hydra added "laundering shops" and dead-drop logistics that reduced interception risk and rerouted value through localized channels. Takedowns showed both the fragility of centralized platforms and the resilience of vendor networks that migrate and reconstitute. These patterns matter in India because they mirror how postal channels, drop shipments, and retail crypto rails have featured in NCB and ED investigations, and because exchange controls and KYC standards determine whether domestic platforms become choke points or conduits.[5]

---

[3] BNS Section 111 Organized Crime, *available at:* https://devgan.in/bns/section/111/ (last visited on October 24, 2025).

[4] Notification No. 75/2022: Specification of Non-Fungible Token as Virtual Digital Asset, *available at:* https://incometaxindia.gov.in/communications/notification/notification-no-75-2022.pdf (last visited on October 23, 2025).

[5] Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, *available at:* https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (last visited on October 22, 2025).

Organised Crime in BNS

The "BNS" codifies an "organized crime" offence that captures continuing unlawful activity by a syndicate to obtain pecuniary benefits, including forms of cyber-enabled conduct when executed through concert and structure. The section supplies an umbrella to plead participation where multiple actors run a scheme that uses VDAs for proceeds or operational facilitation, bridging gaps between predicate wrongs and the laundering layer. The language on extent and application also preserves extraterritorial cognizance tied to Indian interests and nationals, which allows domestic prosecution to reach conduct partly executed abroad but materially affecting India. This complements "PMLA" and "NDPS" predicates when the factual matrix shows coordinated crime using crypto rails.[6]

Typology[7]	Core conduct	Indicative statute and section	Primary agency nexus
Darknet narcotics sales with crypto payments	LSD, ketamine, synthetic distribution with wallet-based receipts	"NDPS Act" "Sections 20, 21, 27A, 29" + "PMLA Section 3" for laundering	NCB lead, ED for proceeds, State Police Cyber Cells
Exchange-centric laundering	Placement via low-KYC accounts, rapid VDA transfers, off-ramps	"PMLA Section 3" + "Maintenance of Records Rules" duties post "S.O. 1072(E)"	FIU-IND for supervision, ED for investigation
Mixer/bridge obfuscation	Cross-asset hopping, tumbler services	"PMLA Section 3" participation or facilitation; "BNS" organized crime where syndicate	ED, State Police, CERT-In technical support
Phishing and ransomware cash-out	Wallet inflows from cyber offences	"PMLA" + "Information Technology Act" predicates + "BNS" where syndicate shown	State cyber units, ED, CERT-In
Terror-finance stablecoin rails	Material support using USDT or equivalent	"UAPA Sections 17, 40" with "PMLA"	NIA where invoked, ED

Table 1: Crypto crime typologies in India with indicative statutes and agencies. Caption: "Typology to Statute and Agency Map"

Indian Legal Framework

The Indian framework has consolidated around four planks. First, AML coverage now expressly extends to VDA-facing services, reclassifying exchanges, custodians, and transfer facilitators as "reporting entities" with FIU-India obligations and exposure to blocking measures when non-compliant. Second, tax policy imposes non-trivial friction through a high rate and a TDS layer that broaden visibility for revenue and, indirectly, AML analysts. Third, technical regulation through CERT-In imposes short-fuse incident reporting, log retention, and subscriber validation across relevant intermediaries, including VASPs and custodial providers. Fourth, criminal law and evidence have been updated through the "BNS", "BNSS", and "BSA", providing an organized-crime anchor, procedural tools like audio-video recording of search and seizure, and a renewed electronic-evidence certificate regime aligned with the former "Section 65B" lineage.[8]

PMLA and VDAs

On 7 March 2023, the Central Government notified that activities such as exchange between VDAs and fiat, exchange between one or more forms of VDAs, transfer of VDAs, safekeeping or administration, and financial services related to a VDA offer and sale would fall within the "designated business or profession" limb of "Section 2(1) (sa)" of the "PMLA." This makes such actors "reporting entities", triggering registration with FIU-IND, KYC, record-keeping, and suspicious transaction reporting duties under the "PML (Maintenance of Records) Rules." FIU-IND has since issued sectoral materials and pursued actions, including show-cause notices and penalties against offshore platforms operating without registration, alongside directions to block URLs for persistent non-compliance. The legal effect is to convert crypto on- and off-ramps into supervised conduits, enabling STR pipelines and cooperation for freezing and seizure.[9]

Income Tax on VDAs

Tax law supplies both a definitional spine and a deterrent overlay. The "Finance Act, 2022" inserted "Section 2(47A)" into the Income-tax Act, defining "virtual digital asset", and "Section 115BBH", which levies a 30 percent tax on income from the transfer of any VDA with no deductions except cost of acquisition and no loss set-offs. The withholding rule "Section 194S" imposes a 1 percent TDS on consideration for VDA transfers above thresholds and requires payer-side compliance, creating information trails valuable to both tax and AML use-cases. Public materials and departmental tutorials have reinforced compliance posture and clarified mechanics. In enforcement narratives, tax data has begun to surface where arbitrage or bot-trading profits were undeclared, reinforcing the compliance ecosystem around AML supervision.[10]

---

[6] The Bharatiya Nyaya Sanhita, 2023, *available at:* https://www.indiacode.nic.in/bitstream/123456789/20062/1/a2023-45.pdf (last visited on October 21, 2025).

[7] Vakul Sharma, *Information Technology Law and Practice* 204 (Universal Law Publishing, Delhi, 1st edn., 2011).

[8] Notification S.O. 1072(E), March 7, 2023: Activities Related to Virtual Digital Assets Under PMLA, available at: https://egazette.gov.in/ WriteReadData/2023/244184.pdf (last visited on October 26, 2025).

[9] *Supra* note 8.

[10] Finance Bill, 2022, *available at:* https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf (last visited on October 28, 2025).

IT Act and CERT-In Directions

CERT-In's Directions of April 28, 2022, issued under "Section 70B (6) of the Information Technology Act, 2000", require, among others, six-hour cyber-incident reporting, 180-day log retention, and customer information validation by data centres, VPS providers, cloud and VPN providers, and explicitly, virtual asset service providers, virtual asset exchanges, and custodian wallet providers. FAQs and subsequent communications clarified scope and implementation timelines. For crypto actors, these directions intersect with AML by reducing anonymity at the infrastructure layer, improving traceability of access, and aligning time-bounds for reporting security incidents that can overlap with fraud or laundering campaigns involving VDA rails. The compliance footprint also engages privacy and data-governance discussions that interact with the "DPDP Act, 2023", particularly on purpose limitation and storage duration.[11]

BNS, BNSS and BSA

Substantive criminal law under the "BNS" incorporates an "organized crime" offence that can accommodate cyber-enabled syndicates, including those using VDAs to not only launder proceeds but also organize and facilitate primary offences. Procedure under the "BNSS" modernizes investigation, including mandatory recording of search and seizure through audio-video means in "Section 105", which strengthens chain-of-custody narratives for device and wallet seizures, and contains broader accommodations for electronic communication and technology-mediated investigation. Evidence law under the "BSA" continues the electronic evidence certification lineage: the statutory "certificate" is now set out in "Section 63" with a detailed Schedule prescribing contents, replacing the former "Section 65B" paradigm while keeping its functional logic. This continuity aids courts in assessing blockchain-derived records, exchange logs, and device outputs.[12]

NDPS and Dark Web Drug Trafficking

The "NDPS Act" remains the principal tool against darknet drug trafficking where payment and logistics leverage crypto and postal networks. Investigations have begun to integrate wallet analytics, exchange cooperation, and device forensics to link sales to specific actors, as illustrated in 2025 by NCB's Operation Melon against the "Ketamelon" syndicate, which reported seizures including LSD, ketamine, and cryptocurrency holdings and proceeded with coordinated custody and asset-freezing moves. In such cases, laundering theories under "PMLA" naturally attach to the narcotics predicates, while "BNS" organized crime framing can capture the structured, repeated coordination among vendors, packagers, and cash-out facilitators. The interplay demonstrates how narcotics and AML law converge on VDA-enabled ecosystems.[13]

UAPA and Terror Financing

For terror financing, "UAPA Section 17" punishes raising funds for terrorist acts, and "Section 40" addresses raising funds for terrorist organizations, with knowledge-based and suspicion-based standards that can fit stablecoin-mediated value movement when purpose and association are proved. Investigative agencies have flagged crypto rails as a policy risk for material support and fundraising, placing VASPs and exchanges within a broader prevention strategy coordinated with "PMLA" reporting. The doctrinal emphasis lies in translating wallet activity, exchange records, and communication evidence into the mental elements required by UAPA, while simultaneously preserving admissibility through "BSA" certificates and meeting procedural safeguards. Comparative FATF assessments and domestic practice underscore licensing, travel-rule alignment, and supervisory reach as levers to constrain terror-finance misuse.[14]

Instrument[15]	**Focus**	**Key provision(s) for VDAs/dark web**	**Procedural or supervisory hook**
"**PMLA**" **and** "**PML Rules**"	AML coverage for VASPs	"S.O. 1072(E)" brings VDA activities within "Section 2(1) (sa)" ambit	FIU-IND registration, STRs, records, blocking for non-compliance
Income-tax Act	Tax treatment and TDS	"Sections 2(47A), 115BBH, 194S"	Revenue visibility supports AML analytics
"**IT Act**" **and CERT-In**	Cyber incident reporting, logs, KYC-like validation	Directions dated 28.04.2022 under "Section 70B (6)"	6-HOUR Reporting, 180-DAY Logs, Subscriber Validation
"**BNS**"	Organized crime and cyber-adjacent offences	Organized crime offence and extraterritorial application clause	Substantive liability for syndicates
"**BNSS**"	Search, seizure, tech-enabled process	"Section 105" audio-video capture of search and seizure	Chain-of-custody reinforcement

[11] Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 25, 2025).

[12] *Supra* note 6.

[13] NCB Busts Top Darknet Drug Vendor Ketamelon in Operation Melon Seizure of LSD, Ketamine, and Cryptocurrency Worth Over ₹1 Crore, *available at:* https://narcoticsindia.nic.in/pressrelease/01_07_25_hq_cochin_darknet.pdf (last visited on October 20, 2025).

[14] Section 17: Punishment for Raising Funds for Terrorist Act Under the Unlawful Activities (Prevention) Act, 1967, *available at:* https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00001_196737_1517807318055&orderno=18 (last visited on October 19, 2025).

[15] Countering the Misuse of Virtual Assets & New Technologies to Finance Terrorism (UNOCT/CTED), *available at:* https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/uncct_cft_va_report_2024_en.pdf (last visited on October 27, 2025).

"**BSA**"	Admissibility of electronic evidence	"Section 63" certificate and Schedule	Continuity of 65B-type certification
"**NDPS Act**"	Narcotics predicates	"Sections 20, 21, 27A, 29"	ED attachment under "PMLA" for proceeds
"**UAPA**"	Terror financing predicates	"Sections 17, 40"	NIA investigations, coordination with FIU-IND

Table 2: Core Indian statutes and provisions relevant to VDAs and dark web offences. Caption: "Indian Statutory Framework on VDAs"

Doctrinal Bases for Criminal Liability

The contemporary Indian framework treats crypto-enabled wrongs as conduct-based offences anchored in statutory text that already exists, rather than as a self-contained new branch of crime. The doctrinal base rests on the coupling of "proceeds of crime" with specific conduct elements under "Section 3 of the Prevention of Money Laundering Act, 2002" where concealment, possession, acquisition, use, projecting as untainted, or claiming as untainted are each sufficient act. The "Bharatiya Nyaya Sanhita, 2023" classifies "organised crime" in "Section 111" and covers continuing unlawful activity by a syndicate, which can include cyber-facilitated revenue streams. The "Unlawful Activities (Prevention) Act, 1967" frames fundraising and material support in "Sections 17 and 40", and the "NDPS Act, 1985" targets financing in "Section 27A" tied to drug trafficking. In parallel, evidentiary doctrine under the "Bharatiya Sakshya Adhiniyam, 2023" preserves the electronic record certificate lineage in "Section 63" and its Schedule, which has operational consequences for blockchain analytics, exchange records, and on-chain attribution in court. The new procedure code, the "BNSS, 2023", shapes crypto seizure and documentation through "Section 105" audio-video recording of search and seizure. Read together, these enactments enable prosecutors to meet actus reus and mens rea thresholds even when value moves through wallets, mixers, and privacy tools.[16]

Actus Reus in VDA Offences

The actus reus analysis starts with the textual sweep of "Section 3 of the PMLA" that treats money-laundering as any attempt, assistance, participation, or actual involvement in processes connected with proceeds of crime, explicitly listing concealment, possession, acquisition, use, and presentation or claim as untainted. This breadth allows attribution to users who move tokens across chains, to OTC brokers who cash out stablecoins, and to exchange accounts used to layer or integrate, provided the value can be linked to a scheduled offence. Where narcotics are concerned, the "NDPS Act" creates separate conduct predicates in "Sections 27A and 29" for financing and conspiracy, enabling parallel or prior prosecutions while PMLA focuses on the laundering stage. Organised crime under the "BNS" in "Section 111" treats a continuing series of unlawful acts by a syndicate as the core conduct, which can encompass extortion proceeds routed through wallets or hawala-on-chain hybrids. Procedural acts such as seizure, imaging, and freezing form part of the chain of lawfully obtained evidence under the "BNSS" with "Section 105" mandating audio-video recording of the process, which courts may weigh when admitting electronic material under the "BSA" certificate pathway in "Section 63."[17]

Mens Rea and Knowledge Standards

Mens rea in crypto episodes often turns on knowledge of illicit provenance and risk awareness. The PMLA's formulation supports liability where a person "knowingly assists", "knowingly is a party", or is actually involved in covered processes, with the continuing nature clause extending culpability while the person enjoys the proceeds. Courts read such language to accommodate wilful blindness and reckless disregard, especially in settings where exchanges or OTC brokers ignore red flags in KYC, fail to verify source of funds, or permit layering without sanctions screening. CERT-In's 2022 directions require time-synced logs and data retention by VPS, VPNs, and exchanges, which narrow plausible deniability and allow post hoc mens rea inferences when logs reveal repeated evasion patterns. FATF's updates to Recommendation 15 describe risk-based expectations such as travel-rule compliance and controls for DeFi interfaces and P2P flows, which inform the standard of care that may be expected from VASPs supervised by FIU-IND. Where the evidence shows design features that enable evasion-by-default, prosecutors can argue aiding-by-design, particularly when transaction splitting, mixer integrations, or no-KYC tiers are built in despite clear supervisory guidance.[18]

Attribution to Platforms and Intermediaries

Attribution to an exchange, mixer, darknet marketplace operator, or a DeFi front-end can arise where the entity falls within "reporting entity" duties or engages in facilitation that constitutes participation in the laundering chain. The 7 March 2023 notification places VDA exchange, transfer, safekeeping, and related services within the PMLA's reporting entity ambit, linking FIU registration and rule-based obligations to VASP conduct. Failures can carry "Section 13 of the PMLA" consequences, seen in enforcement actions and penalties against offshore exchanges that catered to Indian users without registration or adequate controls. Liability may also flow through the organised crime route if a marketplace or operator functions as a syndicate instrument generating revenue by illegal sales where crypto is the medium. The "BNS Section 111" text captures continuing unlawful activity by a syndicate, allowing prosecutors to place platform operations within the definition if facts fit. Meanwhile, evidence admission hinges on proper "BSA Section 63"

[16] The Prevention of Money Laundering Act, 2002 (PMLA), *available at:* https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html (last visited on October 28, 2025).
[17] *Supra* note 16.
[18] *Supra* note 16.

certificates for server logs and wallet records, making compliance failures double-edged, both as substantive risk and as evidentiary vulnerability.[19]

Conspiracy, Abetment, and Common Intention

Crypto-enabled syndicates operate as layered networks of sellers, escrow handlers, mixers, money mules, and exchange accounts. Conspiracy and abetment doctrines map onto this structure by linking individual acts to a common design. Under the "NDPS Act Section 29", conspiracy liability supports charges against wallet custodians and logistics actors who enable narcotics commerce funded through tokens, while "BNS Section 111" captures the continuing unlawful activity binding the enterprise. The laundering stage invites "PMLA Section 3" participation and assistance theories, especially for OTC sellers cashing out stablecoins into cash couriers. UAPA's financing offences in "Section 17" support attachment when value flows are linked to designated groups or acts. The net doctrinal position recognises that mixers and privacy coins complicate attribution, but chain analytics, controlled deliveries, and sting-led wallet tracing bridge evidentiary gaps, provided investigators preserve logs and issue "BSA Section 63" certificates in the prescribed Schedule format. The syndicate's division of labour therefore does not immunise any actor whose conduct and knowledge align with the common plan.[20]

Extraterritoriality and Jurisdiction

Crypto crimes often span exchanges, cloud accounts, and service providers overseas. India's practice relies on effects-based reasoning coupled with Mutual Legal Assistance Treaty channels managed by the Ministry of Home Affairs as the Central Authority. India has not acceded to the Budapest Convention, which affects speed of cross-border evidence access and volatile data preservation, though new UN processes and bilateral arrangements can supplement. BNSS procedure governs domestic steps while letters rogatory and MLAT requests support foreign compulsion. Investigators should expect longer timelines for wallet KYC, server logs, and IP data when hosted abroad, which underscores prompt preservation requests and CERT-In aligned log retention by domestic intermediaries. Where overseas platforms target Indian users, "PMLA" registration expectations and blocking directives have been used to compel alignment or to justify domestic restraints, and penalties have followed registration shortfalls. This composite jurisdictional approach shows a preference for domestic levers, while continuing to pursue treaty and executive cooperation for encrypted or privacy-enhanced data.[21]

Enforcement Architecture and Procedure

India deploys a multi-agency model. FIU-IND supervises reporting entities under the PMLA maintenance of records rules, issues compliance orders, and has proceeded against offshore VASPs for non-registration. The Enforcement Directorate investigates laundering and attaches property. The Narcotics Control Bureau leads NDPS operations, including darknet cases with crypto seizures. State police cyber cells and the Indian Cyber Crime Coordination Centre handle first response, analytics, and portals. CERT-In issues technical directions for logs, time synchronisation, and incident reporting, which supports evidentiary continuity. The BNSS requires audio-video recording of search and seizure steps in "Section 105", which aligns with forensics and due process. Together these bodies build cases through chain analysis, exchange cooperation, and coordinated blocking or takedowns, often combined with MLAT requests to secure remote-hosted data.[22]

Agencies and Roles

FIU-IND's VASP supervisory role derives from the March 2023 notification and the broader PMLA scheme defining reporting entities. It issues orders under "Section 13 of the PMLA" and maintains compliance actions against entities including VASPs and financial firms. The ED exercises search, seizure, summons, and attachment powers under PMLA, while NCB spearheads darknet narcotics actions, as seen in Operation Melon with crypto seizures and vendor arrests. CERT-In's 2022 directions impose data retention and KYC-adjacent record keeping across intermediaries that often intersect with crypto infrastructure such as exchanges, VPS, and VPN services. State cyber cells, through I4C coordination, add threat analytics and training. The BNSS refines procedure and mandates recording of search-seizure events to strengthen evidentiary trails later certified under the BSA. This layered role allocation has recently been applied to off-shore exchange enforcement, culminating in penalties and registrations.[23]

Registration and Compliance Actions

The addition of VDA services to the PMLA reporting net set in motion a sequence of FIU-IND actions against offshore VASPs serving Indian customers without registration. Show-cause notices were issued in December 2023 and later waves involved blocking directions under the IT Act to prevent access to non-compliant platforms. Subsequent registrations by major exchanges followed, alongside penalties for past contraventions. This regulatory trajectory signals that access to the Indian market is conditioned on FIU registration, suspicious transaction reporting, travel-rule style information sharing, and

[19] *Supra* note 8.

[20] The Narcotic Drugs and Psychotropic Substances Act, 1985, *available at:* https://www.indiacode.nic.in/bitstream/123456789/18974/1/narcotic-drugs-and-psychotropic-substances-act-1985.pdf (last visited on October 27, 2025).

[21] Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory Mutual Legal Assistance Request and Service of Summons Notices Judicial Documents in Respect of Criminal Matters, *available at:* https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines_17122019%5B1%5D.pdf (last visited on October 26, 2025).

[22] Compliance Orders, *available at:* https://fiuindia.gov.in/files/Compliance_Orders/orders.html (last visited on October 25, 2025).

[23] *Supra* note 8.

record keeping. Non-compliance can trigger penalties, blocking, and attachment measures, and has already resulted in significant monetary orders and operational constraints for global platforms seeking to serve Indian users.[24]

Search, Seizure, Freezing of Crypto

Investigators rely on a blend of PMLA attachment and BNSS search-seizure powers to restrain or secure crypto assets. Wallets on exchanges can be frozen by directing the platform to restrict withdrawals while on-chain funds face seizure through key capture or device imaging. The BNSS mandate in "Section 105" to record search and seizure through audio-video tools provides a verifiable chain for recovery of seed phrases, hardware wallets, or cloud backups. ED press materials document exchange searches and freezing based on KYC and control findings. Where assets sit with offshore exchanges, FIU blocking and MLAT requests can be combined with domestic orders to preserve value. Across these steps, proper hashing, logging, and eventual "BSA Section 63" certification of electronic records creates the admissibility foundation in court.[25]

Procedural Safeguards

Safeguards have sharpened. Under PMLA "Section 19", arrests require communication of grounds. The Supreme Court in "*Pankaj Bansal v. Union of India*[26]" required furnishing written grounds of arrest, and later benches have discussed prospective application and related implications for pending matters. On the evidence side, the "BSA Section 63" certificate remains mandatory for secondary electronic evidence, following the lineage affirmed in "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[27]," and earlier in "*Anvar P.V. v. P.K. Basheer*[28]„. BNSS "Section 105" reduces contest over search and seizure accuracy by requiring audiovisual capture forwarded to the Magistrate. These safeguards recalibrate investigative practice in crypto cases by aligning chain-of-custody with due process expectations.[29]

Investigative power	**Statute-provision**	**Typical crypto use-case**	**Safeguard hook**	**Evidentiary anchor**
Provisional attachment	"PMLA Sections 5 and 8"	Freeze exchange wallets and banked exits	Furnish grounds if arrest, maintain records	"BSA Section 63" certificate for logs
Search and seizure	"BNSS Section 105"	Image devices, capture seed phrases	Audio-video recording and prompt forwarding	Hashes, recording, certificate
Exchange supervision	"PMLA notification 07.03.2023" and FIU orders	Registration, STRs, travel-rule style info	FIU show-cause and penalties	Audit logs and STR metadata
Darknet drug probes	"NDPS Sections 27A, 29"	Wallets tied to shipments	Judicial oversight under NDPS	Forensic reports with certificate

Table 3: Power and Safeguard Matrix[30]

Case Law Matrix

The jurisprudence frames banking access, AML architecture, arrest safeguards, and electronic evidence admissibility in ways that shape crypto enforcement. The banking access ruling countered blanket exclusion while leaving room for proportionate regulation. PMLA validity confirmed the backbone for FIU-ED actions. Arrest-ground rulings recalibrated practice and paperwork. Electronic evidence doctrine settled the certificate requirement now carried into the BSA. These holdings combine to validate an AML-first model while constraining procedure to guard against overreach, which affects investigations into darknet drug markets, mixer-linked laundering, and offshore VASP non-compliance, including operations where seizures of tokens and exchange logs occur.[31]

Internet and Mobile Association of India v. Reserve Bank of India

In the case of "*Internet and Mobile Association of India v. Reserve Bank of India*[32]", the Supreme Court examined the legality of RBI's circular that had directed entities regulated by RBI not to deal in or provide services for any person or business dealing with virtual currencies. The petitioners argued that the central bank had adopted a measure that effectively shut down crypto business access to banking, despite the absence of a statutory ban, and without

[24] Financial Intelligence Unit India Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers, *available at:* https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372 (last visited on October 24, 2025).

[25] 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 23, 2025).

[26] 2023 SCC OnLine SC 1244

[27] (2020) 7 SCC 1

[28] (2014) 10 SCC 473

[29] Pankaj Bansal v. Union of India, Judgment, *available at:* https://cjp.org.in/wp-content/uploads/2024/06/PANKAJ-BANSAL-SLP-Crl-9275-76-2023-SC-Judgement-03-Oct-2023.pdf (last visited on October 22, 2025).

[30] Landmark Judgments on PMLA — Procedural Safeguards (SCC Online Blog), *available at:* https://www.scconline.com/blog/post/2024/07/15/landmark-judgments-on-pmla-by-supreme-court-and-high-courts-2023-2/ (last visited on October 20, 2025).

[31] Internet and Mobile Association of India v. Reserve Bank of India, Judgment, *available at:* https://www.livelaw.in/pdf_upload/pdf_upload-370875.pdf (last visited on October 21, 2025).

[32] (2020) 10 SCC 274

a proportionate basis in evidence of harm. The Court traced the factual record including stakeholder submissions, RBI affidavits, and the nature of crypto markets in India. It noted the lack of empirical harm to RBI-regulated entities from the operations of crypto exchanges and identified the availability of less restrictive means. The Court applied proportionality review to test whether the circular was suitable, necessary, and balanced against rights. It concluded that the measure failed the necessity and balancing steps because it imposed a near-total banking exclusion without adequate evidence of actual harm to the financial system. The judgment set aside the circular, while recognising RBI's power to regulate and the State's authority to legislate. The effect was to reopen banking rails to crypto businesses, subject to future lawful and proportionate measures. This holding did not confer legality on crypto per se, but it removed a blanket barrier and signalled that risk-based regulation would be assessed for rationality and evidentiary basis rather than mere policy preference.[33]

Vijay Madanlal Choudhary v. Union of India

In the case of "*Vijay Madanlal Choudhary v. Union of India*[34]," the Supreme Court upheld core elements of the PMLA framework, including the offence definition in "Section 3", attachment and confiscation powers, and twin conditions for bail after legislative cure post "Nikesh Tarachand Shah". The Court treated money-laundering as a distinct offence that attaches to the process dealing with proceeds of crime and stressed the continuing nature of the crime until enjoyment of the property ceases. Petitioners challenged ED's powers and procedural departures from the Code, but the Court sustained the special procedure due to the gravity of laundering and its international obligations. The judgment's validation of the architecture has underpinned subsequent FIU-IND and ED initiatives in crypto-linked matters, including exchange-facing actions, wallet freezing, and seizure of digital assets as property involved in laundering. A partial review on certain aspects was later noted as pending, but the doctrinal spine remains. For the crypto context, the ruling affirms that value represented in tokens can count as property in the laundering chain, and that attachment and investigative steps are legitimate provided statutory conditions are met. The decision positions PMLA as the principal AML law whose standards govern the interface between VDAs, proceeds of crime, and prosecutorial conduct in India.[35]

Pankaj Bansal v. Union of India

In the case of "*Pankaj Bansal v. Union of India*[36]", the Supreme Court held that the Enforcement Directorate must provide a copy of the written grounds of arrest to the arrestee under "Section 19 of the PMLA". The Court reasoned that written communication enhances procedural fairness and enables meaningful challenge to arrest and remand, going beyond oral intimation. Subsequent benches have considered the temporal reach of this requirement, with some rulings and arguments on prospectivity or application to earlier arrests. The doctrine, though, has already reshaped AML arrests by formalising a documentary threshold, which has immediate consequences for crypto probes where arrests accompany searches and digital seizures. The ruling emphasises that special statute powers coexist with constitutional benchmarks. In AML matters built on complex electronic trails, the ability of the accused to know the precise grounds promotes contest on attribution, knowledge, and proceeds link. That in turn improves the quality of investigation and the admissibility posture, because agencies must align case files, grounds, and "BSA Section 63" certificates, forming a coherent record.[37]

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal

In the case of "*Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*[38]", the Supreme Court authoritatively reaffirmed that a "Section 65B" certificate (now succeeded in substance by the "BSA Section 63" framework) is mandatory for admitting secondary electronic evidence. The Court disapproved a relaxed "substantial compliance" approach and clarified that the certificate must accompany the electronic record to establish the conditions of lawful production. This holding, when read with the BSA's Schedule certificate template, structures the prosecution's approach to blockchain analytics exports, exchange CSVs, server logs, and cloud backups. For crypto cases, it avoids uncertainty about admissibility by directing investigators to plan certificate generation around the originating system. Where originators are overseas, MLAT requests and platform attestations become relevant. Courts will assess whether the certificate identifies the device or system, the manner of production, and integrity checks such as hash values. The doctrinal clarity has led to better-aligned evidence packages in crypto-linked laundering and NDPS prosecutions that rely on digital trails from wallets, order books, and IP activity.[39]

Anvar P.V. v. P.K. Basheer

In the case of "*Anvar P.V. v. P.K. Basheer*[40]", the Supreme Court shifted Indian evidence law toward a strict statutory pathway for electronic records by requiring the "Section 65B" certificate for admissibility, rejecting prior doctrines that allowed admission on oral proof or general evidence rules. This

---

[33] *Supra* note 28.

[34] 2022 SCC OnLine SC 929

[35] Vijay Madanlal Choudhary and Others v. Union of India and Others, Judgment, *available at:* https://api.sci.gov.in/supremecourt/2014/19062/19062_2014_3_1501_36844_Judgement_27-Jul-2022.pdf (last visited on October 20, 2025).

[36] 2023 SCC OnLine SC 1244

[37] *Supra* note 26.

[38] (2020) 7 SCC 1

[39] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Others, Judgment, *available at:* https://aphc.gov.in/docs/imp_judgements/Arjun Panditrao Khotkar _ Kailash Kushanrao Gorantyal And Ors._1701334263.pdf (last visited on October 19, 2025).

[40] (2014) 10 SCC 473

holding laid the foundation that "Arjun Panditrao" later reaffirmed. Its significance for crypto litigation is practical. Wallet exports, exchange logs, and analytics charts are secondary copies unless the original system output is certified. The requirement imposes discipline on investigators to obtain origin-system certifications or to structure controlled captures that can be certified by the officer in control of the system. In narcotics and PMLA cases that hinge on WhatsApp chats, wallet screenshots, or CSV exports, the doctrine prevents evidentiary shortcuts that would risk exclusion. The BSA has carried forward this certificate architecture in "Section 63" and its Schedule, confirming that crypto-era prosecutions must document provenance and integrity to cross the threshold of admissibility.[41]

NCB Operation Melon Press Release, 1 July 2025"

In the case of "NCB Operation Melon Press Release, 1 July 2025", the agency reported the takedown of a top darknet vendor known as Ketamelon following parcel interceptions and coordinated searches by the Cochin Zonal Unit. The release describes seizures of LSD and ketamine along with digital assets valued in tens of lakhs, while confirming that postal interceptions tied the parcels to the suspect. Subsequent operations, as reported, involved tracing wallets, coordinating with a large global exchange, and freezing value linked to the proceeds stream. The reported outcome shows how NDPS and AML tools converge in darknet cases where tokens serve as the medium of exchange, with crypto seizure complementing drug seizures to prevent reinvestment. While not binding precedent, the press record demonstrates contemporary investigative practice combining chain analysis, exchange cooperation, and traditional controlled deliveries. It provides a ground-level documentary snapshot of how doctrinal elements operate together in a real case.[42]

Theme	Case	Doctrinal takeaway for crypto
Banking access	"IAMAI v. RBI"	Proportionality review of sector-wide restrictions
AML backbone	"Vijay Madanlal Choudhary"	Validates PMLA architecture used in crypto probes
Arrest safeguards	"Pankaj Bansal"	Written grounds of arrest required
E-evidence	"Arjun Panditrao"; "Anvar P.V."	Certificate is mandatory for secondary e-evidence

Table 4: From Banking Access to AML Enforcement[43]

Comparative and International Norms

Global standards guide domestic calibration. FATF's 2019 extension of "Recommendation 15" to virtual assets and VASPs created the baseline for licensing or registration, customer due diligence, suspicious transaction reporting, and the travel rule. Guidance in 2021 and targeted updates in 2023 and 2024 called out DeFi front-ends, NFTs, stablecoins, and P2P risks while urging supervision and enforcement. India's trajectory shows registration of VASPs with FIU-IND and penalties for non-compliance. Yet FATF's monitoring notes continuing implementation gaps worldwide, including patchy travel rule compliance and supervision. For cross-border cooperation, India relies on MLATs and growing bilateral instruments rather than the Budapest Convention, while the new UN cybercrime convention aims to establish broader cooperation pathways. These reference points justify a compliance-first domestic stance and explain procedural frictions in obtaining extraterritorial data.[44]

FATF Standards on Virtual Assets

FATF's 2019 revisions brought VAs and VASPs under AML/CFT rules with an interpretative note to "Recommendation 15". Subsequent guidance clarified the travel rule's application, treatment of unhosted wallets, DeFi interfaces, and stablecoin risks. The 2023 and 2024 targeted updates tracked slow but improving adoption, noting that many jurisdictions still lack active supervision, and DeFi/P2P abuses remain in focus. These texts influence national supervisors, including FIU-IND, in expecting VASPs to collect and transmit originator and beneficiary data, to identify counterparty VASPs, and to document risk assessments. For India's doctrine, FATF's emphasis shapes the standard of care in negligence and wilful blindness analysis when exchanges fail to adopt travel-rule style solutions despite serving cross-border flows.[45]

India's Alignment Status

India has moved from observation to supervision by formally placing VASPs within the PMLA reporting perimeter and requiring FIU registration. Enforcement against offshore exchanges led to blocking steps and later registrations, alongside monetary penalties for past non-compliance. FATF updates recognise progress but continue to highlight implementation deficits worldwide, which implies that supervisory maturation will continue with more granular inspections, STR analytics, and outcomes-based testing. The compliance landscape shows VASPs adjusting systems for data capture, KYC tightness, and case management to meet FIU expectations. This arc indicates a practical convergence with FATF, while acknowledging resource and data-transfer frictions that accompany cross-border crypto trading and custody relationships.[46]

---

[41] Anvar P. V. v. P. K. Basheer, Judgment, *available at:* https://aphc.gov.in/docs/imp_judgements/Anvar PV case.pdf (last visited on October 28, 2025).
[42] *Supra* note 13.
[43] Operation Melon: Pan-India Darknet Drug Bust — Press Release, *available at:* https://narcoticsindia.nic.in (last visited on October 24, 2025).
[44] The FATF Recommendations, *available at:* https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (last visited on October 27, 2025).
[45] *Supra* note 36.
[46] *Supra* note 8.

Cooperation Instruments

India's cooperation rests on MLAT practice under the MHA's Comprehensive Guidelines, letters rogatory through courts, and bilateral understandings. Non-accession to the Budapest Convention affects access to expedited channels available to parties under its 24x7 network and expedited data preservation tools, although India engages with UN processes for a broader convention. In crypto cases, timely preservation letters to exchanges and cloud providers remain critical, paired with domestic blocking orders where needed. The foreseeable path involves deeper bilateral MOUs with key service-provider jurisdictions and more predictable turnaround times for subscriber data, KYC files, and server logs to meet "BSA Section 63" certification standards.[47]

FATF expectation	Indian measure	Status signal
VASP licensing or registration	FIU-IND registration under PMLA notification 07.03.2023	Operational and expanding
Travel rule compliance	FIU supervision and enforcement trajectory	Developing with penalties
DeFi and P2P risk control	Risk-based expectations, exchange actions and blocking	Evolving under updates

Table 5: R.15 Compliance Snapshot[48]

Liability Mapping Across Offence Clusters

The liability grid aligns conduct, mens rea, statutes, and evidence. Laundering via exchanges and mixers tests knowledge and reporting failures. Darknet drug cases join NDPS trafficking predicates with PMLA laundering steps. Terror financing adds UAPA thresholds and asset freezing. Tax non-compliance intersects with 30 percent tax on transfers and 1 percent TDS rules, where evasion can aggravate laundering suspicions if proceeds are linked to scheduled offences. Across clusters, admissibility pivots on "BSA Section 63" certification, while procedure relies on "BNSS Section 105" recordings and FIU log retention expectations reflected in CERT-In directions. Courts will ask whether the platform or actor knew or should have known based on risk indicators, supervisory guidance, and repeated circumvention patterns.[49]

Money Laundering Via Exchanges and Mixers

Negligence becomes facilitation when exchange controls ignore obvious red flags such as mule clusters, sanction-hits, or mixer exposure without enhanced checks. Under "PMLA Section 3", knowingly assisting or being a party to laundering can attach to staff, OTC partners, or corporate actors where internal rules are a façade. FIU-IND actions and penalties against offshore exchanges for operating without registration underscore the baseline duty to monitor and report. FATF travel rule expectations supply a benchmark for what responsible VASPs should capture and share in cross-border flows. Evidence will draw on exchange logs, STRs, chain analytics, and communications, each supported by a "BSA Section 63" certificate. The inquiry asks whether the platform's design and practice made laundering easier despite supervisory clarity.[50]

Darknet Drug Trafficking and NDPS Nexus

The NDPS framework treats financing and conspiracy as distinct offences in "Sections 27A and 29". When crypto wallets are linked to shipments through controlled deliveries, postal interceptions, and order trail mapping, prosecutors can show the trafficking act and the financial facilitation. PMLA adds the laundering stage by tying proceeds to the scheduled predicate. Operation-level materials illustrate how postal seizures, wallet tracing, and exchange cooperation converge to freeze value and arrest actors behind vendor handles. Admissibility depends on capturing chats, wallets, and CSVs with proper certification, while BNSS recordings of search and seizure reduce factual contests over device recovery and key capture. This cluster treats tokens as instruments of payment whose traceability overcomes anonymity claims.[51]

Terror Financing Risks and UAPA

UAPA "Section 17" penalises raising funds for terrorist acts, while "Section 40" addresses raising funds for a terrorist organisation. Stablecoins or USDT used for crowdfunding can fall within these provisions when linked to designated groups or acts, with PMLA supporting attachment as proceeds of crime where the laundering chain is established. FATF's risk articulation on stablecoins and P2P flows informs investigative priorities around exchange on-ramps, OTC brokers, and messaging channels. Evidence will include wallet clustering, exchange KYC, and remittance links, again subject to "BSA Section 63" certification and BNSS process recording. The legal threshold focuses on purpose or knowledge that funds support terrorist activity or organisations, which can be inferred from patterns of transfers, public solicitations, and communication records.[52]

---

[47] *Supra* note 21.

[48] Mutual Legal Assistance Treaty Between India and the United States (Full Text), *available at:* https://www.mea.gov.in/Portal/LegalTreatiesDoc/US01B0634-1-1.pdf (last visited on October 21, 2025).

[49] *Supra* note 2.

[50] Jaspreet Kalra, "India Financial Watchdog Imposes $2.25 Million Penalty on Crypto Exchange Binance", *available at:* https://www.reuters.com/business/finance/india-financial-watchdog-imposes-225-million-penalty-binance-2024-06-20/ (last visited on October 26, 2025).

[51] *Supra* note 20.

[52] The Unlawful Activities (Prevention) Act, 1967, *available at:* https://www.mha.gov.in/sites/default/files/A1967-37.pdf (last visited on October 25, 2025).

Tax Non-Compliance and Predicate Offences

The income tax regime imposes a 30 percent tax on VDA transfers under "Section 115BBH" without set off of losses, and a 1 percent TDS under "Section 194S" above specified thresholds. Non-compliance can trigger independent tax proceedings and feed AML suspicions where undisclosed trading resembles laundering of criminal proceeds, though tax evasion itself is not an automatic laundering predicate without a scheduled offence nexus. The definitional core of VDA in "Section 2(47A)" clarifies the tax perimeter while CBDT notifications refine NFTs and exclusions. In the crypto context, repeated TDS evasion and off-book cash-outs alongside other offences may support ED's parallel action. Evidence will involve exchange statements, broker records, and bank trails, preserved and certified for admissibility.[53]

Conduct	Primary statute	Mental element	Key evidence
Exchange-assisted layering	"PMLA Section 3"	Knowledge or wilful blindness	Logs, STRs, KYC, chain analytics, certificate
Darknet drug sales	"NDPS Sections 27A, 29" plus "PMLA Section 3"	Conspiracy, financing, participation	Parcels, chats, wallet links, certificate
Terror fundraising	"UAPA Sections 17, 40" and "PMLA"	Purpose or knowledge	Wallet clustering, on-ramp KYC, messages
Tax shortfall with criminal nexus	"Sections 115BBH, 194S" and "PMLA" if scheduled offence	Intent to evade coupled with predicate	Exchange and bank records, TDS data

Table 6: Doctrinal Liability Grid[54]

Evidence and Procedure in Crypto Cases

The evidence law posture in India expects disciplined digital forensics. The BSA entrenches the certificate requirement in "Section 63" with a prescribed Schedule format that demands identification of the device or system, the manner of production, and integrity checks. CERT-In directions strengthen time-stamping and log retention practices across relevant service classes. BNSS "Section 105" requires audio-video recording of search and seizure, improving the reliability of device imaging, seed phrase capture, and cloud credential recovery. MLAT practice and letters rogatory remain critical for overseas servers and exchange KYC, which should be anticipated early with preservation requests. Courts will test provenance, continuity, and integrity before weighing probative value, which implies planning certificates and recordings from the outset.[55]

Electronic Evidence under BSA

The BSA continues the evidentiary lineage of the earlier "Section 65B" by prescribing "Section 63" with a detailed Schedule certificate. Certificates must identify the electronic record, describe production, and state particulars of the device and integrity steps. In practice, blockchain exports, exchange CSVs, server logs, and IP data require either an origin-system certificate or a lawful copy with a custodian certificate. The certificate format in the BSA Schedule shapes drafting, while the holdings in "Anvar P.V." and "Arjun Panditrao" underscore the mandatory nature of certification for admissibility. Agencies therefore design collection plans around origin systems and involve exchange custodians early so that MLAT-delivered records arrive with compliant attestations.[56]

Wallet Seizure and Forensics

Investigations prioritise control over private keys and recovery of seed phrases. During searches, teams image devices, seize hardware wallets, and secure cloud backups by capturing authenticator data. BNSS "Section 105" requires audio-video recording of these steps and transmission to the Magistrate, which assists in rebutting later claims of tampering or coercion. CERT-In's directions on clock synchronisation and log retention help align event timelines across systems. For exchange-held assets, restraint orders to VASPs rely on PMLA proceedings and cooperative protocols. Chain analytics link addresses and identify mixers or cross-chain bridges used for obfuscation. All exported artefacts should be hashed and later covered by "BSA Section 63" certificates from custodians or investigators, establishing admissibility and integrity in court.[57]

Cross Border Data and MLATs

Time sensitivity defines cross-border evidence. The MHA's Comprehensive Guidelines clarify the Central Authority process for MLAT requests and letters rogatory, including formats and required annexures. India's non-accession to the Budapest Convention limits access to some expedited preservation tools, so investigators often deploy preservation letters to service providers while MLAT drafting proceeds. Emerging UN treaty processes and bilateral

[53] *Supra* note 2.

[54] Is Tax Evasion a Predicate Offence Under PMLA? — ICLG: Anti-Money Laundering (India), *available at:* https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/india (last visited on October 27, 2025).

[55] The Schedule [See Section 63(4)(c)] Certificate, *available at:* https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163 (last visited on October 24, 2025).

[56] *Supra* note 47.

[57] *Supra* note 25.

MOUs can improve timelines, but present practice still requires early action and clarity on jurisdiction. For crypto records, requests should specify wallet addresses, transaction hashes, and KYC identifiers to avoid overbroad fishing. Once received, records must be secured with proper certificates and integrated into the BNSS search-seizure record.[58]

Evidence source[59]	**Capture step**	**Admissibility step**
Exchange logs and KYC	MLAT or direct custodian export	"BSA Section 63" certificate from custodian
On-chain analytics exports	Investigator-controlled export with hashing	Investigator certificate referencing system and hash
Device images and keys	BNSS "Section 105" recorded seizure and imaging	Hash report plus certificate integrating recording

Table 7: From Hashes to Certificates

Conclusion

The nexus between dark web markets, digital assets, and organised crime shows how quickly criminal enterprise adapts to programmable value. Indian law does not leave a vacuum. The "PMLA Section 3" offence captures laundering processes involving crypto-denominated proceeds. The "BNS Section 111" organised crime text recognises syndicate structures using VDAs to collect and move revenue. The "NDPS Act Sections 27A and 29" and "UAPA Sections 17 and 40" address financing for drugs and terror respectively, while tax law codifies the 30 percent rate and 1 percent TDS in "Sections 115BBH and 194S" to narrow off-book channels. Procedure and evidence have modernised through "BNSS Section 105" audio-video recording and the "BSA Section 63" certificate. Enforcement practice demonstrates coordination across FIU-IND, ED, NCB, CERT-In, and state cyber cells, with offshore exchanges moving toward registration and penalties for gaps. FATF's Recommendation 15 sets the direction for licensing, travel rule, and DeFi-P2P risk management that informs domestic supervisory expectations. Reform should focus on codifying clear travel-rule obligations in subordinate legislation, accelerating bilateral data-sharing instruments, and developing uniform SOPs for wallet restraint and seed recovery aligned with BNSS recording. A measured approach to platform attribution that distinguishes negligence from design-level facilitation will support principled prosecutions without chilling lawful activity. The emerging doctrinal picture is a coherent one: crypto is a medium, not a sanctuary, and Indian criminal law already supplies the tools to trace, restrain, and prosecute when the facts and certified evidence meet the statutory tests.[60]

Bibliography

Books:

- Jamie Bartlett, The Dark Net (William Heinemann, London, 1st edn., 2014).
- Vakul Sharma, Information Technology Law and Practice (Universal Law Publishing, Delhi, 1st edn., 2011).

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 Finance Act, 2022 (Act No. 6 of 2022)
- The Income-tax Act, 1961 (Act No. 43 of 1961)
- 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)
- The Unlawful Activities (Prevention) Act, 1967 (Act No. 37 of 1967)

Websites:

- Anvar P. V. v. P. K. Basheer, Judgment, available at: https://aphc.gov.in/docs/imp_judgements/Anvar PV case.pdf (last visited on October 28, 2025).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Others, Judgment, available at: https://aphc.gov.in/docs/imp_judgements/Arjun Panditrao Khotkar _ Kailash Kushanrao Gorantyal And Ors._1701334263.pdf (last visited on October 19, 2025).
- BNS Section 111 Organised Crime, available at: https://devgan.in/bns/section/111/ (last visited on October 24, 2025).
- Compliance Orders, available at: https://fiuindia.gov.in/files/Compliance_Orders/orders.html (last visited on October 25, 2025).
- Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory Mutual Legal Assistance Request and Service of Summons Notices Judicial Documents in Respect of Criminal Matters, available at: https://www.mha.gov.in/sites/default/files/2022-08/ISII_ComprehensiveGuidelines_17122019%5B1%5D.pdf (last visited on October 26, 2025).
- Countering the Misuse of Virtual Assets & New Technologies to Finance Terrorism (UNOCT/CTED), available at: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/uncct_cft_va_report_2024_en.pdf (last visited on October 27, 2025).
- Directions Under Sub-Section (6) of Section 70B of the Information Technology Act, 2000 Relating to Information Security Practices, Procedure, Prevention, Response and Reporting of Cyber Incidents for Safe & Trusted Internet, available at: https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (last visited on October 25, 2025).

[58] *Supra* note 21.

[59] Mutual Legal Assistance Treaties — Ministry of External Affairs (Overview), *available at:* https://www.mea.gov.in/cpv-mlat-menu.htm (last visited on October 25, 2025).

[60] *Supra* note 16.

- Finance Bill, 2022, available at: https://www.indiabudget.gov.in/budget2022-23/doc/Finance_Bill.pdf (last visited on October 28, 2025).
- Financial Intelligence Unit India Issues Compliance Show Cause Notices to Nine Offshore Virtual Digital Assets Service Providers, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=1991372 (last visited on October 24, 2025).
- Government Notifies Amendments to Rule 3(1)(d) of the IT Rules, 2021, available at: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2181719 (last visited on October 27, 2025).
- Internet and Mobile Association of India v. Reserve Bank of India, Judgment, available at: https://www.livelaw.in/pdf_upload/pdf_upload-370875.pdf (last visited on October 21, 2025).
- Is Tax Evasion a Predicate Offence Under PMLA? - ICLG: Anti-Money Laundering (India), available at: https://iclg.com/practice-areas/anti-money-laundering-laws-and-regulations/india (last visited on October 27, 2025).
- Jaspreet Kalra, "India Financial Watchdog Imposes $2.25 Million Penalty on Crypto Exchange Binance", available at: https://www.reuters.com/business/finance/india-financial-watchdog-imposes-225-million-penalty-binance-2024-06-20/ (last visited on October 26, 2025).
- Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, available at: https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace (last visited on October 22, 2025).
- Landmark Judgments on PMLA - Procedural Safeguards (SCC Online Blog), available at: https://www.scconline.com/blog/post/2024/07/15/landmark-judgments-on-pmla-by-supreme-court-and-high-courts-2023-2/ (last visited on October 20, 2025).
- Mutual Legal Assistance Treaties - Ministry of External Affairs (Overview), available at: https://www.mea.gov.in/cpv-mlat-menu.htm (last visited on October 25, 2025).
- Mutual Legal Assistance Treaty Between India and the United States (Full Text), available at: https://www.mea.gov.in/Portal/LegalTreatiesDoc/US01B0634-1-1.pdf (last visited on October 21, 2025).
- NCB Busts Top Darknet Drug Vendor Ketamelon in Operation Melon Seizure of LSD, Ketamine, and Cryptocurrency Worth Over ₹1 Crore, available at: https://narcoticsindia.nic.in/pressrelease/01_07_25_hq_cochin_darknet.pdf (last visited on October 20, 2025).
- Notification No. 75/2022: Specification of Non-Fungible Token as Virtual Digital Asset, available at: https://incometaxindia.gov.in/communications/notification/notification-no-75-2022.pdf (last visited on October 23, 2025).
- Notification S.O. 1072(E), March 7, 2023: Activities Related to Virtual Digital Assets Under PMLA, available at: https://egazette.gov.in/WriteReadData/2023/244184.pdf (last visited on October 26, 2025).
- Operation Melon: Pan-India Darknet Drug Bust - Press Release, available at: https://narcoticsindia.nic.in (last visited on October 24, 2025).
- Pankaj Bansal v. Union of India, Judgment, available at: https://cjp.org.in/wp-content/uploads/2024/06/PANKAJ-BANSAL-SLP-Crl-9275-76-2023-SC-Judgement-03-Oct-2023.pdf (last visited on October 22, 2025).
- Section 17: Punishment for Raising Funds for Terrorist Act Under the Unlawful Activities (Prevention) Act, 1967, available at: https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00001_196737_1517807318055&orderno=18 (last visited on October 19, 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 23, 2025).
- The Bharatiya Nyaya Sanhita, 2023, available at: https://www.indiacode.nic.in/bitstream/123456789/20062/1/a2023-45.pdf (last visited on October 21, 2025).
- The FATF Recommendations, available at: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html (last visited on October 27, 2025).
- The Income-Tax Act, 1961, available at: https://incometaxindia.gov.in/Acts/Income-tax Act%2C 1961/2024_1/102120000000081156.htm (last visited on October 27, 2025).
- The Narcotic Drugs and Psychotropic Substances Act, 1985, available at: https://www.indiacode.nic.in/bitstream/123456789/18974/1/narcotic-drugs-and-psychotropic-substances-act-1985.pdf (last visited on October 27, 2025).
- The Prevention of Money Laundering Act, 2002 (PMLA), available at: https://fiuindia.gov.in/files/AML_Legislation/pmla_2002.html (last visited on October 28, 2025).
- The Schedule [See Section 63(4)(c)] Certificate, available at: https://upload.indiacode.nic.in/schedulefile?aid=AC_CEN_5_23_00049_2023-47_1719292804654&rid=1163 (last visited on October 24, 2025).
- The Unlawful Activities (Prevention) Act, 1967, available at: https://www.mha.gov.in/sites/default/files/A1967-37.pdf (last visited on October 25, 2025).
- Updated Guidance: FATF Recommendation 15 - Virtual Assets, available at: https://www.fatf-gafi.org/en/publications/Guidance/Guidance-va-vaps.html (last visited on October 23, 2025).
- Vijay Madanlal Choudhary and Others v. Union of India and Others, Judgment, available at: https://api.sci.gov.in/supremecourt/2014/19062/19062_2014_3_1501_36844_Judgement_27-Jul-2022.pdf (last visited on October 20, 2025).