Page 1149 - 1171

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Dark Web Narcotics Markets and the Evidentiary Crisis under the NDPS Act

APARNA M P*

ABSTRACT

Dark web narcotics markets are posing serious challenges to conventional narcotics investigation. The availability of anonymising networks such as The Onion Router (Tor) and the use of decentralised cryptocurrency have produced a major shift in the international drug trade. In India this has generated an evidentiary crisis in the enforcement of the Narcotic Drugs and Psychotropic Substances Act, 1985, a statute drafted to disrupt the operations of physical trafficking networks; read with the law of evidence and the Information Technology Act, 2000, it can no longer keep pace with the investigations that cyber-narcotics cases require. This doctrinal paper examines the conflict between the decentralised character of dark web drug distribution and the exacting procedural demands of Indian criminal law. Its central problem is the difficulty of gathering and validating evidence at the investigative and prosecution stages: attributing encrypted digital identifiers to physical suspects, satisfying the demanding requirements for the admissibility of electronic records, tracing cryptocurrency flows, working across jurisdictions, and maintaining an unbroken chain of custody for digital evidence. The paper examines recent case law, in particular Tofan Singh v. State of Tamil Nadu, as evidence of a genuine tension between strict evidentiary rules that protect constitutional freedoms and guard against investigative abuse, and the equally pressing need to bring technologically sophisticated trafficking networks to justice. That analysis is supported by comparison with cyber-narcotics practice in other jurisdictions, including United States federal enforcement and Europol-coordinated operations in Europe, in order to generate workable proposals for India. The paper concludes that to counter dark web drug networks India must modernise its criminal procedure to address the particular features of investigating and prosecuting cyber-narcotics offences. The specific reforms proposed are the creation of specialised cyber-narcotics investigation units, clearer rules on digital evidence under the NDPS Act, and stronger cooperation among law enforcement agencies at the local, national and international levels. Reconciling enforcement objectives with the principles of procedural fairness offers a coherent route to an effective and constitutionally sound legal framework for this new wave of trafficking.

* Author is an LL.M. Graduate from Maharashtra National Law University, Mumbai, Maharashtra, India.

 [ISSN 2581-5369]

Keywords: *NDPS Act, dark web narcotics, digital evidence admissibility, criminal procedure, cyber-narcotics, cryptocurrency tracing, chain of custody*

I. INTRODUCTION

The trade in narcotic drugs and psychotropic substances has undergone a structural change in the first decades of the twenty-first century. What was once rooted in physical geography, defined by border crossings, illicit warehouses and face-to-face transactions, has migrated at an accelerating pace into the anonymised space of the internet. Dark web narcotics markets, first demonstrated in practice by Silk Road between 2011 and its closure in 2013,[1] are not merely a new route for an existing trade; they are a fundamentally new mode of organising crime, one designed to defeat the investigative strategies with which drug enforcement agencies have traditionally operated. India is no exception to this trend: reporting by the Narcotics Control Bureau and intelligence estimates placed in the public domain through parliamentary processes record an increase in trafficking through online networks, including synthetic drugs, diverted pharmaceutical opioids and new psychoactive substances.[2]

This bears directly and acutely on Indian narcotics law. The Narcotic Drugs and Psychotropic Substances Act, 1985 (hereinafter the NDPS Act)[3] was enacted against a background of physical evidence: drugs found on a person or on premises, statements made to authorised officers, and the chemical examination of the substance recovered. Its procedural architecture, including the strict conditions governing search and seizure in Sections 41 to 43, the presumptions in Sections 35 and 54, and the restricted status of statements made to investigating officers as clarified by the Supreme Court in *Tofan Singh v. State of Tamil Nadu*,[4] presupposes a real-world evidentiary universe. A dark web investigation turns that universe upside down. The evidence is digital, frequently encrypted, and stored on servers in a foreign jurisdiction. The accused need never touch the substance handed over. The record of the transaction sits on a decentralised blockchain rather than in a ledger amenable to legal process in India.

The research question with which this paper is concerned is the structural disparity between the evidence that dark web investigations generate and the evidentiary criteria that the NDPS Act,

[1] *United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).
[2] NARCOTICS CONTROL BUREAU, MINISTRY OF HOME AFFAIRS, GOV'T OF INDIA, ANNUAL REPORT 2022, at 45 (2023).
[3] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, INDIA CODE (1985).
[4] *Tofan Singh v. State of Tamil Nadu*, (2021) 4 S.C.C. 1 (India).

 [ISSN 2581-5369]

the law of evidence and the law of criminal procedure[5] require prosecutors to satisfy in court. This disjunction, which the paper describes as an evidentiary crisis, operates at several levels: establishing who the real offender behind a pseudonym is (the attribution problem); establishing the admissibility and authenticity of electronic records under Sections 65A and 65B of the Evidence Act;[6] establishing the traceability of cryptocurrency transactions in the absence of any statutory framework for the seizure of digital assets; resolving questions of jurisdiction; and preserving the integrity of the chain of custody of volatile digital evidence. No interpretive adjustment can cure these failures. They demand systematic institutional and legislative change.

It is against this background that the paper pursues four research questions. First, what are the mechanics of dark web narcotics marketplaces, and which features of their design produce the evidentiary problems identified above? Second, what is the reach, and what are the gaps, of the current Indian statutory scheme, under the NDPS Act, the Information Technology Act, 2000 and the law of evidence, as it applies to digital narcotics investigations? Third, how have the Indian courts approached evidentiary requirements in NDPS prosecutions, and what does that record suggest for the future? Fourth, what legislative, institutional and procedural changes does India need, and what examples can comparative practice offer?

The methodology of the paper is doctrinal, complemented by comparative analysis. The NDPS Act and its amendment history, the law of evidence, the Information Technology Act, decisions of the Supreme Court and the High Courts in NDPS and digital evidence cases, reports of the Narcotics Control Bureau, and UNODC drug data[7] are the primary sources. Peer-reviewed law journal articles and interdisciplinary work on cryptomarkets and digital forensics are the secondary sources. The comparative element examines the United States federal model and Europol-coordinated prosecutions, selected because both jurisdictions have conducted dark web narcotics prosecutions at comparable scale and because both have generated transferable evidentiary principles. The purpose is not to prescribe wholesale transplantation but to identify patterns that can be adapted to the Indian constitutional setting.

The paper proceeds as follows. Section II sets out a technical and operational description of dark web narcotics markets, tracing the architecture of the Tor network, privacy-enhancing cryptocurrencies and the structure of a complete dark web purchase. Section III sets out the

[5] *See* Indian Evidence Act, No. 1 of 1872, INDIA CODE (1872); Code of Criminal Procedure, No. 2 of 1974, INDIA CODE (1974); *see also* Bharatiya Sakshya Adhiniyam, No. 47 of 2023, INDIA CODE (2023); Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, INDIA CODE (2023) (both in force from 1 July 2024).

[6] Indian Evidence Act, No. 1 of 1872, §§ 65A, 65B, INDIA CODE (1872); *cf.* Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63, INDIA CODE (2023).

[7] United Nations Office on Drugs and Crime [UNODC], *World Drug Report 2022*, U.N. Sales No. E.22.XI.8 (2022).

 [ISSN 2581-5369]

Indian law governing narcotics proceedings, examining the search and seizure machinery of the NDPS Act in relation to digital evidence and the surveillance provisions of the Information Technology Act and the law of evidence. Section IV, the analytical core, examines five discrete evidentiary challenges, tying each to the procedural requirements the NDPS Act imposes. Section V evaluates the judicial response in NDPS prosecutions, and *Tofan Singh* in particular. Section VI draws comparative lessons from the United States and the European Union. Section VII translates the analysis into concrete reform proposals. Section VIII concludes.

II. Evolution of Dark Web Narcotics Markets

The narcotics markets that have emerged on the dark web are not merely a descriptive adjustment to digital communication, nor an incremental adaptation of the illicit drug trade. The phenomenon dates from Silk Road, launched in 2011 by Ross Ulbricht and shut down by the Federal Bureau of Investigation in 2013,[8] which demonstrated that it was possible to operate a full-fledged narcotics marketplace requiring no face-to-face contact between buyer and vendor, no cash, and no conventional paper trail. The closure of Silk Road did not end the model; it accelerated its development. AlphaBay, Hansa, Dream Market and Wall Street Market followed in close succession, each learning the lessons of earlier law enforcement takedowns by building more resilient architectures. The 2017 dismantling of AlphaBay and Hansa, the two largest operational sites at the time, in a joint Europol and United States operation[9] interrupted supply only for vendors to migrate within months to a new generation of successor platforms. The present stage of the market is defined by increased decentralisation, a movement towards end-to-end encrypted messaging applications as partial substitutes for centralised marketplace services, and the spread of privacy-enhancing cryptocurrencies that defeat the blockchain analytics techniques that worked against earlier markets.

Dark web markets are built on The Onion Router (Tor), an open-source anonymisation network first developed at the United States Naval Research Laboratory.[10] A dark web marketplace is a website with a .onion address reachable only through the Tor network; traffic is encrypted in successive layers and passed through a network of volunteer-run relay nodes, each of which decrypts only the outermost layer and learns nothing about the content or the origin of the communication. More importantly, the physical location of the marketplace server is itself concealed: the server communicates through the Tor network, so that even a node adjacent to it

[8] Nicolas Christin, *Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace*, Proc. 22nd Int'l Conf. on World Wide Web 213 (2013).
[9] Press Release, U.S. Dep't of Justice, *AlphaBay, the Largest Online 'Dark Market,' Shut Down* (July 20, 2017).
[10] Roger Dingledine et al., *Tor: The Second-Generation Onion Router*, Proc. 13th USENIX Sec. Symp. 21 (2004).

 [ISSN 2581-5369]

cannot learn its IP address or location. For investigators, this means that the simplest step in a conventional internet investigation, tracing an IP address to a subscriber through an Internet Service Provider, yields the address of a foreign Tor relay entirely outside the reach of Indian law. This anonymity is compounded by security-conscious vendors who layer virtual private networks, privacy-oriented operating systems such as Tails, and open Wi-Fi connections on top of the Tor layer. The cumulative effect is a stack of anonymisation that the search, seizure and disclosure structure of the NDPS Act was never designed to reach. Beyond the Tor infrastructure, the partial displacement of marketplace platforms by Signal, Wickr and Telegram[11] erases even the server-side message records on which earlier platform-based law enforcement countermeasures relied, because end-to-end encrypted messaging applications do not store message content on their servers.

The second architectural building block of the dark web drug economy is the cryptocurrency payment system. Bitcoin was used in the early markets, and its pseudonymous but publicly recorded blockchain proved a partial weakness: blockchain analytics firms developed tools that could cluster related addresses, follow the movement of funds across one or more hops, and, at the point of conversion into fiat currency at a regulated exchange, identify the account holder from know-your-customer records obtained through legal process.[12] The narcotics trade responded by migrating to Monero, a cryptocurrency that uses ring signatures, stealth addresses and confidential transaction amounts so that the transaction graph itself is not accessible.[13] Unlike Bitcoin, where the investigative task is to match publicly visible addresses to real identities, the architecture of Monero means that the relationships between addresses cannot be reconstructed at all from publicly viewable blockchain data. Where Bitcoin is still used, mixing and chain-hopping, converting Bitcoin into Monero and back again, routinely break the on-chain link between payer and payee. For Indian investigators and prosecutors, the result is that the financial records on which proceeds tracing and forfeiture under Chapter VA of the NDPS Act or the Prevention of Money-Laundering Act, 2002[14] depend are practically inaccessible.

Dark web markets have established a globally distributed vendor ecosystem in which the geographic link between supplier and buyer has been decoupled from the physical transport of contraband. A vendor based in the Netherlands, or in any other country with reliable postal

[11] *See generally* K.E. Vance et al., *The Dark Web and the Evolution of Illicit Markets*, 30 J. CRIM. L. & CRIMINOLOGY 150 (2020).
[12] Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, PROC. 2013 INTERNET MEASUREMENT CONF. 127 (2013).
[13] Amrit Kumar et al., *A Traceability Analysis of Monero's Blockchain*, PROC. 22ND EUR. SYMP. ON RSCH. IN COMPUT. SEC. 153, 154 (2017).
[14] Prevention of Money-Laundering Act, No. 15 of 2003, INDIA CODE (2003).

 [ISSN 2581-5369]

facilities, can serve customers in dozens of countries, despatching orders vacuum-packed and sealed in ordinary commercial packaging through standard post and courier services. According to the UNODC World Drug Report 2023,[15] darknet markets have become a structurally significant channel in the international trade in synthetic drugs, pharmaceutical opioids and new psychoactive substances, with postal and courier delivery the predominant physical means of delivery. India is part of this global system both as a destination and, increasingly, as a source jurisdiction. Narcotics Control Bureau enforcement reporting has recorded cases of MDMA, LSD, ketamine and diverted pharmaceutical opioids entering India through the postal stream in connection with dark web purchases, as well as domestic vendors selling under the cover of encrypted messaging services. A weakness specific to the Indian context is that certain pharmaceutical preparations, such as tramadol, codeine mixtures and alprazolam, occupy an ambiguous position between licit medical supply and illicit diversion, which complicates both scheduling and proof.

This operational architecture produces a particular and acute evidentiary problem in NDPS prosecutions. The investigative structure of the statute is directed at the recovery of contraband linked to a named person by physical proximity, observation or admission; these are the categories of evidence that Sections 41 to 43, and the presumptions in Sections 35 and 54, were framed to produce and to weigh.[16] In a dark web case, contraband may be intercepted in the postal stream, but linking that interception to a particular individual requires digital evidence: marketplace account records, device forensics, cryptocurrency transaction records and communications metadata, all of which are encrypted, pseudonymous, stored on foreign servers, or denominated in an untraceable currency. It is this structural disconnection between the evidentiary premises of a statute of 1985 and the evidentiary universe in which dark web investigations must be pursued that Section III begins to examine by reference to the existing Indian legal framework.

III. Legal Framework Governing Narcotics Control in India

The principal legal framework within which dark web narcotics investigations and prosecutions must be conducted in India comprises three statutes: the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act), the Information Technology Act, 2000 (IT Act),[17] and the law of evidence, contained until 30 June 2024 in the Indian Evidence Act, 1872 and thereafter

[15] United Nations Office on Drugs and Crime [UNODC], *World Drug Report 2023*, U.N. Sales No. E.23.XI.6 (2023).
[16] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, §§ 35, 41-43, 54, India Code (1985).
[17] Information Technology Act, No. 21 of 2000, India Code (2000).

 [ISSN 2581-5369]

in the Bharatiya Sakshya Adhiniyam, 2023, whose Section 63 is the successor to Section 65B. Each was enacted in a different historical context and with different regulatory objectives. None was designed with digital drug markets in mind. Together they form the structure within which investigators, prosecutors and courts must operate, and the tensions and gaps between them define the evidentiary problems examined in Section IV. This Section sets out their principal provisions on search and seizure, digital evidence and investigative authority, as they bear on dark web narcotics cases.

The NDPS Act remains the principal substantive and procedural instrument for narcotics investigation in India. Its search and seizure provisions, in Sections 41 to 43, empower officers of the Narcotics Control Bureau, the customs authorities and the police to search persons, vehicles and premises on reasonable grounds for believing that a narcotic drug or psychotropic substance is concealed there. Section 50 lays down a procedural requirement that the Supreme Court has treated as mandatory in *State of Punjab v. Baldev Singh*,[18] namely that a person about to be searched must be apprised of his right to be searched before a gazetted officer or a Magistrate, a safeguard whose breach vitiates reliance on the recovery. Section 35 raises a presumption of culpable mental state, and Section 54 raises a presumption that a person found in possession of a controlled substance has committed an offence unless he accounts satisfactorily for that possession; between them these provisions shift an evidential burden to the accused once the prosecution has proved conscious possession beyond reasonable doubt. Read together, these provisions describe a framework directed at the recovery of tangible contraband from a physically identified accused. Sections 41 to 54 do not contemplate a case in which the accused was never physically in possession of the substance, in which proof of the offence is entirely digital, or in which the transaction constituting the offence was executed pseudonymously on a server in a foreign jurisdiction whose location is unknown.

Beyond search and seizure, Chapter VA of the NDPS Act provides for the forfeiture of property derived from narcotics trafficking, with a competent authority empowered to attach and forfeit such property. In dark web cases, cryptocurrency is the most natural form of property derived from trafficking, yet Chapter VA contains no provision dealing with digital assets: there is no mechanism for the seizure of private cryptographic keys, no treatment of crypto-assets whose value has passed through mixing services or privacy coins, and no treatment of proceeds held in fragmented micro-balances. The same gap appears in Schedules I and II of the NDPS Act: new psychoactive substances and designer drugs sold on dark web markets may have

[18] *State of Punjab v. Baldev Singh*, (1999) 6 S.C.C. 172 (India).

 [ISSN 2581-5369]

pharmacological properties equivalent to a scheduled substance and yet fall outside the Act, which constrains its reach.

The IT Act is the principal statutory foundation for electronic surveillance and interception in India. Section 69 empowers the Central Government to direct any agency to intercept, monitor or decrypt information transmitted through any computer resource in the interests of national security, public order or the investigation of an offence. That power is extended by Section 69B to the monitoring and collection of traffic data. In principle these provisions could support the interception of dark web use or the monitoring of internet activity connected with a narcotics investigation. In practice they encounter the same limitation described in Section II: where traffic passes through the Tor network it is multiply encrypted, and the intermediary relay is a volunteer node outside Indian control against which no direction under Section 69 can be enforced. Section 79 of the IT Act confers a limited safe harbour on intermediaries acting as mere conduits, and the relationship between its conditions and the requirements of Indian narcotics investigations remains unsettled in the courts.

The proof of electronic records in Indian criminal proceedings is governed by Sections 65A and 65B of the Indian Evidence Act, 1872, inserted by the Second Schedule to the IT Act with effect from 2000, and now by Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. Section 65A provides that the contents of electronic records may be proved in accordance with Section 65B. Section 65B(1) renders an electronic record admissible as documentary evidence where it is accompanied by a certificate under Section 65B(4), signed by a person occupying a responsible official position in relation to the operation of the relevant computer or device, attesting to the conditions prescribed in Section 65B(2): that the computer producing the record was in regular use, that it was operating properly when the record was made, and that the information was fed into it in the ordinary course of the activities of the person having lawful control over its use. The rulings of the Supreme Court in *Anvar P.V. v. P.K. Basheer*[19] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal*[20] confirm that this certification is not a procedural formality that may be supplied later or dispensed with. The dark web setting creates acute difficulties: the electronic data most likely to establish the guilt of an accused, that is, marketplace account information, transaction records and communications metadata, are stored on foreign servers, generated and maintained by systems over which no Indian official and no accused has lawful control, and cannot in practice be certified under Section 65B(4).

[19] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
[20] *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal*, (2020) 7 S.C.C. 1 (India).

 [ISSN 2581-5369]

Viewed as a system, the three statutes disclose a structural mismatch between the Indian legal framework and the operational reality of dark web narcotics investigations. The NDPS Act confers robust enforcement and investigative authority but assumes a universe of physical evidence. The IT Act confers electronic monitoring authority but lacks the technical means to exercise it against Tor-structured infrastructure and lacks the evidentiary machinery to convert intercepts into admissible proof. The law of evidence supplies an admissibility regime for electronic records but conditions it on a certification that is unattainable where the evidence was generated on a foreign server. What emerges is a framework that is at once over-armed, in the severity of its substantive punishment, and under-equipped to meet the evidentiary demands of the cases with which it must now deal. Section IV examines the evidentiary crisis that follows, in the areas of attribution, admissibility, cryptocurrency tracing, jurisdiction and chain of custody.

IV. Evidentiary Challenges in Dark Web Investigations

Section III identified the structural gaps in the three-statute framework governing Indian narcotics investigations. This Section translates those gaps into the concrete evidentiary problems that dark web prosecutions under the NDPS Act generate.[21] Five challenges are discussed: the attribution problem, the admissibility of digital evidence, the limits of cryptocurrency tracing, cross-border jurisdiction, and the integrity of the chain of custody of digital evidence. Each is tied to a particular procedural requirement of the NDPS Act and to the standards the Indian courts apply at trial. Together they constitute the evidentiary crisis identified in the introduction: a mismatch between what dark web investigations produce and what the law requires by way of proof.

A. The Attribution Problem: Identifying the Actual Offender

The most basic and most important problem in any dark web narcotics prosecution is attribution: proving beyond reasonable doubt, to the standard the law requires, that the person on trial is the person behind the pseudonym who conducted the transaction. This is not merely a factual difficulty; it goes directly to the allocation of the burden of proof between prosecution and accused under the NDPS Act. Section 35 raises a presumption of culpable mental state and Section 54 raises a presumption from possession,[22] but neither presumption can operate until the prosecution has proved the fact of possession beyond reasonable doubt. In a dark web case in which an order has been despatched to the accused but the contraband has been intercepted

[21] *See generally* Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, India Code (1985).
[22] *Id.* §§ 35, 54.

 [ISSN 2581-5369]

in the postal stream, the prosecution must first prove that the parcel was ordered by, or delivered to, the accused, and that in turn requires precisely the digital evidence whose admissibility and authenticity are in issue throughout the rest of the case.

Dark web investigations usually rely on one or more of the following routes to proof: device forensics, showing that the accused used a device to access a marketplace account; IP address logs, linking an account login to an address traceable to the premises or service account of the accused; cryptocurrency wallet analysis, linking a wallet used to fund a marketplace transaction to a wallet held or used by the accused; and controlled deliveries, that is, monitored postal interceptions establishing that the accused actually received the contraband. Each of these routes has limitations that the NDPS Act framework does not adequately address. Device forensics presupposes lawful acquisition of the device, under Section 43 of the NDPS Act or Section 91 of the Code of Criminal Procedure,[23] and then technical recovery of encrypted data, for which no statutory framework governs authorisation or admissibility. The use of Tor defeats IP address logs where they can be obtained at all. Cryptocurrency wallet analysis depends on the traceability of the currency used, and privacy coins defeat it entirely. Controlled delivery, the most straightforward route in legal terms, establishes only that the parcel reached the accused, and not that it was ordered through the marketplace, a gap the prosecution must fill with independent digital evidence.

The doctrine settled in *Tofan Singh v. State of Tamil Nadu*[24] compounds the attribution problem. The Supreme Court held that officers invested with powers under Section 53 of the NDPS Act are 'police officers' within the meaning of Section 25 of the Evidence Act,[25] with the consequence that a statement recorded under Section 67 of the NDPS Act cannot be used as a confession against its maker. Where it was admissible, the confessional statement of an accused had long been used in a typical NDPS prosecution to bridge a substantial evidentiary gap. That bridge is unavailable in dark web cases, not only because of *Tofan Singh* but because a technically sophisticated defendant operating through encrypted channels is unlikely to make any statement capable of supporting the digital evidence. The prosecution must therefore build its case on attribution entirely on objective technical evidence, without the corroborative element that confession-based material was formerly understood to supply in an NDPS trial.

[23] Code of Criminal Procedure, No. 2 of 1974, § 91, INDIA CODE (1974); *see now* Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 94, INDIA CODE (2023).
[24] *Tofan Singh v. State of Tamil Nadu*, (2021) 4 S.C.C. 1 (India).
[25] Indian Evidence Act, No. 1 of 1872, § 25, INDIA CODE (1872).

 [ISSN 2581-5369]

B. Digital Evidence Admissibility: Electronic Records and Authenticity

Even where investigators succeed in locating and attributing a dark web narcotics sale to a particular accused, the material they have assembled must satisfy the admissibility requirements in Sections 65A and 65B of the Evidence Act.[26] As noted in Section III, Section 65B(4) requires that any electronic record produced by a computer be supported by a certificate signed by a person occupying a responsible official position in relation to the operation of that computer, attesting to specified conditions of operation and reliability. The Supreme Court in *Arjun Panditrao Khotkar*[27] clarified that the certificate is a mandatory precondition of admissibility and not a curable defect that a court may overlook in the interests of substantial justice.

In the dark web setting the most probative records, that is, marketplace transaction logs, vendor account records, internal message logs and cryptocurrency balance records maintained by the platform, are stored on servers controlled by the marketplace, in a jurisdiction that is unknown and, as a matter of practice, subject to no Indian legal process. The only person who could certify those records under Section 65B(4) is the marketplace operator, an anonymous criminal actor who will not cooperate. Where the marketplace has been taken over by a foreign law enforcement agency, the records may become available through mutual legal assistance, but the certification difficulty is the same: the foreign law enforcement official who produces the records does not occupy a position of lawful control over the original computer in the sense in which Section 65B(4) uses that term, and what he or she issues under the evidentiary principles of another jurisdiction cannot satisfy the Indian statutory requirement.

The problem extends to device-level evidence. Where a laptop or mobile telephone is seized and examined, the authorised person who extracts the data can certify in respect of the forensic image he or she has created under Section 65B(4). But because any device whose user has taken minimal precautions will be encrypted, retrieving that data will require either the cooperation of the accused, which cannot be compelled consistently with the right against self-incrimination under Article 20(3) of the Constitution,[28] or a technical means of circumventing the encryption, which no statutory provision regulates. The resulting gap is structural: the best evidence is either unavailable or, where available, not certifiable under the existing Section 65B regime.

[26] *Id.* §§ 65A, 65B.
[27] *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal*, (2020) 7 S.C.C. 1 (India).
[28] INDIA CONST. art. 20, cl. 3.

 [ISSN 2581-5369]

C. Cryptocurrency Tracing: Proceeds, Forfeiture and the Privacy Coin Problem

The third evidentiary problem is the financial dimension of dark web narcotics investigations. Chapter VA of the NDPS Act[29] provides a regime for the attachment and forfeiture of property derived from narcotics trafficking. The practical operation of that regime in cryptocurrency cases raises difficulties that go beyond the absence of explicit statutory guidance: they concern the inherent capacity of investigators to prove, to the evidentiary threshold that attachment and forfeiture require, the connection between a particular cryptocurrency holding and a particular narcotics offence.

Where transactions are conducted in Bitcoin, blockchain analytics, deployed by agencies such as the Financial Intelligence Unit-India in conjunction with commercial analytics providers, can trace the flow of funds across the public blockchain and, at the point of conversion into fiat currency at an authorised exchange, identify the account holder from know-your-customer records. Whether blockchain analytics reports qualify as expert evidence under Section 45 of the Evidence Act[30] remains undecided in Indian jurisprudence: there is no authority on the qualification criteria for blockchain forensics experts, on the reliability of the analytical tools they use, or on the manner in which their findings must be presented to satisfy a court.

Where transactions are conducted in Monero or another privacy coin, or where the trail has been broken by mixing services, the chain of tracing fails altogether. The competent authority under Chapter VA cannot attach property whose connection to narcotics activity cannot be demonstrated on the evidence available. The accused retains the benefit of cryptocurrency balances that are the direct product of the trafficking enterprise, and the preventive and restitutive objects of the forfeiture regime are defeated. India has no statutory analogue to the civil asset forfeiture rules that permit prosecutors in the United States[31] to proceed against cryptocurrency assets on the balance of probabilities without a criminal conviction, a solution of considerable operational value in dark web cases but one that rests on contested civil liberties ground.

D. Cross-Border Jurisdiction: Territorial Limits and Mutual Legal Assistance

Dark web narcotics investigations are almost always multi-jurisdictional. The marketplace server, the vendor, the cryptocurrency exchange, the postal collection point and the buyer may each be located in a different country. Under the NDPS Act, Indian criminal jurisdiction is

[29] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, ch. VA, INDIA CODE (1985).
[30] Indian Evidence Act, No. 1 of 1872, § 45, INDIA CODE (1872).
[31] *See, e.g.*, 18 U.S.C. § 981 (2018) (civil forfeiture procedures in the United States).

largely territorial: the Act applies to offences committed in India and on Indian ships and aircraft, and its extraterritorial operation under Section 3, read with the Extradition Act, 1962,[32] is confined to offences committed by Indian citizens outside India. The prospect of pursuing a vendor under the NDPS Act where the vendor is a foreign national operating entirely outside India, and the only nexus with India is the receipt of a postal consignment by a buyer here, is therefore tenuous, and the realistic prospect of gathering evidence in the vendor's jurisdiction depends wholly on the availability and responsiveness of mutual legal assistance mechanisms.

India's network of mutual legal assistance treaties, though expanding, is incomplete so far as cyber-narcotics investigations are concerned. Through the Central Authority designated in the Ministry of Home Affairs, and in accordance with the Comprehensive Guidelines on Mutual Legal Assistance in Criminal Matters,[33] assistance in gathering evidence, serving process and conducting searches may be sought from treaty partners. The turnaround time on mutual legal assistance requests in complex digital investigations, estimated at between twelve and eighteen months in comparable jurisdictions, is structurally incompatible with the volatility and pace of dark web evidence. Furthermore, treaty coverage does not extend to many of the jurisdictions in which dark web infrastructure is located: states with no treaty relationship, failed states, and jurisdictions with minimal law enforcement cooperation capacity are precisely those in which marketplace operators choose to site their servers.

E. Chain of Custody for Digital Evidence: Integrity and Verification

The fifth evidentiary problem is the chain of custody of digital evidence, that is, the need to establish at every stage of its passage to trial that the material produced in court is the same material originally seized and has not been altered, corrupted or substituted. In a traditional NDPS prosecution, chain of custody is proved through the seizure mahazar, witness signatures, sealed packages and forensic laboratory documentation. The NDPS Act and the rules made under it[34] contain provisions of this kind for physical contraband, but no equivalent provision for digital evidence.

Chain of custody problems with digital evidence are qualitatively different from those affecting physical contraband. A computer file can be copied perfectly and altered undetectably; without a cryptographic hash of the file taken at the time of seizure, a mathematical fingerprint of its contents at that moment, there is no way to demonstrate at trial that the material has not changed

[32] Extradition Act, No. 34 of 1962, INDIA CODE (1962).
[33] *See* MINISTRY OF HOME AFFAIRS, GOV'T OF INDIA, *Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory / Mutual Legal Assistance Requests* (rev. ed. 2019).
[34] Narcotic Drugs and Psychotropic Substances Rules, 1985, GAZ. OF INDIA (1985).

 [ISSN 2581-5369]

between seizure and production. Hash verification at the point of seizure has not been mandatory in Indian forensic practice, and no statutory requirement or binding judicial ruling has imposed it in NDPS investigations, although Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 now requires the certificate accompanying an electronic record to state its hash value. The transfer of evidence across several agencies, from the investigating officer to the forensic laboratory, the prosecutor and finally the court, creates a point of challenge at every handover, and the absence of a standardised scheme for recording the handling of digital evidence exposes prosecutions to precisely the kind of challenge the certification requirement in Section 65B was designed, at least in part, to meet.[35]

The chain of custody problem is aggravated in investigations involving international cooperation. Where digital evidence obtained through mutual legal assistance requests or joint operations with foreign services is produced in Indian proceedings, it has passed through the evidence-handling procedures of at least one other jurisdiction. How far those procedures are compatible with the requirements of Section 65B has not been clarified by the courts. Until Indian law establishes its own procedures for the reception of foreign-acquired digital evidence, addressing not only its authentication but also certification of the conditions in which it was created and transmitted, this gap will leave dark web narcotics prosecutions vulnerable to admissibility challenges at the most critical stage of trial.

F. Synthesis: The Cumulative Evidentiary Deficit

The five challenges considered in this Section are not discrete or independent; they are mutually reinforcing. An attribution gap that financial evidence might have bridged is widened where the financial evidence is denominated in an untraceable currency. An admissibility obstacle that overseas records might have overcome persists because those records cannot be certified under Section 65B. A chain of custody that scrupulous domestic procedure might have preserved is exposed where international transfers do not observe the same standards. Compounded, the net result is that a dark web narcotics prosecution in India faces an evidentiary shortfall at every stage of the evidential chain, from identifying the offender, to authenticating the evidence, to proving the financial nexus. This cumulative deficit cannot be met by judicial interpretation of the existing scheme, however ingenious; it must be met legislatively, in the manner discussed in Section VII.[36] Before turning to reform, Section V examines how the Indian courts have applied existing evidentiary standards in NDPS prosecutions and what principles emerge for

[35] Indian Evidence Act, No. 1 of 1872, § 65B, INDIA CODE (1872).
[36] *See infra* Section VII.

 [ISSN 2581-5369]

the dark web context.

V. Judicial Approach and Case Law

The Indian courts have consistently treated the evidentiary requirements of NDPS prosecutions as matters of strict legal compliance rather than judicial discretion. This judicial posture is not incidental: it reflects the constitutional rationale that the severity of the minimum sentences the NDPS Act imposes in commercial quantity cases, extending to twenty years of rigorous imprisonment, requires that a corresponding standard of procedural integrity be observed at every stage of the chain of proof. On repeated occasions the Supreme Court has intervened to set aside convictions in which mandatory procedural protections were absent, treating their absence as fatal to the prosecution however culpable the accused may appear. This history of strict judicial scrutiny supplies the necessary context in which the evidentiary problems of dark web prosecution must be considered: if the courts have been unwilling to relax procedural requirements in conventional NDPS cases, they are unlikely to relax them merely because the evidence in question is digital and correspondingly harder to authenticate.

The decision of the Constitution Bench of the Supreme Court in *State of Punjab v. Baldev Singh*[37] established the foundational principle that the protections written into the NDPS Act are not technicalities but substantive rights whose breach affects the admissibility of the recovery itself. The Court held that the failure to inform a suspect of his right to be searched before a gazetted officer or a Magistrate under Section 50 rendered the resulting seizure of contraband unusable against him,[38] notwithstanding that the contraband was in fact present. The implications of this principle for digital evidence in dark web cases are straightforward: if a physical recovery conducted without the prescribed procedure cannot support a conviction, no judicial device can admit digital evidence gathered without equivalent safeguards.

The recent NDPS ruling of greatest consequence for the dark web evidentiary crisis is the three-judge bench decision of the Supreme Court in *Tofan Singh v. State of Tamil Nadu*, decided on 29 October 2020 and reported in 2021. The question before the Court was whether officers invested with powers under Section 53 of the NDPS Act are 'police officers' within the meaning of Section 25 of the Evidence Act, so that a confession made to them is inadmissible. The majority, departing from earlier authority holding that such officers are not police officers and that statements recorded by them could constitute substantive evidence against their maker, held that they are police officers and that a statement recorded under Section 67 of the NDPS Act

[37] *State of Punjab v. Baldev Singh*, (1999) 6 S.C.C. 172 (India).
[38] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, § 50, India Code (1985).

 [ISSN 2581-5369]

cannot be used as a confession. The minority took the contrary view, which illustrates the genuine doctrinal difficulty of the question, but the majority opinion is now binding law. The implications for dark web prosecutions are immediate. In conventional NDPS cases, a statement in which the accused admits possession, or knowledge of the nature of the substance, or participation in a trafficking arrangement, has traditionally supplied the connective tissue between the physical recovery and the mental and participatory elements of the offence. *Tofan Singh* removes that instrument from the prosecutor's armoury altogether and throws the entire evidential burden on to objective evidence. That burden falls very heavily indeed in dark web cases, where the objective evidence is digital, encrypted, pseudonymous and of contested authenticity.

The jurisprudence on Section 65B of the Evidence Act has moved over the last decade from relative flexibility to strict insistence on mandatory compliance. In *Anvar P.V. v. P.K. Basheer*,[39] the Court departed from its earlier decision in *State (NCT of Delhi) v. Navjot Sandhu* and held that electronic records are inadmissible without a Section 65B certificate and cannot be proved by oral testimony or as secondary evidence under Section 65 of the Evidence Act by way of an alternative route. *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal* reaffirmed this, holding that the certificate must be obtained and tendered at the time the electronic record is produced and cannot be supplied afterwards to cure a defect arising at an earlier stage. Taken together, these decisions foreclose any prospect that a court in a dark web narcotics trial could receive marketplace records, device extractions or blockchain transaction data without satisfying the strict requirements of Section 65B, requirements which Section IV has shown to be structurally unattainable for the most probative categories of dark web evidence.

A body of High Court jurisprudence addressing digital evidence in NDPS matters is emerging, but it remains fractured and fragmented. Several High Courts have acquitted accused persons where digital evidence such as mobile telephone records, WhatsApp messages and call detail records was tendered without a Section 65B certificate, or where the certificate was defective. Other courts have been asked whether electronic evidence obtained through surveillance authorised under Section 69 of the IT Act[40] satisfies the predicate conditions for certification under Section 65B, particularly where the certifying body is the intercepting agency rather than the service provider. No settled principle has emerged, and no reported High Court decision in the NDPS context has squarely addressed whether foreign-sourced digital evidence can ever

[39] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
[40] Information Technology Act, No. 21 of 2000, § 69, INDIA CODE (2000).

 [ISSN 2581-5369]

satisfy the certification requirement of Section 65B.

The body of case law discussed in this Section sends a consistent signal for dark web narcotics prosecutions: the Indian courts enforce the evidentiary burden strictly, they have shown no inclination to relieve the evidential difficulties that dark web prosecutions generate, and the cumulative effect of *Tofan Singh*, *Anvar P.V.* and *Arjun Panditrao Khotkar* is to withdraw from prosecutors the two instruments formerly used to fill evidential gaps, namely confessional statements and informally produced electronic material. This judicial posture is not hostile to justice; it is a statement of it. The constitutional principle that the severity of punishment must be matched by the integrity of the proof applies with equal force to dark web prosecutions. It does not follow that dark web offenders should go unprosecuted, only that the legal infrastructure on which their prosecution rests must be built to the standard the Constitution and the courts prescribe. Section VII considers what that infrastructure must comprise.

VI. Comparative Perspective

The evidentiary problems examined in Section IV are not peculiar to India. They have confronted every jurisdiction that has attempted to prosecute dark web narcotics offences, and the responses developed in the United States, and through the coordination of investigations among European Union member states, offer instructive lessons. The comparison is not made to suggest that Indian law must reproduce those foreign systems wholesale, since constitutional constraints, institutional capacities and legal cultures differ substantially, but to identify the values and institutional processes that can be carried across into the reforms proposed in Section VII.

United States federal investigative agencies have combined legal powers and technical capabilities in a way that addresses, with some success, each of the evidentiary problems identified in this paper. On attribution, the FBI and the DEA have used Network Investigative Techniques (NITs), court-authorised software deployed against marketplace servers to reveal the true IP addresses of users connecting through Tor, under warrants issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure,[41] as amended in 2016 to permit judges to authorise searches of computers whose location is unknown. The Internal Revenue Service Criminal Investigation division and the Department of Justice have developed cryptocurrency blockchain analytics that supported the seizure of assets valued at over USD 3.36 billion in the Silk Road-related forfeiture announced in November 2022, and have obtained civil forfeiture

[41] Fed. R. Crim. P. 41(b)(6).

 [ISSN 2581-5369]

orders against cryptocurrency wallets[42] on the balance of probabilities without any criminal conviction. The Federal Rules of Evidence also permit the circumstantial authentication of digital evidence under Rule 901(b),[43] without the certification requirement that Section 65B imposes in Indian law.

The operational consequences of this structure are significant. The prosecution of Ross Ulbricht in connection with Silk Road[44] established that marketplace server logs, Bitcoin blockchain records and forum posts could together prove identity and intent beyond reasonable doubt even where the accused had conducted his activities entirely under a pseudonym. The 2017 AlphaBay takedown, coordinated with Europol, led to the arrest of the platform operator Alexandre Cazes in Thailand[45] and to the confiscation of cryptocurrency holdings across several jurisdictions, demonstrating that multi-jurisdictional forfeiture of digital assets can be achieved where the legal frameworks are aligned and established bilateral cooperation models are already in place.

The European Union Joint Cybercrime Action Taskforce (J-CAT), based at Europol since 2014,[46] is a standing multi-jurisdictional investigative platform that has proved highly effective against dark web narcotics enterprises. The J-CAT model addresses the mutual legal assistance delay that Section IV described as structurally damaging to Indian investigations: instead of routing evidence requests through slow treaty channels, J-CAT embeds officers of member state law enforcement agencies in a single operational unit, which enables timely intelligence sharing, simultaneous cross-jurisdictional execution of warrants, and the immediate transmission of digital evidence in formats suited to the admissibility requirements of each member state involved. It was this standing operational capacity that made possible the simultaneous takedown of AlphaBay and Hansa in 2017, in which authorities in the Netherlands, Germany, Lithuania, France and the United States acted within a single overlapping window. The European Union e-Evidence Regulation, adopted in July 2023 and applicable from 18 August 2026,[47] will further facilitate cross-border production orders for electronic evidence among member states through standardised request formats and binding response deadlines, addressing directly the delay and compatibility problems identified in Section IV.

---

[42] *See, e.g.*, *United States v. Approximately 69,370 Bitcoin (BTC)*, No. 20-cv-07811 (N.D. Cal. filed Nov. 5, 2020) (civil forfeiture action concerning Silk Road digital assets).
[43] Fed. R. Evid. 901(b).
[44] *United States v. Ulbricht*, 858 F.3d 71, 83 (2d Cir. 2017).
[45] Press Release, U.S. DEP'T OF JUSTICE, *AlphaBay, the Largest Online 'Dark Market,' Shut Down* (July 20, 2017).
[46] EUROPOL, *Joint Cybercrime Action Taskforce (J-CAT)* (2014).
[47] Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for Electronic Evidence in Criminal Matters, 2023 O.J. (L 191) 118 (applicable from 18 August 2026).

 [ISSN 2581-5369]

Three lessons from these comparative models apply directly to the Indian context. First, the attribution problem calls for legal authority as much as technical capability: the 2016 amendment to Rule 41 of the Federal Rules of Criminal Procedure, which authorised NITs against computers of unknown location, shows that a focused statutory amendment can give investigators the means to act in circumstances the original procedural arrangements did not contemplate, without abandoning the warrant requirement or diluting the judicial supervision the Constitution demands. Second, cryptocurrency forfeiture requires a dedicated statutory framework that does not depend on privacy coin traceability or on a completed criminal conviction: a civil forfeiture route, analogous to the United States civil asset forfeiture system and expressly extending to digital assets, should be introduced, with appropriate procedural protections against unwarranted deprivation. Third, the J-CAT model shows that mutual legal assistance delay is not a necessary consequence of inter-state cooperation but a function of institutional design: joint investigative units with embedded liaison officers reduce evidence transfer times from months to hours.

These lessons must be received with care. The United States civil asset forfeiture regime has attracted sustained criticism on the ground that it permits deprivation of property without adequate procedural protection, and any Indian analogue would have to be designed with the safeguards that Article 300A of the Constitution and the standards of natural justice require. The J-CAT model presupposes a degree of sustained bilateral trust and institutional investment that India's existing law enforcement relationships do not uniformly provide. The value of the comparative exercise lies not in supplying a ready-made solution but in demonstrating that the evidentiary crisis described in this paper is capable of being overcome, and that the design choices involved are legislative and institutional rather than technical. Section VII develops reform proposals on the basis of this analysis.

VII. Policy and Legal Reform

The discussion above has shown that the evidentiary crisis in Indian dark web narcotics prosecutions is not accidental but structural: it cannot be overcome by judicial accommodation of the existing provisions, however innovative, because its roots lie in statutory gaps that only legislative change can close. This Section proposes four specific reforms, each addressed to one of the evidentiary failures identified in Section IV and each drawing on the comparative lessons of Section VI. The proposals are ordered from those capable of immediate implementation to those that are institutionally most demanding, and all are framed to remain compatible with the constitutional rights of the accused which, as the judicial review in Section V demonstrated, the

 [ISSN 2581-5369]

courts enforce strictly.

The first and most basic reform is the creation of specialised cyber-narcotics investigation units within the Narcotics Control Bureau,[48] properly staffed and trained in digital forensics, blockchain analytics and dark web investigation. The current operational structure of the NCB, organised around traditional drug-type specialisations, does not correspond to the technical demands of online narcotics investigation. The skills that dark web investigation requires, in preserving volatile digital evidence, conducting device forensics on encrypted hardware, interpreting blockchain transaction records and explaining technical evidence to courts, are not taught in conventional narcotics enforcement training and are not reflected in the documented capability profile of the NCB. The operational advantage of dedicated standing units over ad hoc task forces assembled for particular investigations is demonstrated by the J-CAT model discussed in Section VI. A permanent cyber-narcotics arm of the NCB, with a separate budget line, a defined training curriculum, and liaison relationships with the INTERPOL cybercrime directorate and with J-CAT,[49] would address the capability shortfall underlying the attribution and chain of custody failures documented in this paper.

The second reform is legislative amendment of the NDPS Act and the law of evidence to establish a coherent statutory framework for digital evidence in narcotics investigations. Three amendments are required. First, the NDPS Act should be amended to state expressly the power to search for and seize digital devices and data:[50] what authorisation is required, on what conditions encrypted devices may be seized, what obligations a service provider or device owner has to render technical assistance, and how far decryption may be compelled consistently with Article 20(3) of the Constitution.[51] Second, the certification provision[52] should be amended to close the gap that arises where electronic records are produced from a foreign server or through mutual legal assistance. An amended certification provision, permitting certification by the foreign law enforcement agency that received the records, accompanied by an authenticated translation and a statement of compliance with the standards the Indian provision prescribes, would retain the reliability rationale of Section 65B while removing the structural impossibility that the present provision creates for foreign-obtained digital evidence. Third, the forfeiture regime in Chapter VA of the NDPS Act should be extended to digital assets, with provision for

[48] *See* Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, § 4, INDIA CODE (1985) (measures by the Central Government, including the constitution of a central authority).
[49] *See generally* INTERPOL, *Cybercrime Directorate Overview* (2021).
[50] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, §§ 41-43, INDIA CODE (1985).
[51] INDIA CONST. art. 20, cl. 3.
[52] Indian Evidence Act, No. 1 of 1872, § 65B, INDIA CODE (1872); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63, INDIA CODE (2023).

 [ISSN 2581-5369]

the identification, seizure and valuation of cryptocurrency assets, for the treatment of assets held in privacy coins or passed through mixing services, and for the standard of proof applicable to a forfeiture application where no criminal conviction has been obtained.

The third reform is the issue of binding digital evidence guidelines addressing the chain of custody failure identified in Section IV. Such guidelines should at a minimum require: cryptographic hash verification of every digital exhibit at the point of seizure, with the resulting hash value recorded in the seizure mahazar and re-verified at each subsequent handover; standardised imaging and storage protocols for every seized device, aligned with international forensic guidance such as that issued by NIST[53] and with the Council of Europe Convention on Cybercrime;[54] mandatory use of write-blocking devices when handling a digital exhibit, so that inadvertent modification is prevented; and a documented chain of custody log for every digital exhibit, recording each transfer, the person responsible and the verification performed. These requirements do not call for fresh primary legislation: they can be introduced by executive instruction or by rules made by the Central Government under Section 76 of the NDPS Act, which empowers the government to make rules for carrying out the purposes of the Act.

The fourth reform addresses the deficit in international cooperation which Section IV identified as structurally inconsistent with the evidentiary demands of dark web investigation. India should negotiate dedicated cyber-narcotics clauses into its existing bilateral mutual legal assistance arrangements with the United States, the United Kingdom, the Netherlands, Germany and Australia, specifying expedited response periods, aligned digital evidence production formats, and reciprocal terms for the acceptance of foreign-authenticated electronic certificates before domestic courts. In parallel, India should institutionalise its engagement with Europol's J-CAT by seeking associate status under the existing law enforcement cooperation arrangement between India and Europol, which would give Indian investigators access to real-time information sharing and operational planning in dark web narcotics matters with a foreign element. All these reforms depend on sustained investment in training. Carefully drafted legislative frameworks will be of little use to prosecutors who cannot explain blockchain evidence to a judge, or to judges who cannot evaluate it. The training division of the Central Bureau of Investigation and the National Judicial Academy should establish specialised courses on digital evidence, cryptocurrency forensics and dark web investigative procedure for prosecutors, investigators and judicial officers.

---

[53] *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., *NIST Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response* (2006).

[54] COUNCIL OF EUROPE, *Convention on Cybercrime*, Nov. 23, 2001, E.T.S. No. 185.

 [ISSN 2581-5369]

These four reforms are complementary: specialised investigative capacity produces the digital evidence that amended statutory provisions can render admissible; binding chain of custody protocols ensure that the evidence survives its passage to trial; and strengthened international cooperation makes available the foreign-sourced records that the present law cannot receive. Importantly, every reform is designed to improve the ability of the prosecution to prove its case, not to erode the procedural protections that the courts have consistently recognised as the constitutional entitlement of any person accused under the NDPS Act. The objective is a legal infrastructure that is both effective and fair, a framework equal to the offence it addresses and equal to the rights it must respect.

VIII. CONCLUSION

As this paper has argued, the arrival of dark web narcotics markets in the Indian criminal landscape has exposed an evidentiary crisis within the structure of the Narcotic Drugs and Psychotropic Substances Act, 1985 and its associated procedural framework.[55] This is not a problem of particular investigative practice or judicial disposition; it is a creation of the statute. The NDPS Act was built for a world of physical contraband, face-to-face dealing and recoverable confessions. The dark web is a world of pseudonymous identities, encrypted messages, irreversible cryptocurrency transfers and data held on foreign servers. Interpretation offers no way of bridging the gap between those two worlds. The way out lies in legislation, institutional investment and sustained inter-agency cooperation.

The crisis has the five dimensions identified in this paper. Attribution reaches a dead end: linking a pseudonymous online identity to a named accused is structurally difficult in the presence of Tor anonymisation and in the absence, after *Tofan Singh v. State of Tamil Nadu*,[56] of any confessional statement capable of corroboration. The Section 65B certification requirement obstructs the admissibility of digital evidence, and that certification cannot in practice be satisfied for records held on foreign marketplace servers or extracted from encrypted devices. Privacy coins and mixing services defeat cryptocurrency tracing, rendering the Chapter VA forfeiture regime largely ineffective.[57] Cross-border jurisdiction is confined by territorial limits and mutual legal assistance delays that are simply incompatible with the volatility of digital evidence. And in the absence of any binding standard requiring cryptographic verification of a digital exhibit at the point of seizure, the chain of custody is left exposed.

[55] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, INDIA CODE (1985).
[56] *Tofan Singh v. State of Tamil Nadu*, (2021) 4 S.C.C. 1 (India).
[57] Narcotic Drugs and Psychotropic Substances Act, No. 61 of 1985, ch. VA, INDIA CODE (1985).

 [ISSN 2581-5369]

Addressing these failures matters not only for prosecutorial effectiveness but because of the gravity of the consequences under the NDPS Act, which carries some of the harshest mandatory sentences in Indian criminal law. The constitutional principle affirmed by the Supreme Court in *State of Punjab v. Baldev Singh*, that the severity of the penalty must be matched by the integrity of the proof,[58] and reaffirmed in the specific setting of digital evidence in *Anvar P.V. v. P.K. Basheer*[59] and *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal*,[60] applies in full to dark web prosecutions. Reform of this kind is not an indulgence towards the offender; it creates the conditions in which a prosecution can be brought home consistently with constitutional principle.

The position taken throughout this paper is that a shortage of admissible evidence is not a reason to relax the procedural safeguards available to persons accused under the NDPS Act. Section V showed that Indian courts have treated strict enforcement of those safeguards as integral to evidentiary integrity, and the same discipline must govern digital evidence. The reform proposals advanced in Section VII, comprising dedicated cyber-narcotics investigation units, targeted statutory amendments, binding digital evidence protocols and strengthened international cooperation, are directed at enabling the prosecution to satisfy the existing evidentiary standard rather than at lowering that standard because investigation has become difficult. The balance between enforcement effectiveness and procedural fairness is not a zero-sum trade-off: a properly equipped legal system can achieve both.

India stands at a turning point in its engagement with technology-facilitated narcotics trafficking. The present moment, in which dark web drug markets are growing in number, scale and sophistication but have not yet outstripped the investigative capacity of Indian law enforcement, offers the best opportunity to begin the legislative work of addressing trafficking through the dark web and of equipping enforcement agencies to apply whatever new framework emerges. The comparative material discussed in Section VI indicates that the evidentiary crisis identified in this paper can be resolved: other jurisdictions have built both the statutory and the institutional infrastructure needed to prosecute large-scale dark web narcotics offences while maintaining the procedural protections that the rule of law guarantees. India has the legal tradition, the institutional capacity and the constitutional framework to do the same. What it now needs is the political will to legislate.

*****

[58] *State of Punjab v. Baldev Singh*, (1999) 6 S.C.C. 172 (India).
[59] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).
[60] *Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal*, (2020) 7 S.C.C. 1 (India).

 [ISSN 2581-5369]