

# INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

---

Volume 9 | Issue 3

---

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

---

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact [support@vidhiaagaz.com](mailto:support@vidhiaagaz.com).

---

**To submit your Manuscript** for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to [submission@ijlmh.com](mailto:submission@ijlmh.com).

---

# Cyber-Enabled Drug Trafficking: Under the NDPS Act Challenges Faced by the Narcotics Control Bureau

---

M. KAVINILAVU\*, TAMILSELVAN M\*\* AND PRATHIKSHA KAMINI P\*\*\*

## ABSTRACT

*The unprecedented growth of digital technology has fundamentally reshaped the dynamics of narcotics trafficking, enabling organised criminal networks to use darknet marketplaces, encrypted communication platforms, social-media applications, and cryptocurrency-based transactions to facilitate the illicit drug trade with enhanced anonymity and operational sophistication. In India, the proliferation of cyber-enabled narcotics networks has posed significant challenges to law-enforcement agencies, particularly the Narcotics Control Bureau (NCB), in the prevention, detection, investigation, and prosecution of offences under the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act). The borderless and anonymous nature of digital platforms has substantially undermined traditional investigative mechanisms and exposed critical limitations within the existing legal and regulatory framework. This paper critically analyses the emerging phenomenon of digital drug trafficking in India and examines the enforcement challenges encountered by the Narcotics Control Bureau under the NDPS Act. It explores the increasing reliance on darknet marketplaces, encrypted messaging services, anonymous digital payment systems, and cryptocurrency transactions in facilitating transnational narcotics operations, and evaluates the legal and evidentiary issues arising from electronic-evidence collection, cyber-surveillance, jurisdictional complexity, digital anonymity, and cryptocurrency tracing in contemporary narcotics investigations. Assessing the effectiveness of the NDPS Act in addressing cyber-enabled narcotics offences, it highlights the need for advanced cyber-forensics, modern investigative mechanisms, and international cooperation, and concludes that legal reform, technological modernisation, and coordinated enforcement strategies are essential to combat online narcotics trafficking and to strengthen India's narcotics-control framework in the digital era.*

**Keywords:** NDPS Act, Cyber-Enabled Narcotics Trafficking, Narcotics Control Bureau, Dark Web, Cryptocurrency Transactions, Digital Evidence, Online Narcotics Trade.

---

\* Author is an LL.M. (CBCS) Criminal Law student at The Tamil Nadu Dr. Ambedkar Law University, Chennai, Tamil Nadu, India.

\*\* Author is an Advocate in Chengalpattu, Tamil Nadu, India.

\*\*\* Author is an LL.M. (Constitutional and Administrative Law) student at The Tamil Nadu Dr. Ambedkar Law University, Chennai, Tamil Nadu, India

## **I. INTRODUCTION**

The increasing dependence on digital technology has transformed the manner in which criminal activities are conducted in the modern era. Narcotics trafficking, traditionally associated with physical networks and street-level operations, has expanded into the digital sphere through darknet platforms, encrypted communication applications, and cryptocurrency transactions. The anonymity and global reach provided by digital technology have enabled organised criminal groups to conduct the narcotics trade with greater secrecy and operational efficiency. In India, the emergence of cyber-enabled drug trafficking has created serious challenges for the law-enforcement agencies responsible for narcotics control. Traffickers increasingly use online platforms and digital financial systems to conceal identities, transfer funds, and coordinate illegal transactions across jurisdictions, and these technologically advanced methods have substantially complicated investigation and prosecution under the existing legal framework.

The Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act) is the principal legislation governing narcotics offences in India. Its enforcement is undertaken primarily by the Narcotics Control Bureau, which plays a crucial role in preventing illicit drug trafficking and coordinating narcotics-enforcement activities nationwide. The growing misuse of digital technology in narcotics operations has, however, exposed several legal and practical limitations within the traditional enforcement structure, and challenges relating to electronic evidence, cyber-surveillance, cryptocurrency tracing, digital anonymity, and cross-border jurisdiction continue to hinder effective enforcement. In this context, the present paper critically examines the emerging threat of cyber-enabled drug trafficking and analyses the challenges faced by the Narcotics Control Bureau in addressing technologically sophisticated narcotics offences in the digital era.

## **II. EVOLUTION OF CYBER-ENABLED NARCOTICS TRAFFICKING**

### **A. Transition from Conventional Drug Trafficking to Digital Networks**

Drug trafficking has shifted from physically coordinated supply chains to technology-driven and anonymised networks. According to global drug-monitoring assessments, a significant proportion of illicit drug transactions are now facilitated through online communication channels rather than direct physical contact, indicating a structural shift toward the digitalisation of narcotics markets.

### **B. Emergence of Darknet Marketplaces**

Darknet platforms have become central hubs for the illicit drug trade, operating through encry-

pted networks that conceal user identity and location. Reports from international drug-control authorities highlight that these marketplaces enable global access to narcotics with minimal geographical restriction.<sup>1</sup> The use of escrow systems and anonymous vendor ratings has further increased trust and scale in illicit online drug economies.

### **C. Encrypted Communication and Digital Anonymity**

Encrypted messaging systems, such as end-to-end secure applications and VPN-based communication tools, are widely used by traffickers. The International Narcotics Control Board (INCB) has reported that encryption technologies significantly obstruct law-enforcement surveillance and digital-evidence collection, creating major operational barriers to identifying criminal networks operating online.<sup>2</sup>

### **D. Cryptocurrency and Online Financial Transactions**

Cryptocurrency has become a dominant payment mechanism in the cyber-enabled narcotics trade because of its pseudonymous structure. The research literature indicates that a large portion of darknet drug transactions are conducted through Bitcoin and other virtual currencies, allowing cross-border fund transfers without reliance on traditional banking systems and increasing the investigative complexity of tracing illicit financial flows.<sup>3</sup>

### **E. Social-Media Platforms and Online Drug Distribution**

Recent studies and enforcement reports indicate the increasing misuse of social-media platforms for drug marketing and distribution. Criminal actors use coded language, private groups, and temporary accounts to avoid detection, and the INCB has observed that social-media applications are increasingly exploited for drug supply chains targeting younger users and urban populations.

### **F. The Transnational Nature of Cyber-Enabled Narcotics Operations**

Cyber-enabled narcotics trafficking is highly transnational, involving multiple jurisdictions across production, distribution, and financial routing. Global reports indicate that a significant share of illicit drug flows now involves cross-border digital coordination, making mutual legal assistance and international cooperation essential for enforcement.

---

<sup>1</sup> INT'L NARCOTICS CONTROL BD., *Annual Report 2024*.

<sup>2</sup> INT'L NARCOTICS CONTROL BD., *supra* note 1.

<sup>3</sup> U.N. OFF. ON DRUGS & CRIME, *World Drug Report 2024*.

### III. DIGITAL EXPANSION AND THE CRYPTOCURRENCY-BASED DRUG ECONOMY

#### A. Scale of the Darknet Drug Trade

The worldwide drug trade has changed dramatically with the growth of darknet marketplaces, moving from physically controlled networks to highly organised digital ecosystems. These platforms use encrypted networks that permit anonymous access, communication, and transactions, limiting the efficacy of conventional enforcement methods. According to empirical research, the majority of illicit products traded online are narcotics, which make up between 60 and 80 per cent of all listings on prominent darknet markets, and monitoring reports suggest that there may be more than 100,000 active drug listings at any given time, reflecting the platforms' extensive commercialisation and global reach.<sup>4</sup> Darknet drug ecosystems today operate as coordinated global supply chains with thousands of vendors and geographically scattered buyers, in contrast to earlier fragmented criminal markets.

#### B. Platformisation of Drug Markets

Darknet drug markets increasingly resemble legitimate e-commerce platforms in their structure and operational design. According to the Global Initiative Against Transnational Organized Crime, these markets have evolved into structured digital systems that replicate commercial models through product catalogues, vendor profiles, ratings, and escrow-based payment mechanisms. Escrow services ensure that payments are released only after delivery is confirmed, building trust among anonymous participants while reducing the risk of fraud. This "platformisation" has transformed narcotics trafficking into a service-oriented digital economy characterised by anonymity, efficiency, and global scalability without physical interaction between actors.

#### C. Cryptocurrency-Based Financial Architecture

Cryptocurrency has become the backbone of financial transactions within darknet drug markets because of its decentralised structure and pseudonymous nature. The United Nations Office on Drugs and Crime (UNODC) notes that digital currencies are widely used in the narcotics trade, as they allow peer-to-peer transfers without reliance on traditional banking systems, and their borderless nature enables the rapid cross-jurisdictional movement of funds, weakening conventional financial-monitoring and anti-money-laundering systems. Blockchain-intelligence research, including findings from Elliptic, shows that traffickers use layered wallet transfers, repeated conversions, intermediary exchanges, and privacy tools such as mixers to

---

<sup>4</sup> GLOB. INITIATIVE AGAINST TRANSNAT'L ORGANIZED CRIME, *Cryptomarkets Report*.

obscure transaction trails. This represents a shift from cash-based laundering to advanced blockchain-enabled concealment embedded within a decentralised financial infrastructure.

#### **D. Case Studies on Cryptocurrency-Enabled Drug Trade**

**Silk Road (United States).** Silk Road was one of the earliest darknet marketplaces to use Bitcoin exclusively for narcotics transactions. It enabled thousands of anonymous drug sales before being shut down by the Federal Bureau of Investigation. The case demonstrated how cryptocurrency can sustain large-scale illegal drug markets and highlighted the major challenges of tracing decentralised financial activity.<sup>5</sup>

**AlphaBay (International Enforcement Operation).** AlphaBay operated as one of the largest darknet drug markets globally, facilitating the narcotics trade through Bitcoin and Monero. In 2017 it was dismantled through a coordinated international enforcement operation, and the investigation revealed extensive cross-border cryptocurrency flows used to process drug payments, showing the transnational complexity of cyber-enabled narcotics networks.<sup>6</sup>

### **IV. LEGAL FRAMEWORK UNDER THE NDPS ACT, 1985 AND THE INVESTIGATIVE POWERS OF THE NARCOTICS CONTROL BUREAU**

#### **A. Overview of the NDPS Act, 1985**

The Narcotic Drugs and Psychotropic Substances Act, 1985 is the principal legislation governing narcotic drugs and psychotropic substances in India. It was enacted to consolidate and strengthen narcotics-control law and to impose stringent penalties for drug-related offences, and it aligns with India's obligations under international conventions such as the Single Convention on Narcotic Drugs, 1961 and the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988. The Act adopts a strict deterrent approach, criminalising not only direct trafficking but also ancillary activities such as financing, abetment, and the facilitation of the illicit drug trade. It was, however, primarily designed for conventional trafficking networks and does not explicitly address cyber-enabled narcotics operations involving digital platforms and cryptocurrency systems.

#### **B. Offences and Punishment under the NDPS Act (Sections 8 and 15–40)**

Section 8 of the NDPS Act prohibits the cultivation, production, manufacture, possession, sale, purchase, transport, import, export, and use of narcotic drugs and psychotropic substances except for medical or scientific purposes. Sections 15 to 40 prescribe punishment for various

---

<sup>5</sup> *United States v. Ulbricht*, S.D.N.Y. (2015).

<sup>6</sup> U.S. DEP'T OF JUST., *AlphaBay Takedown Report* (2017).

offences depending on the nature and quantity of the substance involved, classified as small, intermediate, and commercial quantities,<sup>7</sup> and the Act imposes stringent penalties, including enhanced punishment for repeat offenders and organised criminal activity. Section 27A is significant because it criminalises the financing of illicit trafficking, making it relevant to cases involving digital payments and cryptocurrency-based transactions, while Section 29 extends liability to abetment and criminal conspiracy, thereby covering organised trafficking networks operating through darknet platforms and encrypted communication systems.

### **C. Investigative Powers under the NDPS Act**

The NDPS Act grants wide investigative powers to enforcement authorities to ensure effective implementation. Section 42 empowers officers to conduct search and seizure without a warrant on the basis of prior information; Section 43 allows search, seizure, and arrest in public places; and Section 50 provides safeguards during personal search to ensure procedural fairness and constitutional compliance. Sections 52 and 52A regulate the handling, custody, and disposal of seized narcotic substances so as to maintain evidentiary integrity, and Section 67 empowers officers to call for information, examine persons, and record statements during investigation. These powers are also extended in practice to cyber-enabled investigations involving electronic devices, communication records, and digital platforms, though the Act does not provide a specific procedural framework for cyber-forensic investigation.

### **D. Role and Institutional Framework of the Narcotics Control Bureau (NCB)**

The Narcotics Control Bureau is the apex coordinating agency under the Ministry of Home Affairs responsible for the enforcement of the NDPS Act, coordinating with the State police, Customs, and other enforcement agencies for narcotics-control operations. It is responsible for intelligence collection, analysis, and the coordination of investigations involving drug-trafficking networks, particularly organised syndicates operating at the national and transnational levels, and it conducts coordinated enforcement operations to dismantle such networks. In recent years the NCB has increasingly focused on cyber-enabled narcotics trafficking involving darknet marketplaces, encrypted communication platforms, and cryptocurrency-based transactions, relying on cyber-intelligence and surveillance and coordinating with forensic agencies for digital-evidence extraction and analysis, as well as cooperating with international agencies such as INTERPOL for cross-border enforcement.

---

<sup>7</sup> The Narcotic Drugs and Psychotropic Substances Act, 1985, No. 61, Acts of Parliament, 1985 (India).

### **E. Digital Dimensions of Narcotics Trafficking**

Cyber-enabled narcotics trafficking operates through darknet marketplaces, encrypted communication systems, and anonymous financial networks, with cryptocurrency a preferred mode of payment because of its pseudonymous nature and its ability to facilitate cross-border transactions. Blockchain analysis is increasingly used in investigations, though techniques such as mixers, tumblers, and privacy tools significantly complicate financial tracing. Digital evidence such as chat logs, IP addresses, and blockchain records plays a central role in modern narcotics investigations, even as anonymisation technologies limit enforcement effectiveness.

### **F. Electronic Evidence and Cyber-Investigation Challenges**

Electronic evidence in NDPS cases is governed by the Bharatiya Sakshya Adhiniyam, 2023, which recognises electronic records as admissible evidence subject to authentication, integrity, and certification requirements; such evidence includes digital communications, emails, CCTV footage, and blockchain transaction records.<sup>8</sup> Cyber-enabled narcotics investigations rely heavily on digital forensics, including the extraction of data from electronic devices and the analysis of encrypted communications and cryptocurrency transactions, but enforcement is challenged by encryption technologies, darknet anonymity tools, VPN usage, and privacy-enhancing cryptocurrencies. Ensuring a proper chain of custody for electronic evidence is essential, as any procedural lapse may affect admissibility and weaken the prosecution under the NDPS framework.

## **V. CHALLENGES FACED BY THE NARCOTICS CONTROL BUREAU IN CYBER-ENABLED NARCOTICS TRAFFICKING**

Cyber-enabled narcotics trafficking has significantly transformed enforcement under the NDPS Act, 1985. The Narcotics Control Bureau, as the apex coordinating agency, faces multiple challenges arising from technological advancement, jurisdictional complexity, operational limitations, and judicial evidentiary requirements.

### **A. Technological Challenges**

The increasing use of advanced digital technologies by offenders poses a serious challenge to enforcement agencies. Darknet marketplaces, encrypted messaging applications, VPNs, and anonymising tools such as Tor are widely used to conceal identity and location, and cryptocurrency transactions further complicate investigations by enabling pseudonymous cross-border transfers. The use of mixers, tumblers, and privacy-focused coins makes the tracing of

---

<sup>8</sup> The Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India).

illicit financial flows highly complex, reducing the effectiveness of conventional investigative methods.

### **B. Jurisdictional and Cross-Border Challenges**

Cyber-enabled narcotics offences operate across multiple jurisdictions, making it difficult to determine territorial jurisdiction under the NDPS Act, since offenders, servers, and financial systems are often located in different countries, creating legal uncertainty. Enforcement agencies rely on mutual legal assistance treaties (MLATs) and international cooperation mechanisms, but delays in data-sharing often hinder timely investigation and evidence preservation. Differences in cybercrime laws across jurisdictions further complicate enforcement and create safe havens for trafficking networks.

### **C. Operational and Institutional Challenges**

The Narcotics Control Bureau faces operational constraints such as limited cyber-forensic infrastructure, a shortage of trained digital investigators, and a lack of specialised technical tools for darknet investigations. Coordination among agencies such as the State police, Customs, cybercrime units, and financial-intelligence agencies is often delayed, affecting efficiency,<sup>9</sup> and the rapid evolution of technology makes it difficult for enforcement agencies to keep pace with emerging cyber-enabled trafficking methods.

### **D. Judicial Approach towards Cyber-Enabled Narcotics Offences**

Indian courts have adopted a strict approach in NDPS cases while ensuring procedural fairness and evidentiary discipline.

In *State of Punjab v. Baldev Singh* (1999), the Supreme Court held that the procedural safeguards under the NDPS Act are mandatory, particularly during search-and-seizure operations.<sup>10</sup> In *Tomaso Bruno v. State of Uttar Pradesh* (2015), the Court recognised the importance of electronic evidence and its growing relevance in criminal trials.<sup>11</sup> In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020), the Court reaffirmed the mandatory nature of the certification of electronic records,<sup>12</sup> and in *Anvar P.V. v. P.K. Basheer* (2014), the Court emphasised the strict certification requirements for the admissibility of electronic evidence.<sup>13</sup>

---

<sup>9</sup> INTERPOL, *Reports on Cyber-Enabled Drug Trafficking*.

<sup>10</sup> *State of Punjab v. Baldev Singh*, (1999) 6 S.C.C. 172 (India).

<sup>11</sup> *Tomaso Bruno v. State of Uttar Pradesh*, (2015) 7 S.C.C. 178 (India).

<sup>12</sup> *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 S.C.C. 1 (India).

<sup>13</sup> *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473 (India).

In *Tofan Singh v. State of Tamil Nadu* (2020), the Court held that confessional statements made to NDPS officers are inadmissible, thereby increasing reliance on independent and digital evidence,<sup>14</sup> and in *Union of India v. Mohanlal* (2016), the Court stressed the importance of maintaining a proper chain of custody in narcotics cases.<sup>15</sup> Collectively, these judgments reflect a judicial approach that balances strict enforcement of the NDPS Act with procedural safeguards, particularly in cases involving digital and electronic evidence.

### **E. Emerging Challenges in Enforcement Practice**

Despite legal and technological developments, enforcement agencies continue to face emerging challenges in cyber-enabled narcotics cases. The NDPS Act does not explicitly address darknet operations, cryptocurrency-based trafficking, or encrypted communication systems, and investigations are further complicated by the rapid evolution of digital platforms and the use of sophisticated anonymisation techniques. There is also a growing need for enhanced cyber-forensic capacity, real-time international cooperation, and specialised training for enforcement personnel, as the increasing convergence of technology and narcotics trafficking continues to outpace existing enforcement capabilities.

## **VI. REGULATORY GAPS AND REFORM MEASURES IN CYBER-ENABLED NARCOTICS ENFORCEMENT**

Cyber-enabled narcotics trafficking exposes significant limitations in India's existing legal and institutional framework. Although the Narcotic Drugs and Psychotropic Substances Act, 1985 provides a stringent structure for narcotics control, it was primarily designed for conventional drug trafficking and does not adequately address the complexities of digital drug markets operating through darknet platforms, encrypted communication systems, and cryptocurrency networks.

### **A. Limitations of the NDPS Act in the Digital Context**

The NDPS Act does not explicitly define or regulate cyber-enabled narcotics trafficking. Emerging elements such as darknet marketplaces, encrypted communication platforms, virtual currencies, and anonymisation technologies are not directly covered by the statute. As a result, enforcement agencies rely on a broad interpretation of existing provisions, particularly Sections 27A and 29, to address digital offences, which creates legal ambiguity and inconsistency in application.

---

<sup>14</sup> *Tofan Singh v. State of Tamil Nadu*, (2021) 4 S.C.C. 1 (India).

<sup>15</sup> *Union of India v. Mohanlal*, (2016) 3 S.C.C. 379 (India).

## **B. Gaps in the Cyber-Forensic and Investigative Framework**

The NDPS Act lacks a dedicated procedural framework for cyber-forensic investigations. Although general investigative powers are provided under Sections 42, 43, and 67, these were not designed for digital-evidence collection or analysis, which results in procedural uncertainty in handling encrypted devices, darknet communications, and blockchain-based transactions, and in turn affects investigative efficiency and evidentiary reliability.

## **C. Regulatory Gaps in Cryptocurrency Oversight**

Cryptocurrency has become a key instrument in cyber-enabled narcotics transactions because of its decentralised and pseudonymous nature. India, however, lacks a comprehensive regulatory mechanism specifically targeting the misuse of virtual assets for illicit drug financing. While general financial and anti-money-laundering frameworks exist, there is no real-time monitoring system for darknet-linked cryptocurrency transactions, making enforcement significantly more difficult.<sup>16</sup>

## **D. Institutional and Coordination Gaps**

Effective enforcement requires coordination among multiple agencies, such as the Narcotics Control Bureau, the State police, Customs, the Financial Intelligence Unit, and cybercrime units. Inter-agency coordination is, however, often fragmented and delayed, and international cooperation through mutual legal assistance treaties is slow, hampering timely access to cross-border digital evidence in darknet-related investigations.

## **E. Reform Measures and Policy Recommendations**

To address these challenges, the NDPS Act requires modernisation to include cyber-enabled narcotics offences explicitly, such as darknet operations, cryptocurrency-based trafficking, and encrypted digital communication networks. A dedicated cyber-narcotics investigation framework should be developed, including standardised protocols for digital-evidence collection, blockchain analysis, and darknet monitoring, and the cyber-forensic infrastructure within the Narcotics Control Bureau should be strengthened and specialised digital investigators trained. Faster international cooperation mechanisms and reforms in mutual legal assistance procedures are necessary to address the transnational nature of cyber-enabled narcotics trafficking, and regulatory oversight of cryptocurrency exchanges and digital-asset platforms must be strengthened to prevent misuse for illicit financing.

---

<sup>16</sup> FIN. ACTION TASK FORCE, *Guidance on Virtual Assets and Virtual Asset Service Providers*.

## VII. CONCLUSION AND RECOMMENDATIONS

### A. Recommendations

To address the challenges posed by cyber-enabled narcotics trafficking effectively, a multi-dimensional reform strategy is required, encompassing legal, institutional, and technological measures.

**Legislative modernisation of the NDPS Act.** The NDPS Act, 1985 should be amended to include cyber-enabled narcotics offences explicitly, such as darknet drug markets, cryptocurrency-based trafficking, and encrypted communication networks.

**Strengthening cyber-forensic infrastructure.** A dedicated cyber-narcotics forensic framework should be established with advanced capabilities in blockchain analysis, darknet monitoring, and digital-evidence extraction.

**Capacity-building of enforcement agencies.** Specialised training programmes should be implemented for Narcotics Control Bureau officials and allied agencies to enhance expertise in cyber investigations and digital-intelligence handling.

**Enhanced inter-agency coordination.** A real-time integrated mechanism should be developed among the NCB, the State police, Customs, the Financial Intelligence Unit, and cybercrime units for faster intelligence-sharing and coordinated operations.

**International cooperation.** Faster and more efficient mutual legal assistance mechanisms are required to address the transnational nature of cyber-enabled narcotics trafficking, along with stronger collaboration with global enforcement agencies.

**Regulation of the cryptocurrency ecosystem.** A comprehensive regulatory framework should be introduced to monitor virtual-asset service providers and prevent the misuse of cryptocurrencies for illicit narcotics financing.

### B. Conclusion

Cyber-enabled narcotics trafficking represents a significant evolution in the global drug trade, characterised by the use of advanced digital technologies such as darknet platforms, encrypted communication systems, and cryptocurrency transactions. This transformation has fundamentally challenged the traditional enforcement mechanisms under the NDPS Act, 1985. In India, while the Act continues to serve as a strong deterrent framework, its pre-digital structure limits its effectiveness in addressing technologically sophisticated narcotics offences, and the Narcotics Control Bureau, though central to enforcement, faces persistent challenges relating to technology, jurisdiction, and the handling of digital evidence.

Judicial developments, particularly under the Bharatiya Sakshya Adhiniyam, 2023, have strengthened the admissibility framework for electronic evidence, yet enforcement continues to struggle against the rapidly evolving cyber tools used by traffickers. Ultimately, effective control of cyber-enabled narcotics trafficking requires a coordinated approach combining legislative reform, technological advancement, institutional strengthening, and international cooperation, so that narcotics-control mechanisms remain effective in the digital era.

\*\*\*\*\*