CHALLENGES IN PROSECUTING DARK WEB DRUG OFFENDERS: ISSUES OF JURISDICTION AND EVIDENCE

by

Gaurav Kumar[1]

&

Sujata Sarkar[2]

ABSTRACT

The rise of illegal drug trade on the dark web presents serious hurdles for law enforcement and prosecutors worldwide. A key challenge is obtaining and verifying digital evidence, especially when offenders use tools like Tor, VPNs, and cryptocurrencies to mask their identities.[3] These technologies make it hard to trace criminal activities and collect evidence that courts will accept. Moreover, such evidence is often scattered across various digital platforms and countries, creating concerns about the chain of custody and reliability.

Another major difficulty lies in proving criminal intent (mens rea) in a virtual environment, where online behavior can be ambiguous and hard to interpret. Jurisdictional issues further complicate matters. Because dark web crimes cross borders, it's often unclear which country has the authority to investigate or prosecute. Differences in legal systems, privacy laws, and treaty obligations can slow down or prevent effective international cooperation.[4] Offenders take advantage of these gaps by operating from regions with weak cybercrime laws or no extradition treaties.

This paper explores these challenges in depth, critiques current global legal frameworks, and suggests improvements. These include better international coordination, updated digital evidence practices, and more precise jurisdictional rules. Tackling dark web drug crimes requires not just advanced technology but also stronger global legal cooperation to close enforcement gaps and keep up with fast-changing online drug markets.

[1] Assistant Professor, School of Law,IILM UNIVERSITY, GREATER NOIDA. EMAIL-: gaurav.kumar@iilm.edu

[2] LLM Student,School of Law, IILM UNIVERSITY, GREATER NOIDA. EMAIL-: sujata.sarkar.gnllm25@iilm.edu

[3] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

[4] Council of Europe, *Convention on Cybercrime*, opened for signature Nov. 23, 2001, E.T.S. No. 185.

Evolution of Drug Trade on the Dark Web

The advent of the dark web has revolutionized how illegal drugs are bought and sold, offering a level of secrecy and reach previously unavailable to drug traffickers. Unlike the open internet, the dark web functions through hidden encrypted networks like Tor (The Onion Router), which obscure a user's identity and location. Originally developed for secure communication, Tor was soon adapted by criminal networks who saw its potential for conducting illicit activities beyond the gaze of authorities.

One of the first major platforms that capitalized on this technology was Silk Road, launched in 2011 by Ross Ulbricht. [5]Operating like an underground version of Amazon, it allowed users to browse, buy, and sell a variety of illegal drugs anonymously. All transactions were conducted using Bitcoin, a digital currency that further removed the need for traceable financial intermediaries. Although law enforcement eventually shut down Silk Road, it sparked the creation of newer platforms like AlphaBay, Agora, and Dream Market. Each of these built upon the previous one's security and operational design, making detection and takedown increasingly difficult.

These platforms flourished due to several key technologies. The Tor network makes it nearly impossible to trace internet traffic back to its source by rerouting connections through multiple global servers. Peer-to-peer (P2P) systems and blockchain-based payments added another layer of complexity, helping traffickers send and receive funds without relying on formal banking channels.[6]Secure communication tools like end-to-end encryption further protected user exchanges from surveillance.

[5] Andy Greenberg, *The Untold Story of Silk Road, Part 1: The Rise,* WIRED (May 18, 2015), https://www.wired.com/2015/05/silk-road-1/.

[6] Michael Chertoff & Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security,* 6 GLOBAL COMM'N ON INTERNET GOVERNANCE 1 (2015), https://www.cigionline.org/sites/default/files/gcig_n o6web.pdf.

One surprising element in this hidden ecosystem is the introduction of customer feedback systems. Much like on legal online marketplaces, buyers could rate sellers based on service, quality, and delivery, which built a degree of trust and reliability. This eliminated the risks of street-level drug buying and created a self-regulating community where reputation mattered.[7]

The dark web also enabled access for people in remote or conservative regions, where physical drug markets may be inaccessible or dangerous. With just an internet connection and cryptocurrency, users could order narcotics discreetly, which contributed to a rise in consumption—especially among younger, tech-savvy individuals. Studies have shown that many users believed drugs bought on these platforms were purer or safer than street alternatives.

Unlike traditional narcotics trafficking that involves smuggling across borders or hand-to-hand deals, dark web transactions often require minimal physical interaction. Drugs are typically shipped through standard postal services in inconspicuous packaging, making detection harder for authorities.

So, the digital shift in the drug trade has added a new layer of complexity to law enforcement's efforts. The combination of anonymity tools, decentralized platforms, and global accessibility has created a resilient underground economy. As new marketplaces emerge and evolve, the legal system and enforcement technologies must also advance to keep pace with this constantly adapting threat.

---

[7] James Martin, *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs* 32–45 (2014).

Legal Frameworks Governing Cyber Narcotics

With the rapid evolution of digital technologies, narcotics trafficking has moved into cyberspace, creating new challenges for existing legal systems. The use of the dark web, cryptocurrency, and encryption tools in drug trade has significantly weakened the effectiveness of traditional enforcement models. To address these changes, several legal mechanisms—both at the national and international levels—have been developed or adapted. In India, the key frameworks include the Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act), the Information Technology Act, 2000 (IT Act), and the newly introduced Bharatiya Sakshya Adhiniyam, 2023 (BSA). International instruments such as UN conventions, along with legal systems in the United States and the European Union, offer comparative insights and models for cooperation.

The NDPS Act is India's primary law for regulating narcotic and psychotropic substances.[8] It criminalizes activities such as manufacturing, transporting, selling, and using these substances. While the Act effectively covers conventional drug trafficking, it was not originally designed with digital or cyber-based transactions in mind. However, certain provisions—like Section 8(c), in conjunction with Sections 22 and 27A—have been interpreted to support actions against drug trafficking involving digital tools. When digital evidence is available, these sections can be used to prosecute offenders operating online. In recent years, agencies like the Narcotics Control Bureau (NCB) have started using cyber intelligence to identify and disrupt drug networks on the dark web. Still, the Act lacks specific language dealing with internet-based drug crimes, limiting its reach in this evolving area.

The United Nations Office on Drugs and Crime (UNODC) has recently published guidelines aimed at tackling drug markets on the darknet. These guidelines highlight the importance of using digital forensic tools to investigate and dismantle such networks. [9]

[8] Narcotic Drugs and Psychotropic Substances Act, 1985, No. 61, Acts of Parliament, 1985 (India).
[9] U.N. Office on Drugs & Crime, Darknet Markets: Monitoring and Investigating (Practical Guide), U.N. Doc. V.21-01593 (2021), https://www.unodc.org/documents/organized-crime/darknet/UNODC_Darknet_Practical_Guide_2021.pdf.

In contrast, the United States follows a more technology-driven and agency-coordinated model. Through bodies like the Drug Enforcement Administration (DEA), and laws including the Controlled Substances Act and the Computer Fraud and Abuse Act (CFAA), the U.S. has adopted an aggressive posture against cyber narcotics. Notable crackdowns such as "Operation Disruptor" and "Operation Darknet" have demonstrated how federal agencies employ sophisticated techniques—such as cryptocurrency tracing, digital forensics, and international collaborations—to combat darknet drug markets. The U.S. legal system also allows civil forfeiture, enabling authorities to seize assets such as digital wallets linked to illicit drug trades.

In the European Union, the legal response is coordinated under frameworks like the EU Drugs Strategy and Action Plan. This policy emphasizes the growing threat of cyber-enabled drug trafficking and prioritizes intelligence sharing among EU member states. Agencies like Europol and Eurojust are central to efforts targeting drug crimes conducted over the dark web. The Budapest Convention on Cybercrime, also known as the European Convention on Cybercrime, serves as a cornerstone for international cooperation in digital crime investigations. [10]Although India has not signed this convention, its structure and principles are often studied for guidance in building domestic legal standards.

One of the most difficult obstacles to international cooperation is the lack of uniformity in how countries define and enforce laws against cyber narcotics. Privacy laws, encryption standards, and admissibility rules for digital evidence vary widely. For instance, while nations like the U.S. employ proactive cyber monitoring, countries such as Germany or Switzerland are more cautious due to strict data privacy norms, limiting surveillance efforts.

So, while India possesses certain legal instruments to tackle online drug trafficking, these are not fully suited to meet the challenges of today's digital drug networks. There is a need to either

[10] Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention).

amend the NDPS Act or introduce a dedicated statute that focuses specifically on cyber narcotics. Alongside this, India's role in global treaty frameworks must be strengthened, ensuring its domestic laws are aligned with international standards. Combating drug crimes in cyberspace requires not only updated legal mechanisms but also stronger technology, institutions, and global partnerships.

Collection and Admissibility of Digital Evidence

As crimes move increasingly into the digital domain—especially with the growth of the dark web—digital evidence has become central to criminal investigations and trials. However, due to its fragile and intangible nature, collecting and presenting such evidence in court involves unique technical and legal challenges. In cases involving cyber narcotics, where transactions are masked by encryption, anonymity tools, and cryptocurrency, the handling of digital evidence requires a high level of precision and compliance with legal protocols.

Digital evidence can include a wide range of items such as email records, IP logs, chat histories, cryptocurrency transactions, device metadata, and more. Law enforcement agencies often rely on advanced forensic tools like EnCase, FTK, and Cellebrite to collect and preserve such data from devices and networks without altering the original content.[11] Maintaining the integrity of this evidence from the point of seizure to courtroom presentation is crucial for its admissibility.

One foundational principle is maintaining a proper chain of custody. This means documenting every stage of evidence handling, from the initial discovery through each handover. If even a single step in the chain is missing or unclear, questions of tampering or manipulation may arise. In cybercrime cases, where devices and data can be easily accessed or altered, courts are

[11] Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet 207–223* (3d ed. 2011).

especially cautious and demand strict procedural compliance. “Courts now increasingly rely on hash values to determine whether the evidence presented is original and unaltered.”[12]

A technical safeguard used to verify digital integrity is the generation of hash values—unique digital fingerprints of files created by algorithms like MD5 or SHA-256. These hashes ensure that the file hasn't been modified: any change to the original file, even a single character, results in a different hash value. Investigators calculate these values before and after handling the file to confirm that the evidence remains untouched.

Indian law has evolved to accommodate the specific needs of digital crime cases. Initially, the Indian Evidence Act, 1872, through Section 65B, provided the legal basis for admitting electronic records. This section required a certificate affirming the source and authenticity of the data, usually from someone in charge of the device or system where the data was stored. This was essential to ensure that digital records were not tampered with or fabricated.

With the introduction of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the legal framework has become more attuned to modern digital crime realities. The BSA formally recognizes digital records as documents and raises the bar for admissibility. It stresses that screenshots or printouts alone are insufficient unless supported by metadata and expert verification. Forensic processes and certifications are now vital, especially when dealing with sophisticated networks such as the dark web or blockchain.

The BSA also emphasizes that electronic evidence must not only be relevant to the case but also reliable. Technical reliability means the evidence has not been altered, while procedural reliability concerns whether the evidence was collected lawfully and properly. In complex cases, such as tracing a crypto wallet used in a drug transaction, investigators must also link

[12] National Institute of Standards and Technology, Guide to Integrating Forensic Techniques into Incident Response, SP 800-86 (2006), https://csrc.nist.gov/publications/detail/sp/800-86/fi-nal.

the digital evidence to the accused—often requiring supporting material like login credentials, IP logs, and communication records.

Judicial pronouncements in India have significantly influenced how digital evidence is treated. In **Anvar P.V. v. P.K. Basheer (2014),**[13] the Supreme Court ruled that electronic records are admissible only with a proper Section 65B certificate, treating such records as secondary evidence. Later, in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020),**[14] the Court clarified that even if there is no dispute over authenticity, the procedural requirement of Section 65B must still be fulfilled unless the original device is presented.

Despite these developments, real-world challenges persist. Much digital evidence is stored across borders, and retrieving it from foreign servers often requires mutual legal assistance or compliance with international data-sharing rules. Privacy laws in other jurisdictions can delay or even prevent access. Tools like end-to-end encryption, disappearing messages, and anonymizing platforms such as Tor make surveillance and attribution even more difficult.

To overcome these challenges, India needs to build more capacity in cyber forensics and improve the training of law enforcement, prosecutors, and judicial officers. Institutions like CERT-IN and the National Cyber Forensics Laboratory have been instrumental, but more standardized protocols and investment are necessary. International models, such as the Budapest Convention on Cybercrime, though not signed by India, offer useful benchmarks for reform and collaboration.

In summary, digital evidence plays a critical role in prosecuting cyber narcotics cases. Its credibility depends on sound forensic techniques, legal safeguards like hash values and chain of custody, and compliance with evidentiary standards under laws like the BSA. As dark web-

[13] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (India).
[14] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

related drug trafficking expands, it is essential that India's legal and investigative framework continues to evolve to ensure effective and lawful prosecutions.

Proving Mens Rea in Virtual Environments

In criminal jurisprudence, mens rea, or the guilty mind, is an essential element required to establish a person's criminal responsibility. It encompasses mental states such as intent, knowledge, recklessness, or negligence at the time of committing an offense. While in traditional crimes, establishing mens rea may rely on direct testimony, behavior, or contextual clues, the digital environment presents unique challenges in identifying and proving a person's mental state. As crimes increasingly shift to cyberspace— particularly in areas like dark web drug trafficking—courts and investigators must adopt new methods to assess intent amid anonymity and technical complexity.

One of the biggest obstacles in cybercrime cases is the anonymity the internet provides.Individuals engaging in online transactions can hide behind pseudonyms, spoofed IP addresses, or encrypted messaging platforms. As a result, even when illegal activity is detected, proving that a specific individual acted with intent becomes difficult.[15] For instance, in dark web drug transactions, a person could argue that their account was compromised or accessed without their knowledge—raising questions about their awareness or consent.

Unlike in-person transactions, where intent might be inferred from physical cues like gestures, conversations, or suspicious behavior, online actions often lack context.

[15] Orin S. Kerr, *Attribution and the Dif iculty of Proving Identity in Cyberspace*, 102 IOWA L. REV. 517 (2017).

Communications are usually brief, encrypted, or carried out through automated systems. This leaves little for prosecutors to work with when attempting to demonstrate the mental element of a crime.

Complicating matters further, many darknet platforms operate using automated software that facilitates sales without direct input from the seller for each transaction. In such cases, investigators must determine whether the accused knowingly used or programmed such tools to facilitate illegal trade. Additionally, when multiple users share a network or a single device, it becomes critical to establish who was responsible for the specific digital actions in question.

Under Indian law, the burden of proof lies on the prosecution to establish guilt beyond a reasonable doubt. When mens rea is involved, this includes demonstrating not only that the act was committed (actus reus) but also that it was done with the required mental state. To prove this in cyber narcotics cases, investigators often trace digital communications, track cryptocurrency movements, analyze browsing patterns, and connect digital footprints to the accused. However, this evidence must be legally admissible and free from suspicion of manipulation, in line with the procedural requirements of the Bharatiya Sakshya Adhiniyam (BSA).

Indian courts have gradually begun recognizing the complexities in proving digital intent. In **State of Tamil Nadu v. Suhas Katti (2004),** the court accepted electronic communications like emails and chat logs as valid indicators of intent, marking one of the earliest instances where
digital mens rea was acknowledged. More recently, in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020),**[16] the Supreme Court reaffirmed the strict need for procedural compliance when presenting electronic evidence, emphasizing that even undisputed digital records must meet the formalities under Section 65B or its BSA equivalent.

[16] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).

Defendants in digital crime cases often rely on defenses such as lack of technical knowledge, unintentional exposure to illicit content, or mistaken identity. Courts must then evaluate whether these defenses are credible or a means to evade liability. Expert testimony, digital behavior analysis, and sometimes circumstantial indicators are used to assess the truth of such claims.

In the absence of direct evidence, prosecutors often turn to circumstantial patterns. Multiple logins to illegal platforms, possession of privacy tools like VPNs, frequent use of crypto wallets associated with illegal trades, or conversations with known offenders can collectively build a case pointing to intentional wrongdoing. "Though not direct evidence, such circumstantial links can help establish a pattern consistent with knowledge and willfulness."[17]

Given the rapid evolution of digital crime, there is a growing need for tailored legal standards on how mens rea should be inferred in the cyber domain. Legal professionals must be trained to understand digital behavior and apply forensic evidence effectively. Expert witnesses who can translate complex technical activity into legally meaningful insights will likely play a bigger role in future trials.

In essence, proving mens rea in virtual environments demands a combination of digital literacy, investigative accuracy, and legal adaptability. As criminal activities increasingly shift into the digital realm, the tools and approaches for proving intent must also evolve to ensure justice is effectively served in the virtual age.

Jurisdictional Dilemmas in Cross-Border Cybercrimes

[17] Susan W. Brenner, *Cybercrime: Re-thinking Crime Control Strategies*, 8 J. HIGH TECH. L. 1, 18–20 (2008).

The surge in cybercrimes, especially those involving dark web drug trafficking, has exposed critical gaps in global legal systems. The internet's borderless nature allows individuals to commit crimes in one country, store data in another, and affect victims elsewhere—all at the same time. This multi-jurisdictional dynamic raises pressing questions: which country has the legal authority to investigate and prosecute such offenses? The challenge intensifies when anonymity tools and cryptocurrencies obscure both the offender's identity and location.

Most countries operate on the principle of territorial jurisdiction, meaning they enforce laws within their own geographical boundaries. According to this principle, a country may prosecute an offense only if it occurs within its borders or has a significant link to them. For instance, if a person in India uses the internet to sell drugs to someone in the U.S., Indian authorities could assert jurisdiction based on the perpetrator's presence in India. However, if key evidence, collaborators, or infrastructure lie outside Indian territory, the effectiveness of such jurisdiction weakens.

To fill this gap, the idea of extraterritorial jurisdiction is applied. This allows a state to act against crimes committed beyond its borders under specific conditions. In India, Section 4 of the Indian Penal Code, 1860 permits such action, especially if the accused is an Indian national or the victim is Indian.[18] Yet, asserting this type of jurisdiction in cybercrime cases often requires foreign cooperation, which isn't always forthcoming. Cybercriminals frequently operate from countries with weak enforcement or no extradition arrangements, making prosecution difficult or impossible.

Another layer of complexity is added by the conflict of laws between nations. Each jurisdiction has its own rules on data protection, privacy, evidence collection, and criminal procedures. These legal differences can delay or even obstruct investigations. For example, a dark web marketplace's servers might be hosted in a European country with strong privacy protections, making it hard for Indian authorities to gain access. Even with Mutual Legal Assistance Treaties (MLATs) in place, bureaucratic hurdles and slow diplomatic communication can hinder timely data exchange.

[18] Indian Penal Code, 1860, § 4.

Extradition is yet another challenge. If a suspect resides in a country without an extradition treaty—or where the alleged offense isn't recognized as a crime—the process may stall indefinitely. Additionally, when criminals use cryptocurrency for drug transactions, their activities can become untraceable, further complicating efforts to assign jurisdiction. In some cases, multiple countries may claim jurisdiction over the same offender, which can lead to diplomatic conflicts and procedural confusion.

To navigate these jurisdictional dilemmas, international agreements like the Budapest Convention on Cybercrime aim to establish a cooperative legal structure for investigating and prosecuting cyber offenses.[19] The Convention encourages member countries to harmonize their cyber laws and share data. However, India is not a party to this treaty, which limits its ability to benefit from the Convention's legal tools and global collaboration framework.

Nevertheless, India has signed various bilateral and multilateral agreements aimed at improving cooperation in cyber investigations, though implementation often falls short.

One of the unresolved legal questions in cybercrime cases is how to determine the "location" of the offense. Courts worldwide differ in approach—some prioritize the server's location, others focus on where the victim is harmed, and some consider the origin of the criminal act. Indian laws, including the Information Technology Act, 2000, and the NDPS Act, allow jurisdiction if the crime has a connection to India—whether through the offender, the digital infrastructure, or the victim. Yet, such claims can be difficult to enforce internationally if they're not supported by reciprocal legal recognition.

Modern cloud computing and offshore data storage further complicate matters. Service providers may refuse to share user data without a local court order, citing data sovereignty or compliance with home-country laws. A landmark example is the Microsoft Ireland case, where U.S. authorities sought access to data stored on servers in Ireland. The legal conflict highlighted the tension between national sovereignty, individual privacy, and law enforcement demands.[20]

[19] Council of Europe, Convention on Cybercrime, opened for signature Nov. 23, 2001, E.T.S. No. 185 [Budapest Convention].

[20] In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

In sum, cybercrime and dark web drug offenses challenge traditional ideas of legal jurisdiction. The friction between territorial and extraterritorial claims, combined with inconsistent international laws and fragile cooperation systems, creates a major gap in enforcement. To close this gap, India and other nations must reform cybercrime legislation, strengthen diplomatic and legal cooperation mechanisms, and become more involved in international agreements. Only through coordinated global efforts can jurisdictional uncertainties in cybercrime cases be effectively resolved.

Role of Cryptocurrency in Drug Transactions

Cryptocurrencies have transformed the way financial transactions are conducted by offering decentralized, secure, and pseudonymous channels for transferring value. While this innovation has enabled growth in fintech and international commerce, it has also created opportunities for illegal use—especially in cyber narcotics markets. On dark web platforms, digital currencies such as Bitcoin, Monero, and Ethereum are widely used to facilitate drug sales.[21] These currencies offer a way to bypass traditional banking systems and obscure the identities of the parties involved, making them ideal for illicit trade.

At the core of this ecosystem is blockchain technology, which supports most cryptocurrencies. For instance, Bitcoin transactions are recorded on a public ledger accessible to anyone, but users are only identified by cryptographic wallet addresses. This system offers transparency in record-keeping while maintaining pseudonymity for participants. In the context of dark web drug transactions, buyers send cryptocurrency directly to sellers, who then ship the drugs through standard postal systems, often disguised in everyday packaging to avoid detection.

To further erase transaction trails, many traffickers use Bitcoin mixers—also known as tumblers. These services combine funds from multiple sources and redistribute them through a

[21] Joon Ian Wong, *The Dark Web's Favorite Currency Is Bitcoin, and It's Making Law Enforcement's Job Harder,* QUARTZ (July 19, 2017), https://qz.com/1031940/.

series of micro-transactions. This process makes it difficult to trace a direct link between the sender and recipient. Additionally, some drug vendors opt for privacy-oriented cryptocurrencies like Monero and ZCash, which conceal transaction histories entirely, making law enforcement's job even more challenging. So in this way it breaks the transaction link between sender and receiver, making it extremely difficult for law enforcement agencies to trace the origin of the funds.[22]

The legal status of cryptocurrency in India remains ambiguous. The Reserve Bank of India (RBI) had previously barred banks from facilitating cryptocurrency transactions, but this restriction was struck down by the Supreme Court in the 2020 case of Internet and Mobile Association of India v. RBI.[23] Currently, India has not outlawed the use or possession of cryptocurrencies. However, the government has taken steps to regulate digital assets under taxation laws, including mandatory disclosure of virtual asset holdings under the Income Tax Act, 1961.

Despite these regulatory measures, there is still no specific law in India criminalizing the use of cryptocurrency in drug-related activities. The NDPS Act and the Information Technology Act, 2000 do not directly address cryptocurrency transactions. As a result, law enforcement agencies rely on indirect evidence such as screenshots of transactions, communication records, and wallet IDs. Newer tools in blockchain forensics are being used to follow money trails, but these efforts often face resistance from overseas crypto exchanges and are complicated further by mixing services that obscure the origin of funds and they are often hindered by the use of mixing services and international crypto exchanges that do not cooperate with Indian authorities." [24]

In summary, cryptocurrencies play a pivotal role in facilitating drug trades over the dark web due to their decentralized design and limited traceability. While Indian authorities are developing technical expertise to investigate such crimes, the absence of a clear legal framework around the use of cryptocurrency in cyber narcotics remains a serious gap. To

[22] Michael del Castillo, Bitcoin Mixing Services Tumble Privacy and Risk, FORBES (Oct. 26, 2016),https://www.forbes.com/sites/michaeldelcastillo/2016/10/26/bitcoin-mixing.
[23] Internet & Mobile Ass'n of India v. Reserve Bank of India, (2020) 10 SCC 274 (India).
[24] U.N. Office on Drugs & Crime, Cryptocurrencies and the Dark Web: A Critical Emerging Challenge for Law Enforcement (2020), https://www.unodc.org/documents/data-and-analysis/tocta/2020/Ch6_Cryptocurrencies_UNODC_TOCTA2020.pdf.

ensure more effective enforcement and prosecution, India must move toward creating specific laws addressing the role of virtual currencies in digital drug trafficking.

Cooperation Mechanisms: Interpol, MLATs, and Cybercrime Units

Cybercrimes that span multiple countries—particularly those involving the dark web and illicit drug trafficking—require strong international cooperation. Without coordinated efforts between nations, investigations often stall due to jurisdictional obstacles, legal conflicts, and delays in information exchange. While tools like Interpol coordination, Mutual Legal Assistance Treaties (MLATs), and specialized cybercrime task forces are in place, they are often too slow or limited in scope to counter the speed and anonymity of online criminal networks.

Interpol plays a pivotal role in linking law enforcement agencies worldwide. Through its Cybercrime Directorate and the secure I-24/7 global police network, it enables real-time sharing of intelligence, including IP data, threat assessments, and criminal profiles. Interpol also issues Red Notices to alert member nations about wanted individuals. "Interpol facilitates real-time information exchange, issues notices (such as Red Notices), and conducts joint operations."[25] In cases involving dark web drug markets, Interpol can assist national agencies in tracing activity across borders, analyzing cryptocurrency flows, and identifying darknet vendors. However, Interpol itself cannot enforce laws—it relies entirely on member states to act on the intelligence provided, and their willingness often depends on national priorities and legal systems.

Mutual Legal Assistance Treaties (MLATs) are formal agreements that allow one country to request legal cooperation from another, such as obtaining digital records, accessing foreign-hosted servers, or identifying account holders. While MLATs are vital tools, their practical

[25]INTERPOL,Cybercrime,https://www.interpol.int/en/Crimes/Cybercrime (last visited May 6, 2025).

implementation is often sluggish. Requests can take weeks or even months to process, during which time critical evidence may vanish. In cyber narcotics cases, where messages may be deleted and crypto assets moved quickly, these delays can undermine the entire investigation. So, "In practice, however, MLATs are plagued by delays, bureaucratic red tape, and diplomatic complications."[26] In some cases, countries with strict data privacy laws, like Germany or Switzerland, may reject requests unless their domestic legal standards are met, creating further friction.

One notable example of successful cross-border cooperation was during the Silk Road investigation, where U.S. agencies had to collaborate with multiple countries to trace Bitcoin transactions and identify suspects.[27] Similar efforts involving Indian law enforcement often run into roadblocks, such as differences in crime classification, lack of treaties, or limited political will from the other country.

Within India, cybercrime units have been developed at both central and state levels. The Cyber Crime Coordination Centre (I4C) and the National Cyber Crime Reporting Portal are part of an effort to centralize the reporting and analysis of digital offenses. These units have played a growing role in tackling cyber narcotics, but their ability to act internationally is constrained. When Indian authorities reach out to global platforms like WhatsApp, Telegram, or foreign crypto exchanges, responses are often delayed—or ignored—due to jurisdictional conflicts or absence of a legal obligation to comply.

To address these limitations, countries are increasingly turning to bilateral agreements, expedited legal channels, and participation in multilateral frameworks. While India is not currently a party to the **Budapest Convention on Cybercrime,** several of its recommended

[26] Bert-Jaap Koops & Morag Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation, 14 U.ST. THOMAS L.J. 647, 655–60 (2018).

[27] U.S. Dep't of Justice, Ross Ulbricht, Founder and Operator of Silk Road Website, Found Guilty on All Counts (Feb. 4, 2015), https://www.justice.gov/usao-sdny/pr/ross-ulbricht-founder-and-operator-silk-road-website-found-guilty-all-counts.

practices—such as rapid preservation requests and the creation of 24/7 contact points—can still be voluntarily adopted to strengthen international collaboration. [28]

In turn , while Interpol, MLATs, and cybercrime units serve as critical tools in the global response to cyber narcotics, their current structure is not agile enough to keep pace with the complexities of digital crime. There is an urgent need for reforms, including enhanced diplomatic coordination, harmonization of legal procedures, and investment in technology that enables faster, more effective responses. Only then can these cooperation mechanisms function as effective barriers to cyber-enabled drug trafficking.

Role of Undercover Operations and Ethical Dilemmas

Undercover operations have historically played an important role in narcotics enforcement. As drug trafficking moves to the digital sphere, law enforcement agencies have adapted by deploying undercover cyber agents who operate covertly within online drug markets, encrypted chat forums, and darknet platforms. These agents interact with suspects under false identities, gather intelligence, monitor illegal activities, and occasionally conduct controlled purchases to secure evidence. While effective in uncovering criminal networks, such operations raise several legal and ethical questions.

The dark web's structure—where users operate anonymously and communications are heavily encrypted—creates a unique challenge. Officers posing as buyers or sellers often need to mimic criminal behavior to gain credibility and access. In the process, they may use deceptive tactics or, in rare cases, become involved in illegal transactions to maintain their cover. This raises concerns about the line between legitimate investigation and entrapment—a situation where law enforcement may induce someone to commit a crime they wouldn't have otherwise

[28] Council of Europe, Convention on Cybercrime, opened for signature Nov. 23, 2001, E.T.S. No. 185.

committed. "These operations help agencies uncover organized crime groups, trace cryptocurrency flows, and collect digital evidence." [29]

A central legal issue is the admissibility of evidence gathered during such undercover activities. Courts are tasked with determining whether the law was followed during the operation and whether the rights of the accused were respected. If the methods used were seen as coercive or misleading, the defense may argue that the evidence is inadmissible. "It may be argued that the evidence was obtained unfairly or that the accused was entrapped into committing a crime they otherwise wouldn't have committed."[30] Indian courts have generally permitted evidence from covert cyber operations, provided there is clear documentation and adherence to procedural norms. However, judicial scrutiny remains strict to avoid potential misuse.

Human rights concerns also arise from these operations. In digital environments, surveillance can be far-reaching, and individuals not under suspicion may also be monitored or exposed. Without strict legal oversight, such practices risk violating privacy rights and due process. The absence of a specific legal framework in India governing undercover cyber operations makes this area particularly vulnerable to overreach. [31]

Given the growing reliance on covert tactics in cyberspace, there is a pressing need for a dedicated statutory framework to regulate digital undercover work. This should include clear limits on permissible actions, provisions for judicial oversight, safeguards for individual rights, and mechanisms to ensure accountability. Only then can such operations be carried out effectively without compromising ethical standards or constitutional protections.

In conclusion, while undercover cyber operations are a necessary tool in fighting online drug trafficking, they must be balanced with respect for legal boundaries and human rights. Ethical conduct, transparency, and proper regulation are essential to ensuring that the pursuit of justice does not come at the cost of fairness or abuse of power.

[29] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/iocta-report (last visited May 6, 2025).

[30] S. R. Sharma, *Admissibility of Evidence Collected Through Undercover Operations:* An Analysis in the Context of Indian Law, 7 INDIAN J.L. & PUB. POL'Y 42, 45–48 (2020).

[31] U.N. Human Rights Council, The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/39/29(2018),https://undocs.org/A/HRC/39/29 .

Impact of AI and Digital Surveillance on Enforcement

The integration of Artificial Intelligence (AI) and digital surveillance into law enforcement strategies has significantly changed how cybercrimes, particularly dark web drug trafficking, are investigated. With traditional methods often falling short in the face of anonymized platforms, encrypted messages, and cryptocurrency-based transactions, law enforcement agencies around the world are turning to advanced technologies to keep pace. These tools enable real-time monitoring, pattern recognition, and intelligent targeting—but they also raise serious legal, ethical, and privacy concerns.

Predictive policing, powered by AI and machine learning, allows authorities to forecast potential criminal activity using historical crime data, behavioral trends, and digital indicators.[32] In cyber narcotics cases, AI systems can flag suspicious searches, analyze patterns in cryptocurrency wallets, and track repeat offenders across various darknet platforms. By identifying likely threats early, agencies can better allocate resources and respond more effectively.

AI is also proving valuable in scanning darknet marketplaces, where automated systems search hidden networks like Tor for keywords, listings, and activity linked to drug trafficking. These tools collect data from anonymous websites, track language patterns, and generate leads that would be nearly impossible to find manually. Since many darknet markets constantly shift or rebrand, the speed and scope offered by AI gives law enforcement a strategic edge in spotting trends and responding before drugs make their way into communities.[33]

[32] INTERPOL, Artificial Intelligence and Robotics for Law Enforcement (2019), https://www.interpol.int/en/News-and-Events/News/2019/INTERPOL-report-examines-use-of-AI-and-robotics-in-law-enforcement .

[33] Europol, IOCTA 2023: Internet Organised Crime ThreatAssessment,https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023(last visited May 6, 2025)

However, these technological advances come with significant privacy risks. Surveillance systems that monitor digital behavior without proper oversight can easily infringe on civil liberties—particularly the right to privacy, freedom of expression, and protection from arbitrary searches. In India, where legal frameworks regulating AI in policing are still underdeveloped, there is a lack of clarity on how data should be handled, how long it can be stored, and under what conditions it may be shared. This regulatory gap creates the potential for misuse.

Another challenge is the potential for bias in AI algorithms. If the data used to train these systems reflects existing inequalities or inaccuracies, the results may disproportionately target specific groups or locations, leading to unfair scrutiny or even wrongful investigations.[34] Relying on such systems without critical oversight risks undermining constitutional safeguards and public trust.

Looking ahead, the deployment of AI in law enforcement must be guided by clear and enforceable policies. This includes establishing ethical review boards, updating legislation to include AI-specific safeguards, and ensuring that digital evidence is assessed under fair judicial standards. Surveillance technologies should support, not substitute, investigative reasoning—and must always be applied with transparency and accountability.

To conclude, while AI and digital surveillance offer powerful tools in the battle against dark web drug trafficking, they must operate within a framework that respects individual rights and upholds the rule of law. A balanced approach—embracing innovation while ensuring fairness, privacy, and legal clarity—is essential to creating a sustainable and just model for enforcement in the digital age.

Conclusion

[34] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor 133–138 (2018).

The growing threat of dark web drug trafficking has introduced a new layer of complexity for legal systems, enforcement bodies, and international governance structures. Unlike conventional drug crimes, these operations are highly decentralized, masked by anonymity, and stretch across borders—making them especially hard to track, investigate, or prosecute using traditional methods. Technologies such as Tor, cryptocurrency, and encrypted messaging have enabled a digital marketplace that often lies beyond the effective reach of existing law enforcement tools.[35]

This study has shown that while laws like the NDPS Act, the Information Technology Act, and the Bharatiya Sakshya Adhiniyam offer an important legal base in India, they fall short of fully addressing the intricacies posed by cyber narcotics.[36] Jurisdictional disputes, slow mutual legal assistance processes, and inconsistencies in national legal standards remain significant obstacles to effective international collaboration. On the other hand, newer tools—like AI-driven analysis, blockchain tracing, and covert cyber operations—have expanded the investigative toolkit but must be applied within a legal and ethical framework that upholds civil liberties.

The need for policy reform is pressing. India must revise and expand its legal codes to specifically address online drug markets, virtual currency transactions, and digital evidence from foreign jurisdictions. Internationally, there is a strong case for aligning cybercrime laws, updating treaties such as the Budapest Convention, and developing specialized international mechanisms to address the specific challenges of cyber-enabled drug crimes.

Ultimately, defeating the challenge of dark web drug trafficking requires more than isolated national efforts. It demands a collective, tech-savvy, and legally robust response—one that fosters cooperation among countries while respecting their individual sovereignty. Without such a harmonized strategy, the law risks falling behind as criminal enterprises continue to exploit digital loopholes. A united front, driven by innovation and guided by justice, is the only sustainable path forward in addressing this complex and evolving global threat.

---

[35] U.N. Office on Drugs & Crime, Cryptocurrencies and the Dark Web: A Critical Emerging Challenge for Law Enforcement (2020), https://www.unodc.org/documents/data-and-analysis/tocta/2020/Ch6_Cryptocurrencies_UNODC_TOCTA2020.pdf

[36] Prashant Mali, *Cyber Law & Cyber Crimes*, 2nd ed. (2017).


Journal of Multi-Disciplinary
Legal Research