VOLUME 7 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

ILLEGAL DRUG TRADE THROUGH THE DARK WEB: LEGAL AND ENFORCEMENT CHALLENGES IN INDIA

- Karolin C[1]

ABSTRACT:

The rapid growth of digital technology has changed the way crimes are committed, including the illegal trade of drugs through the dark web. The dark web allows users to remain anonymous by using encrypted networks and cryptocurrencies, making it difficult for law enforcement agencies to identify offenders and trace illegal transactions. In India, this emerging form of cyber-enabled drug trafficking has created serious legal and enforcement challenges. This research examines the issue from a legal perspective by analysing the effectiveness of the Narcotic Drugs and Psychotropic Substances Act, 1985**, the** Information Technology Act, 2000**, the** Bharatiya Nyaya Sanhita, 2023, and other relevant laws in addressing dark web drug offences. The study also discusses the practical difficulties faced by investigating agencies, such as collecting digital evidence, tracking cryptocurrency transactions, dealing with cross-border crimes, and ensuring international cooperation. Using a doctrinal research methodology, the paper relies on statutes, judicial decisions, government reports, and academic literature to evaluate the strengths and weaknesses of the existing legal framework. The study finds that although India has laws to punish drug-related offences, they are not fully equipped to deal with the unique challenges of the dark web. It concludes that stronger cyber laws, better digital forensic facilities, specialised training for law enforcement agencies, and improved international cooperation are necessary to effectively combat illegal drug trade through the dark web while protecting the principles of justice, due process, and the rule of law.

INTRODUCTION:

[1] Student at School of Excellence in Law, Chennai

© 2023 International Journal of Advanced Legal Research

The internet has become an important part of everyday life, but it has also created new ways for criminals to commit offences. One such development is the use of the dark web for the illegal sale and purchase of drugs. The dark web is a hidden part of the internet that cannot be accessed through ordinary search engines. It provides users with a high level of anonymity through encrypted networks and cryptocurrencies, making it difficult for law enforcement agencies to identify offenders.

In recent years, the illegal drug trade through the dark web has become a growing concern across the world, including in India. Drug traffickers use online marketplaces to sell narcotic drugs, while buyers can purchase them without revealing their identities. This creates serious challenges for law enforcement agencies in detecting crimes, collecting digital evidence, tracing cryptocurrency transactions, and dealing with cross-border criminal networks.

India has enacted laws such as the Narcotic Drugs and Psychotropic Substances Act, 1985, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 to address drug-related and cyber offences. However, the rapid growth of technology has exposed certain gaps in the existing legal and enforcement framework. This study examines these legal and practical challenges and suggests measures to strengthen India's response to dark web drug trafficking while protecting the rule of law and public safety.

RESEARCH OBJECTIVE:

- To examine the concept, evolution, and functioning of the dark web and its role in facilitating illegal drug trafficking.
- To analyse the legal framework governing illegal drug trade through the dark web in India, particularly the Narcotic Drugs and Psychotropic Substances Act, 1985, the Information Technology Act, 2000, and other relevant laws.
- To identify the legal and enforcement challenges faced by Indian authorities in investigating and prosecuting dark web drug-related offences.
- To analyse the ethical and constitutional issues relating to privacy, surveillance, and digital investigations in the context of dark web crimes.

© 2023 International Journal of Advanced Legal Research

- To evaluate the international legal framework and compare India's approach with that of the United States, the United Kingdom, the European Union, and Australia in combating dark web drug trafficking.
- To suggest legal, policy, and technological reforms for strengthening India's response to illegal drug trade through the dark web while ensuring the protection of fundamental rights and the rule of law.

CONCEPT OF DARK WEB AND DRUG TRAFFICKING:

The internet has become an essential part of modern life, helping people communicate, learn, conduct business, and access information. The internet is generally divided into three layers: the surface web, the deep web, and the dark web. The surface web includes websites that can be easily accessed through search engines such as Google, Bing, and Yahoo. These websites include news portals, educational websites, social media platforms, and online shopping sites. The deep web consists of content that is not indexed by search engines. It includes online banking services, medical records, government databases, academic journals, and password-protected websites. The dark web is a hidden part of the deep web that requires special software, such as The Onion Router (Tor), to access it. Tor protects users' identities by routing internet traffic through several encrypted servers, making it difficult to identify the location or identity of users. The dark web was originally created to support secure communication, protect privacy, and allow journalists, researchers, whistle-blowers, and human rights activists to communicate safely. In countries where freedom of expression is restricted, the dark web also provides a secure platform for sharing information without fear of surveillance. Therefore, the dark web itself is not illegal; its legality depends on how it is used.

Over time, however, criminals have started using the dark web for illegal activities because of the anonymity it provides. One of the most common illegal activities is the trafficking of narcotic drugs. Dark web marketplaces operate similarly to legal e-commerce websites. Sellers create online stores, display products, provide prices, and receive customer reviews and ratings. Buyers can browse different products, compare prices, and communicate with sellers through encrypted messaging systems. These features create trust between buyers and sellers while keeping their identities hidden.Payments on dark web marketplaces are usually

© 2023 International Journal of Advanced Legal Research

made through cryptocurrencies such as Bitcoin and Monero. Unlike traditional banking systems, cryptocurrencies allow users to transfer money without directly revealing their personal identities. Although blockchain technology records cryptocurrency transactions, identifying the individuals involved often requires advanced cyber-forensic investigation. After payment is completed, illegal drugs are usually delivered through postal or courier services using false names, fake addresses, or concealed packaging to avoid detection. This method has made drug trafficking faster, more organised, and capable of reaching buyers across different countries.

The growth of internet access, encrypted communication, digital payment systems, and anonymous technologies has significantly increased the scale of illegal drug trade through the dark web. Law enforcement agencies face challenges in tracing cryptocurrency payments, identifying anonymous users, collecting electronic evidence, and exercising jurisdiction over international cybercrimes. The increasing use of the dark web for illegal drug trafficking has created serious concerns for governments, law enforcement agencies, and society. It threatens public health by making harmful drugs more easily available, especially to young people, and strengthens organised criminal networks.

LEGAL FRAMEWORK GOVERNING DRUG TRAFFICKING IN INDIA:

India has a strong legal framework to prevent and punish drug trafficking, including offences committed through the dark web and other digital platforms. The Constitution of India provides the basic legal principles for protecting both public safety and individual rights. Article 14 guarantees equality before the law and equal protection of laws, ensuring that every person is treated fairly during investigation and trial. Article 19(1)(a) guarantees freedom of speech and expression, but Article 19(2) allows the Government to impose reasonable restrictions in the interest of public order, morality, and national security. This enables the Government to take action against illegal online activities, including dark web drug trafficking.

Article 21 guarantees the right to life and personal liberty.[2] In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court held that the right to privacy is a fundamental

[2]Constitution of India, arts. 14, 19(1)(a), 19(2) & 21.

© 2023 International Journal of Advanced Legal Research

right. Therefore, while investigating cyber-enabled drug offences, authorities must balance effective enforcement with the protection of privacy and due process.[3]

The main law governing drug-related offences in India is the Narcotic Drugs and Psychotropic Substances Act (NDPS), 1985. Section 8 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 21 and 22 provide punishment for offences involving manufactured drugs and psychotropic substances, Section 23 deals with illegal import into and export from India, and Section 27A punishes financing illegal drug trafficking and harbouring offenders. Although the Act was enacted before the growth of the dark web, its provisions also apply to online drug trafficking.[4]

The Information Technology Act, 2000 supports the investigation of cyber-enabled crimes. Section 69authorises the Government to intercept, monitor, or decrypt electronic information in specific situations such as national security and crime prevention. Section 79 provides conditional protection to intermediaries while requiring them to exercise due diligence and cooperate with law enforcement authorities.[5]

The Bharatiya Nyaya Sanhita, 2023 (BNS) contains provisions relating to organised crime, criminal conspiracy, cheating, forgery, and other offences that may be committed together with dark web drug trafficking.[6] The BharatiyaNagarik Suraksha Sanhita, 2023 (BNSS) lays down the procedure for investigation, arrest, search, seizure, and prosecution of criminal offences, including those involving digital evidence.[7] The BharatiyaSakshyaAdhiniyam, 2023 (BSA)recognises electronic and digital records as admissible evidence before courts, making digital evidence collected from computers, mobile phones, servers, and blockchain records legally important.[8]

[3]**Justice K.S. Puttaswamy v. Union of India**, (2017) 10 SCC 1.
[4]**Narcotic Drugs and Psychotropic Substances Act, 1985**, Sec. 8, 21, 22, 23 and 27A.
[5]**Information Technology Act, 2000**, Sec. 69 and 79.
[6]Bharatiya Nyaya Sanhita, 2023
[7]BharatiyaNagarik Suraksha Sanhita, 2023
[8]BharatiyaSakshyaAdhiniyam, 2023

© 2023 International Journal of Advanced Legal Research

The Digital Personal Data Protection Act, 2023 (DPDP Act) regulates the processing of personal data and ensures that personal information collected during investigations is handled lawfully while protecting individual privacy.[9]

The Narcotics Control Bureau (NCB) is the central agency responsible for enforcing the NDPS Act, investigating organised drug trafficking, and coordinating with international agencies. State Police and Cyber Crime Cells assist by identifying online drug networks, tracing cryptocurrency transactions, collecting digital evidence, and conducting cyber-forensic investigations. The Supreme Court in Anvar P.V. v. P.K. Basheer[10] and Arjun PanditraoKhotkar v. Kailash KushanraoGorantyal clarified the legal requirements for the admissibility of electronic evidence, which are highly relevant in dark web investigations.[11] Together, these constitutional provisions, statutes, and enforcement agencies provide the legal framework for combating illegal drug trafficking through digital technologies.

INTERNATIONAL LEGAL FRAMEWORK AND COMPARATIVE ANALYSIS:

The illegal drug trade through the dark web is a global problem that cannot be controlled by one country alone. Drug traffickers use encrypted networks, cryptocurrencies, and online marketplaces to sell illegal drugs across national borders. Therefore, international cooperation and common legal standards are essential to investigate and prosecute these crimes effectively.

The **United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988** is the main international treaty dealing with drug trafficking. It requires member countries to criminalise the production, manufacture, possession, sale, transport, import, export, and financing of illegal drugs. The Convention also encourages countries to cooperate in extradition, mutual legal assistance, confiscation of criminal property, and information sharing to combat international drug trafficking.[12]

[9]Digital Personal Data Protection Act, 2023
[10]**Anvar P.V. v. P.K. Basheer**, (2014) 10 SCC 473.
[11]**Arjun PanditraoKhotkar v. Kailash KushanraoGorantyal**, (2020) 7 SCC 1.
[12]**United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances**, 1988, arts. 3, 5,6 and 7.

© 2023 International Journal of Advanced Legal Research

Similarly, the **United Nations Convention against Transnational Organized Crime (UNTOC), 2000**provides a legal framework for tackling organised criminal groups that operate across national borders. It promotes international cooperation, joint investigations, extradition, and protection of witnesses involved in organised crime cases.[13]

The **Budapest Convention on Cybercrime, 2001** is the first international treaty dealing specifically with cybercrime. It provides rules for investigating electronic evidence, preserving digital data, and improving international cooperation in cybercrime investigations.[14] Although India is not a party to this Convention, many countries follow its standards when investigating offences committed through the dark web. Another important international body is the **Financial Action Task Force (FATF)**, which issues global standards to prevent money laundering, terrorist financing, and the misuse of virtual assets. FATF recommends that countries regulate cryptocurrency service providers, maintain customer identification records, and strengthen financial monitoring to prevent illegal transactions.[15]

India has enacted the **Narcotic Drugs and Psychotropic Substances Act, 1985**, the**Information Technology Act, 2000**, and other criminal laws to address drug trafficking and cybercrime. However, India has not yet adopted a separate law specifically dealing with dark web offences. In contrast, the **United States** has successfully dismantled several dark web drug marketplaces through coordinated investigations by the **Federal Bureau of Investigation (FBI)** and the **Drug Enforcement Administration (DEA)** using advanced cyber-forensic techniques. The **United Kingdom** addresses online drug trafficking through the **Misuse of Drugs Act, 1971** and the **Computer Misuse Act, 1990**, supported by the **National Crime Agency (NCA)**. The **European Union** strengthens cross-border cooperation through **Europol**and **Eurojust**, while the **European Union Agency for Criminal Justice Cooperation** facilitates joint investigations among member states.

[13]**United Nations Convention against Transnational Organized Crime (UNTOC)**, 2000, arts. 5, 16 & 18.
[14]**Convention on Cybercrime (Budapest Convention)**, 2001, arts. 16, 19, 23 and 25.
[15]Financial Action Task Force (FATF)

© 2023 International Journal of Advanced Legal Research

A comparison of these jurisdictions shows that countries with specialised cybercrime laws, stronger digital forensic infrastructure, cryptocurrency regulation, and active international cooperation are more effective in combating dark web drug trafficking. India has made significant progress in strengthening its legal framework, but further reforms, improved cyber investigation capabilities, and closer international cooperation are necessary to address the growing challenges posed by illegal drug trade through the dark web.

ETHICAL AND HUMAN RIGHTS PERSPECTIVE:

The fight against illegal drug trafficking through the dark web raises several ethical issues because governments must protect society from crime while also respecting the fundamental rights of individuals. One of the most important ethical concerns is the balance between **privacy and national security**. The dark web provides anonymity through encryption and hidden networks, making it difficult for law enforcement agencies to detect drug traffickers. To investigate these crimes, authorities may use digital surveillance, interception of communications, monitoring of cryptocurrency transactions, and cyber-forensic tools. Although these methods help prevent organised crime, excessive or unlawful surveillance may interfere with the privacy of innocent individuals and may result in misuse of personal information.

In India, the **Constitution of India** protects individual rights while permitting reasonable restrictions in the interest of public safety. **Article 21**guarantees the right to life and personal liberty, which includes the **right to privacy**, as recognised by the Supreme Court in **Justice K.S. Puttaswamy v. Union of India**. The Court held that any interference with privacy must be based on law, serve a legitimate public purpose, and be necessary and proportionate. Similarly, **Article 19(1)(a)** guarantees freedom of speech and expression, while **Article 19(2)** allows reasonable restrictions for public order, national security, and the prevention of crime. Therefore, surveillance measures must always be carried out within constitutional limits.

Human rights concerns also arise during cyber investigations. Investigating agencies must respect the principles of fairness, due process, and non-discrimination while collecting electronic evidence. Arbitrary monitoring, unlawful interception of communications, or unnecessary collection of personal data may violate fundamental rights and reduce public

© 2023 International Journal of Advanced Legal Research

confidence in the justice system. The Information Technology Act, 2000, particularly **Section 69**, authorises interception or monitoring of electronic information only under specific legal conditions and procedural safeguards. In addition, the Digital Personal Data Protection Act, 2023 establishes a framework for the lawful processing of personal data while recognising certain exemptions for law enforcement and national security.

The ethical use of surveillance technology requires transparency, accountability, and judicial oversight. Technologies such as artificial intelligence, facial recognition, blockchain analysis, and digital forensic tools should be used only for legitimate investigations and not for mass surveillance or unnecessary intrusion into private lives. A balanced approach is essential to ensure that law enforcement agencies can effectively combat dark web drug trafficking without undermining constitutional values, human rights, or the rule of law. Protecting both national security and individual freedoms is necessary for maintaining public trust in the criminal justice system.

CYBER INVESTIGATION AND DIGITAL FORENSICS IN ILLEGAL DRUG TRAFFICKING:

Cyber investigation and digital forensics are essential tools for detecting and prosecuting illegal drug trafficking through the dark web. Since offenders use encrypted communication, anonymous networks, and cryptocurrencies, traditional investigation methods are often insufficient. A cyber investigation usually begins when law enforcement agencies receive intelligence, a public complaint, or information from international agencies. Investigators identify the suspected offence, secure electronic devices, preserve digital records, and analyse the available evidence. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) provides the legal procedure for investigation, search, seizure, and arrest, ensuring that electronic evidence is collected in accordance with the law.

Digital evidence includes emails, chat messages, social media communications, browsing history, computer files, CCTV recordings, mobile phone data, cloud storage records, GPS data, cryptocurrency wallet information, and blockchain transaction records. Because digital evidence can be easily altered or deleted, investigators must collect and preserve it carefully. The Bharatiya Sakshya Adhiniyam, 2023 (BSA**)** gives legal recognition to electronic and

© 2023 International Journal of Advanced Legal Research

digital records and lays down the rules for their admissibility before courts. It ensures that electronic evidence, if properly collected and authenticated, can be relied upon during criminal trials. The Supreme Court in Anvar P.V. v. P.K. Basheer **and** Arjun PanditraoKhotkar v. Kailash KushanraoGorantyal clarified that electronic records must comply with the statutory requirements before they can be admitted as evidence.

An important principle in digital forensics is the chain of custody, which means maintaining a complete record of how electronic evidence is collected, handled, stored, examined, and presented before the court. Every person who handles the evidence must be identified so that its authenticity and integrity are not questioned during trial. This process reduces the risk of tampering and strengthens the credibility of digital evidence.

Another important aspect of cyber investigation is blockchain analysis. Criminals often use cryptocurrencies such as Bitcoin and Monero to hide financial transactions related to drug trafficking. Blockchain analysis helps investigators trace cryptocurrency transfers, identify suspicious wallet addresses, and connect digital transactions with criminal activities. In addition, mobile forensics helps recover deleted messages, photographs, call records, application data, and location information from smartphones, while cloud forensics focuses on collecting evidence stored on remote servers, including emails, cloud backups, and online documents.

The Information Technology Act, 2000 supports cyber investigations by providing legal recognition to electronic records and empowering authorities to investigate cyber offences. Together with the Bharatiya Sakshya Adhiniyam, 2023 and the Bharatiya Nagarik Suraksha Sanhita, 2023, it forms the legal basis for investigating and prosecuting cyber-enabled drug trafficking. Therefore, effective cyber investigation and digital forensics are essential for identifying offenders, preserving reliable evidence, and ensuring successful prosecution while protecting the fairness and integrity of the criminal justice system.

RECOMMENDATIONS:

This research study recommends that India should strengthen its legal and enforcement system to effectively combat the illegal drug trade through the dark web. The existing laws, including the Narcotic Drugs and Psychotropic Substances Act, 1985 and the Information

© 2023 International Journal of Advanced Legal Research

Technology Act, 2000**,** should be reviewed and updated to specifically address cyber-enabled drug trafficking, anonymous online marketplaces, and cryptocurrency-based transactions. The Government should establish more advanced cyber forensic laboratories and provide modern investigation tools to the Narcotics Control Bureau (NCB)**,** State Police, and Cyber Crime Cells. Regular training should be given to investigators, prosecutors, and judges on digital evidence, blockchain technology, cryptocurrency investigations, and dark web operations. Strong monitoring of cryptocurrency exchanges through effective **Know Your Customer (KYC)** and **Anti-Money Laundering (AML)** measures is necessary to identify suspicious financial transactions and prevent money laundering. India should also strengthen international cooperation with organisations such as **INTERPOL**,**UNODC**, and **FATF**, as well as with foreign governments, to improve intelligence sharing, joint investigations, and extradition of offenders. Public awareness programmes should be conducted in schools, colleges, and communities to educate people about the dangers of illegal online drug markets and the legal consequences of using the dark web for criminal activities. At the same time, all cyber investigations must respect constitutional principles, including the right to privacy, due process, and fair trial, so that law enforcement actions remain lawful and accountable. Finally, continuous research, policy development, and the use of emerging technologies such as artificial intelligence and blockchain analytics should be encouraged to strengthen India's capacity to detect, investigate, and prevent dark web drug trafficking. These measures will help create a stronger legal framework, improve enforcement efficiency, and protect public health, national security, and the rule of law in the digital age.

CONCLUSION:

This research concludes that the illegal drug trade through the dark web has become a major challenge for India's legal system and law enforcement agencies. The use of anonymous networks, encrypted communication, and cryptocurrencies has made drug trafficking more organised, difficult to detect, and capable of operating across national borders. Although India has important laws such as the **Narcotic Drugs and Psychotropic Substances Act, 1985**, the **Information Technology Act, 2000**, the **Bharatiya Nyaya Sanhita, 2023**, the **BharatiyaNagarik Suraksha Sanhita, 2023**, the **BharatiyaSakshyaAdhiniyam, 2023**, and the **Digital Personal Data Protection Act, 2023**, these laws face practical challenges when dealing with modern cyber-enabled drug crimes.

© 2023 International Journal of Advanced Legal Research

The study also finds that law enforcement agencies face difficulties in identifying offenders, tracing cryptocurrency transactions, collecting electronic evidence, and investigating offences that involve multiple countries. International cooperation, advanced cyber-forensic techniques, and effective intelligence sharing are therefore essential for tackling dark web drug trafficking. At the same time, cyber investigations must respect constitutional rights, including the right to privacy, due process, and fair trial.

The research concludes that legal reforms, stronger cyber investigation capabilities, specialised training for enforcement agencies, better regulation of cryptocurrency transactions, and greater international cooperation are necessary to address this growing threat. A balanced approach that combines effective law enforcement with the protection of human rights will help strengthen India's response to illegal drug trafficking through the dark web and contribute to a safer, more secure, and accountable digital environment.

REFERENCE:

BOOKS:

- David Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, 2007).
- Majid Yar& Kevin F. Steinmetz, *Cybercrime and Society* (3rd ed., Sage Publications, 2019).
- Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2015).
- Yvonne Jewkes& Majid Yar (eds.), *Handbook of Internet Crime* (Willan Publishing, 2010).
- Neal Kumar Katyal et al., *Cybercrime: Criminal Threats from Cyberspace* (Aspen Publishers, 2005).
- Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues and Outcomes* (Northeastern University Press, 2012).

JOURNALS:

- Brenner, Susan W., "Cybercrime Investigation and Prosecution: The Role of Digital Evidence," *John Marshall Journal of Information Technology & Privacy Law.*

© 2023 International Journal of Advanced Legal Research

- Martin, James, "Lost on the Silk Road: Online Drug Distribution and the Cryptomarket," *Criminology & Criminal Justice*.
- Aldridge, Judith &Décary-Hétu, David, "Cryptomarkets and the Future of Illicit Drug Markets," *International Journal of Drug Policy*.
- Lusthaus, Jonathan, "How Organised Crime Uses the Internet," *Trends in Organized Crime*.
- Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (latest edition).

INTERNATIONAL CONVENTIONS AND INSTRUMENTS:

- Convention on Cybercrime (Budapest Convention), 2001.
- Financial Action Task Force (FATF), *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (FATF Recommendations)*, updated 2023.
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.
- United Nations Convention against Transnational Organized Crime (UNTOC), 2000.
- Universal Declaration of Human Rights, 1948.
- International Covenant on Civil and Political Rights (ICCPR), 1966.

© 2023 International Journal of Advanced Legal Research