INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DARK WED MARKETPLACES: INVESTIGATION CHALLENGES

AUTHORED BY - HANUMANT WAGHAMODE & ANIKET SHINDE

ABSTRACT:

The rapid growth of illegal Dark Web marketplaces is one of the most complex aspects of modern cybercrime. It presents challenges for traditional criminal justice systems. Hidden services operate through encrypted overlay networks, especially The Onion Router (Tor). These networks create anonymous, decentralized commercial platforms. On these sites, illegal goods such as drugs, firearms, zero-day exploits, and stolen personally identifiable information (PII) are frequently traded using privacy-focused cryptocurrencies and multi-signature escrow setups. This paper looks closely at the technological, procedural, and legal challenges law enforcement faces in investigating Dark Web businesses.

From a technological view, onion routing, PGP encryption, and cryptocurrency mixing services significantly weaken traditional surveillance techniques, traffic analysis, and identity attribution methods. On the procedural side, gathering and preserving digital evidence is difficult due to unstable memory environments, cloud storage spread across different locations, and strict rules for maintaining an unbroken chain of custody. Legal inquiries into the Dark Web expose significant legal loopholes in India's existing legislation. Although they offer a legal foundation for addressing cybercrimes and the admissibility of electronic evidence, the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita (BNS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023 were not designed with decentralized criminal networks operating across multiple jurisdictions in mind. The legal system of India is examined against global investigative techniques by studying case laws, statutes, and some prominent global enforcement actions such as Silk Road, Alpha Bay, and Hydra. Legislative modifications, the legalization of covert cyber operations in the name of law, increased technical means available to law enforcement authorities, and amendment to MLATs in response to the growing problem of anonymous business transactions on the Darknet are recommended.

Keywords: Dark web Marketplaces, Cybercrime Investigation, Decentralized criminal Network, Tor network, Digital Evidence, Cryptocurrencies

ISSN: 2582-6433

INTODUCTION

Public administration, communication, and commerce have all been impacted by the swift expansion of the world's digital infrastructure. Additionally, it has created new avenues for cybercrime. One of the most complicated issues in criminal law and technology is the emergence of illegal Dark Web Marketplaces.[1]

It is essential to differentiate between the phrases surface web, deep web, and dark web in order to comprehend the legal difficulties surrounding the dark entities. The portion of the internet that may be reached using search engines is known as the surface web. The databases, cloud storage, and private networks that are not accessible thru search engines—which make up around 90% of the internet are referred to as the "deep web." The dark web is a subset of the deep web that is mostly used to hide identities and data and requires specialized software, networks, and authorization to access. The primary difference between the deep web and the dark web is that the deep web is not indexed and may not have any intention to stay hidden while the dark web uses onion-routing systems to keep its location private and secure data traffic.[2] Dark web forums and marketplaces have been used by organized cybercrime groups to market and deliver their services.

The evolution of darknet markets and services has progressed from primitive bulletin board systems to enterprise-grade services such as Silk Road, AlphaBay, Hansa, Hydra, and numerous other platforms. In other words, the current marketplaces offer a variety of customer experiences and services comparable to any conventional online trade. Modern dark web marketplaces have sophisticated user interfaces, rating systems, Automated Vendor Systems (AVS), multisignature escrow systems, and encrypted messaging services for buyers and sellers to communicate and resolve disputes. As a result, traditional law enforcement investigative methods are inappropriate and ineffective in countering dark web-related crimes, including but not limited to trafficking, financial fraud, terrorist financing, and distribution of illicit goods and services.

This paper will provide an in-depth analysis of the investigative, technical, and legal aspects of Dark Web marketplaces. The paper will further discuss the procedural issues related to evidence collection and de-anonymization techniques and review Indian laws concerning the regulation and legal framework for dark web activities. Specifically, this paper will address the

[1] W. Gordon Correy, Cybercrime and the Dark Web: Digital Evidence in Underground Economies 45–48 (2d ed. 2021)

[2] Roger Dingledine, Nick Mathewson & Paul Syverson, Tor: The Second-Generation Onion Router, Proc. 13th USENIX Security Symp. 303, 305–308 (2004)

ISSN: 2582-6433

Information Technology Act, 2000, Bharatiya Nyaya Sanhita (BNS) Act, 2023, Bharatiya Sakshya Adhiniyam (BSA) Act, 2023, and relevant penal laws[3] alongside cyber laws and their limitations, if any, in handling evidence and processing cases related to the dark web. Finally, this paper will discuss the judicial system's response to electronic evidence, international collaboration, and suggested reforms to protect citizens' civil liberties and privacy, especially the balancing act between freedom and security.

I. ARCHITECTURE AND OPERATIONAL DYNAMICS OF DARK WEB MARKETPLACES

i. Technical Infrastructure and Onion Routing Protocol

The Dark Web is built of onion routing networks that provide anonymity to their users. The network is based on The Onion Router (Tor), I2P, and Freenet technologies, among which Tor is the most popular platform for darknet marketplaces.[4] Tor is the product of the US Naval Research Laboratory that takes care of anonymity by masking the user's IP address with the help of a distributed number of volunteer servers.

When a user requests to access any onion address, his device establishes an encrypted connection through Tor relays called guards, middlemen, and rendezvous nodes. Those nodes decrypt the traffic step by step and reveal one layer of encryption. As a result, every relay in the network only knows the IP address of the next node but not the client's original IP and the destination server's IP address.[5] Hidden services are hosted on onion relays and have rendezvous points and descriptors stored in the distributed hash table to hide the IP address under the onion link. Consequently, the police cannot track any dark web activity by simply typing in an onion link or searching for an IP address.

ii. Cryptocurrencies, Anonymity Tools, And Pseudonymous Escrow Systems

The dark web has protocols that enable payments to bypass traditional banking systems and regulatory oversight such as Anti-Money Laundering (AML) and Know Your Customer

[3] Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India); Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023 (India).
[4] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023, Europol Publications Office 14–22 (2023)
[5] Roger Dingledine, Nick Mathewson & Paul Syverson, Tor: The Second-Generation Onion Router, Proc. 13th USENIX Security Symp. 310. (2004)

ISSN: 2582-6433

(KYC). Initially the Bitcoin was the preferred medium of exchange in darknet markets.[6] At the time, Bitcoin transactions were pseudonymous and not fully anonymous because they were recorded on a transparent block chain. Using big data forensic accounting tools and heuristic analysis, law enforcement could follow transactions from the Tor marketplace wallets to fiat cashouts in regulated exchanges.

The dark web users circumvented block chain surveillance by using privacy-centric crypto currencies such as Monero and Zcash. The Monero cryptocurrency, for instance, utilizes ring signatures, stealth addresses, and Ring Confidential Transactions (RingCT) to hide the source, destination, and value of transactions, making it difficult to track illicit activities on the block chain.[7] Darknet marketplace participants also use crypto tumblers and mixers to maximize confidentiality by severing the connection between the sender's and recipient's addresses. Most platforms use multisig escrow wallets to hold customer payments in trust until the items are delivered. Escrow accounts have at least two private keys, usually 2-of-3 multisig, meaning that two wallets must approve any transaction for it to go through. The marketplace administrators, law enforcers, or hackers cannot access the shipment details because the PGP encrypted message can only be decrypted by the buyer using the seller's public key.

iii. Business Models and Modus Operandi of Underground Vendors

Modern darknet marketplaces are typically based on the software as a service (SaaS) or commission-based business model. The platform's owners operate the infrastructure and ensure the security of transactions on the websites while collecting fees for their services (usually 2–5%). Sellers, in turn, handle specific categories of goods and organize their presentation in an accessible manner, often with the possibility of searching through forums and leaving reviews about the marketplace's vendors.

Counterfeit goods are usually delivered through regular mail or courier services under alternative return addresses to avoid suspicion. In addition, couriers use abandoned buildings or private boxes as drop sites so that sellers and buyers are not seen in the same location at the same time. Such precautions help both parties avoid immediate discovery and identity reveal if the delivery is inspected.[8]

[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Decentralized Business Review 2126 (2008).
[7] Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, Proc. 2013 ACM SIGCOMM Conf. Internet Measurement Comm. 127, 129–132 (2013).
[8] UNODC, Comprehensive Study on Cybercrime, United Nations Office on Drugs and Crime Report 112–118 (2020).

ISSN: 2582-6433

II. INVESTIGATIVE AND PROCEDURAL CHALLENGES IN ANONYMOUS NETWORKS

i. Attribution and De-Anonymization Hurdles

The principal challenge in investigating darknet crimes is the transition from a digital entity, be it a human actor or server, behind a pseudonym or onion domain to a natural person or server IP address. Traditional methods such as IP log subpoenas to the user's ISP are ineffective due to the nature of the Tor network's design which makes it possible for ISPs to only see that their client is a Tor entry guard and not the destination server they intended to visit.

The authorities have to rely on advanced de-anonymization methodologies. Network Traffic Analysis and Timing Attacks allow investigators to associate an anonymous client with hidden server destinations, based on the timing and size of packets sent through guards and exits.[9] In reality, most successful operations relied on human error reports, such as the use of real email addresses for administrator accounts, code reuse across different dark web forums, or non-cryptocurrency transactions on KYC-friendly platforms. Moreover, law enforcement agencies can utilize Network Investigative Techniques – zero-day exploits that target the browser software, forcing it to reveal the machine's public IP, MAC address, and hostname.[10]

ii. Volatile Digital Evidence and Chain of Custody

Digital evidence stored on servers located on darknet is at significant risk of being wiped since the system is designed to eliminate all traces of data on it. Modern darknet servers are designed in such a way that they are protected from seizure by investigators. In most cases, the servers are run from RAM (random-access memory) using tools such as Tails OS or modified Linux systems.[11] Once the server is powered off, or, for example, a physical raid triggers a kill-switch, all evidence that was in the RAM will be lost forever.

Investigators would have to make a memory dump to save the evidence. Such a memory image will have to be made while the server is running. It is a rather involved process that requires special training and can only be done on-site. Another challenge investigators face when collecting digital evidence is ensuring that the chain of custody is maintained. It implies that the evidence's integrity should be ensured from collection to presentation in court. In practice,

[9] Central Bureau of Investigation, Standard Operating Procedures for Digital Evidence Collection and Handling 88–94 (3d ed. 2022).
[10] W. Gordon Correy, Cybercrime and the Dark Web: Digital Evidence in Underground Economies 89 (2d ed. 2021).
[11] CBI SOP, supra note 9, at 102.

ISSN: 2582-6433

it means that hash values of binary files with evidence, forensic images of hard drives, and database extracts should be consistent during all stages. For example, it can be technically challenging to ensure that hash values are consistent during cross-border investigations during the judicial process.[12]

iii. **Encryption and Cryptographic Barriers**

Even when physical possession of a device is gained, investigators often run into the problem that the data on them is protected by some form of Full-Disk Encryption (FDE) using AES-256 encryption such as with VeraCrypt, LUKS, or BitLocker. This poses a problem in terms of legal implications of being forced to give up a passphrase.

In cases where an accused has to give up a complicated cryptographic password or has to be forced to decrypt a hard disk, the practice may be considered to violate article 20(3) of the Indian Constitution that protects against self-incrimination.[13] Section 69 of the IT Act, 2000 empowers the state to require a person who is in charge of a computer resource to provide information and assistance. However, such directions from the state must be carefully weighed against the constitutional rights to privacy and protection against self-incrimination as provided by the Indian Constitution.

IV. INDIAN LEGAL AND REGULATORY FRAMEWORK GOVERNING DARK WEB CRIMES

i. Provisions under the Information Technology Act, 2000 and IT Amendment Act, 2008

The Information Technology Act, 2000 (IT Act) is the main law in India that addresses cyber-crimes. However, it was primarily created to address conventional computer crimes, which means that its interpretation requires some degree of judicial extrapolation when it comes to darknet-related activity. Unauthorized access, extraction of information, causing damage or obstruction to computer systems, and hacking fall under the jurisdiction of Section 43 and Section 66. Specifically, the illegal deployment of malware or Remote Access Trojan (RAT) for exfiltrating data from a target server is considered a crime under these sections, which typically cover any damage or unauthorized use of a computer system. According to

[12] Id. at 115.
[13] INDIA CONST. art. 20, cl. 3.

ISSN: 2582-6433

Section 66B, dishonest or fraudulent appropriation of any computer-related resources or communication devices also constitutes cybercrime, including the purchase of any of the aforementioned illicit assets from the dark web marketplace. This section also covers dishonest or fraudulent receipt or retention of stolen computer resources, communication devices, databases, finances records, and Personal Identifying Information (PII).[14]

Identity theft and cheating by impersonation using computer resources are covered under Section 66C and 66D, which apply to vendors dealing in stolen credentials, credit card details, and fake official documents. Section 66F covers the unlawful act of cyber-terrorism, which is defined as the use or threat to use computer power to sabotage or penetrate computer systems with the intent to damage or destroy India's unity, integrity, sovereignty, or security, or that of its citizens or any foreign state. This section applies to any number of cyber-espionage activities conducted by terrorist entities utilizing the dark web to fundraise, transfer funds, and acquire weapons.[15] Lastly, Section 69 and Section 69B empowers the government to conduct surveillance or intercept encrypted data from any computer resource for the purposes of investigations or national security, and requires any computer intermediary service to provide decryption assistance upon demand.

ii. Interplay with Bharatiya Nyaya Sanhita (BNS), 2023

Following the enforcement of The Bharatiya Nyaya Sanhita, 2023 (BNS) replacing the Indian Penal Code, 1860, several relevant sections have been inserted in the BNS which hold implications for the offenses committed via the dark web. For instance, Section 111 of the BNS prescribes punishment for organized crime syndicates that perpetrate cyber-crimes, trafficking of banned items, weapons, and narcotic goods using force, coercion, or cyber-espionage for monetary or material gains.[16] Hence, the owners of the dark web marketplace, networks of international vendors, and money laundering syndicates can be charged under section 111 of the BNS for their roles in organized crimes.

Besides, sections 336 and 340 of the BNS prohibit the production of forged computer-generated records and electronic signatures. Therefore, dark web vendors dealing in counterfeit licenses, passports, and degrees will be charged under sections 336 and 340 of the BNS. Additionally, various sections of the Indian Penal Code, 1860, including section 61 (criminal conspiracy), alongside the Information Technology Act, 2000, are used to prosecute buyers, administrators,

[14] Information Technology Act, 2000, Sec. 43, 66, 66B, 66C, 66D, No. 21, Acts of Parliament, 2000 (India).
[15] Information Technology Act, 2000, Sec. 66F, No. 21, Acts of Parliament, 2000 (India).
[16] Bharatiya Nyaya Sanhita, 2023, Sec 111, No. 45, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

escrow agents, and couriers involved in the execution and facilitation of organized cyber-crimes in the dark web.

iii. Specialized legislation: NDPS Act, 1985 and PMLA, 2002

As narcotics constitute a significant portion of darknet transactions, the relevant special laws play an important role in prosecuting darknet crimes. The Narcotic Drugs and Psychotropic Substances (NDPS) Act, 1985 regulates traffic of drugs through the postal channels or "crypto-postage" and prescribes penalties for their illegal sale, purchase, or transportation. To prosecute violations of the crypto-postage rules, Sections 8, 20, 21, 22, and 23 of the NDPS Act, 1985 can be invoked which criminalize importing, exporting, selling, purchasing, and transporting narcotic substances.[17] However, in cases when crypto-drugs are delivered anonymously to the buyer's address, proving possession of narcotic substances can be difficult since such delivery can be performed by anyone else in case of using a false address.

According to Section 3 of the Prevention of Money Laundering Act (PMLA), 2002, laundering of illicit cryptocurrency profits is illegal. Under PMLA, the Directorate of Enforcement (ED) can seize cryptocurrency, crypto-wallets, and other proceeds of crime, including property, rights, and assets obtained through darknet crimes.[18]

V. JUDICIAL APPROACHES AND STATUTORY LIMITATIONS IN DIGITAL EVIDENCE

i. Admissibility and Certification of Electronic Evidence

The evidentiary value of the digital traces retrieved from dark web investigations depends significantly on their compliance with the statutory requirements for admissibility. In India, electronic evidence was governed by Section 65B of the Indian Evidence Act, 1872, which has now been repealed by Section 63 of the Bharatiya Sakshya Adhiniyam (BSA), 2023.[19]

Section 63 of the BSA stipulates procedures for the production of printouts, forensic mirror images, server logs, RAM captures, extracted chat records, etc., in courts as secondary evidence. The interpretation of "secondary evidence" has been clarified by various rulings of the Supreme Court. In State (NCT of Delhi) v. Navjot Sandhu , 2005, it was held that

[17] Narcotic Drugs and Psychotropic Substances Act, 1985, Sec 8, 20–23, No. 61, Acts of Parliament, 1985 (India).
[18] Prevention of Money Laundering Act, 2002, Sec 3, No. 15, Acts of Parliament, 2003 (India).
[19] Bharatiya Sakshya Adhiniyam, 2023, Sec 63, No. 47, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

"secondary evidence" of electronic records could be produced in court without any mandatory technical certification by an expert.[20] However, this view was reversed in P.V. Anvar v. P.K. Basheer , 2014, wherein the Supreme Court ruled that secondary evidence of electronic records was inadmissible unless a certificate was affixed by a person in responsible official charge of the computer or a record.[21] Subsequently, in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal , 2020, the Supreme Court reiterated that a certificate of responsible official charge under Section 65B was an essential requirement for admitting secondary electronic evidence in court.[22] This principle continues to govern the production of secondary evidence under Section 63 of the BSA, 2023. In dark web investigations, such certification under Section 65B or Section 63 may become difficult if the server logs and Tor exit node are located abroad or the foreign company administering the Tor node is unresponsive to a certificate request.

ii. Territorial and Extra-Territorial Jurisdiction under Section 75 of the IT Act

Dark web markets have global outreach where any particular transaction can take place between a buyer in Pune, a seller in Eastern Europe, a relay node in Germany, a database server in Iceland, and a cryptocurrency mixer in jurisdiction "X." Section 75 of the Information Technology Act, 2000 provides extra-territorial jurisdiction to Indian law enforcement agencies over any offense committed outside India by any person, regardless of nationality, if the offense was committed against a computer, computer system, or computer network located in India.[23] Similarly, Section 1 (5) of the Bharatiya Nyaya Sanhita (BNS), 2023 also has extra-territorial jurisdiction over offenses committed outside India against Indian persons, property, or interests by any person.

However, even if Section 75 of the IT Act or Section 1(5) of the BNS, 2023 applies to the dark web transaction, Indian law enforcement agencies cannot conduct raids, searches, or arrests of the foreign nationals involved without violating the principles of sovereignty and territorial integrity of other nations. 23

iii. Search, Seizure and Interception Norms

Dark web investigation often involves the seizure of computer hardware and forensic

[20] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 S.C.C. 600 (India).
[21] P.V. Anvar v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).
[22] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).
[23] Information Technology Act, 2000, Sec 75, No. 21, Acts of Parliament, 2000 (India).

ISSN: 2582-6433

decryption of digital devices. Such acts require adherence to the constitutional and statutory standards for searches and seizures. Under Section 69 of the Information Technology Act, 2000 and the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, any interception, monitoring, or decryption of communications by the government must be approved by the Union Home Secretary or the State Home Secretary.[24]

Moreover, any unreasonable surveillance, digital searches, and seizures of digital evidence would violate the judgment of the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India 2017 and the Constitution of India, 1950, particularly Article 21. The Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017 held that for state surveillance and interception of digital communication and data, there must be legality, a legitimate state objective, and proportionality; mass surveillance, indiscriminate search and seizure of computer data, and decryption of personal digital devices without a warrant would violate the fundamental right to privacy.[25]

VI. GLOBAL STRATEGIES, CROSS-BORDER COOPERATION, AND PROPOSED REFORMS

i. International Law Enforcement Operations and Case Studies

Darknet investigations benefit considerably from global law enforcement cooperation mechanisms. During Operation Anonymous and Silk Road takedown in 2013, the FBI and its international partners were able to seize the servers hosting Silk Road in Iceland by exploiting operational security mistakes by the marketplace administrator Ross_Ulbricht, the physical seizure of his live unencrypted laptop in a public library, and undercover operations that successfully infiltrated the ranks of the marketplace's administrators and moderators.[26]

Operation Bayonet (2017) conducted by the FBI, the Dutch National Police, and Europol also saw the joint operation by the Dutch and US law enforcement agencies. The Hansa marketplace was secretly taken over while its users were redirected to AlphaBay which was concurrently shut down by the FBI. While Dutch investigators physically took over the servers hosting Hansa, user encryption keys were compromised allowing investigators to track down thousands

[24] Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 (India).
[25] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[26] United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).

ISSN: 2582-6433

of buyers and sellers across national jurisdictions.[27] Similar undercover operations are illustrated by Operations DisNet and J-CODE that target dark web drug trafficking, where crypto-postage letters are intercepted at the domestic receiving sorting facility.

ii. Mutual Legal Assistance Treaties (MLATs) and INTERPOL Mechanisms

Darknet investigations targeting servers located on foreign jurisdictions require international data-sharing agreements such as Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory (LRs) as operationalized under Section 105 of the Code of Criminal Procedure (CrPC) and the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023. In practice, however, an MLAT request can take between ten to eighteen months for processing. Therefore, if evidence is hosted on darknet servers, such evidence could have been deleted by the time MLAT-authorized requests are processed.[28]

The National Central Bureau (NCB–New Delhi) that serves as the primary agency for India for liaising with INTERPOL, issues Red Notices for wanted persons and Purple Notices for darknet intelligence. However, since India has not ratified the 2001 Budapest Convention on Cybercrime, Indian investigators cannot use the 24/7 contact points established by the signatories of the treaty for expeditious gathering of evidence.[29]

iii. Legislative, Technical, and Capacity-Building Reforms for India

India must embark on a capacity-building and legislative review process to ensure that domestic investigative agencies are better positioned to investigate darknet crimes. First, Parliament needs to consider a legislation that guides controlled undercover operations and controlled delivery in cybercrime investigations. Such an approach will ensure that evidence obtained from online undercover investigations is admissible in court while also negating challenges to evidence extraction on the grounds of entrapment. Second, investigation agencies such as cyber cells within State Police, CBI, NCB, ED, and NIA should create specialized darknet and blockchain forensic units that feature state-of-the-art cryptocurrency trace software and automated PGP decryption tools.[30]

[27] United States Department of Justice, Report on the Takedown of AlphaBay and Hansa Marketplaces, DOJ Press Release No. 17-798 (July 20, 2017).
[28] Bharatiya Nagarik Suraksha Sanhita, 2023, Sec 105, No. 46, Acts of Parliament, 2023 (India).
[29] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185 (Budapest Convention).
[30] UNODC, supra note 8, at 145.

ISSN: 2582-6433

Third, CFSLs and SFSLs need to develop expertise in live RAM acquisition and chip-off investigations as well as cloud investigations to reduce the time taken in forensic investigation processes. Fourth, India needs to pursue bilateral treaties with major data host countries to enable faster processing of electronic evidence preservation requests. Finally, it is recommended that Section 69 of the IT Act, 2000 be amended to allow for independent judicial oversight of investigative agencies while also developing appropriate procedures for decrypting data.

This version is slightly shorter than the original while retaining the same level of detail and complexity. It uses more formal academic language and structure compared to the first version.

VII. CONCLUSION

Dark web marketplaces represent a paradigm shift in the current state of affairs involving organized cyber-crime. By utilizing anonymizing overlay networks, crypto-monetary policies, PGP-encrypted communications, and regular mail services, dark web marketplaces have created highly sophisticated platforms for trade that border on near-total anonymity. Investigating such marketplaces presents perennial jurisdictional and evidentiary challenges to the criminal justice system, which has traditionally relied on geographical and institutional oversight and control over the financial system.[31]

The scourge of the dark web marketplace highlighted in this paper, therefore, calls for a multi-faceted and multi-layered response, one that responds to challenges in technology, procedure, and law. From a technological standpoint, Tor's onion routing, cryptocurrency mixing, and RAM-based computing have severely limited investigative options available to investigators. From a procedural standpoint, the need for preserving volatile digital evidence, and the need for chain of custody of such evidence in accordance with the relevant procedures, for instance, in Section 63 of the Bharatiya Sakshya Adhiniyam 2023, require resources.[32] Finally, while the Information Technology Act 2000 and the Bharatiya Nyaya Sanhita, 2023 represent a good conceptual framework for prosecuting cyber-crimes, jurisdictional constraints and procedural delays in the Mutual Legal Assistance Treaties between nations impede seamless responses to crimes on dark web marketplaces.

This need not require a reversal of the stated policy of privacy and protection of rights. Rather, India can review its legal responses and procedures to ensure that they are in tandem with the

[31] Europol, supra note 4, at 40.
[32] Bharatiya Sakshya Adhiniyam, 2023, Sec 63, No. 47, Acts of Parliament, 2023 (India).

ISSN: 2582-6433

requirements of the times. Statutes criminalizing undercover investigations on such marketplaces, coupled with the development of relevant skills and competencies in digital forensics, and updated procedures for preserving evidence, including leveraging on the chain of custody principles in the Evidence Act, will be necessary if India is to meet its obligations to prosecute and punish crimes committed in cyberspace.