INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

"JURISDICTIONAL ISSUES IN INVESTIGATING DARK WEB CRIMES IN INDIA: A CRITICAL ANALYSIS"

AUTHORED BY - NAVANIT KUMAR SINGH,
Research Scholar,
Pt. Motilal Nehru Law College, Maharaja Chhatrasal Bundelkhand University, Chhatarpur (M.P.)

Abstract

The rise of the dark web has created complex jurisdictional issues for law enforcement agencies worldwide. In India, these challenges are heightened by the country's expanding digital ecosystem, the transnational nature of cybercrime, and the legal gaps within domestic cyber legislation. The inherent anonymity of Tor-based networks, encrypted communication channels, offshore server locations, and cryptocurrency-driven economic models complicate the process of identifying offenders and securing admissible evidence. Although Indian law attempts to exercise extra- territorial jurisdiction under Section 75 of the Information Technology Act, 2000, practical enforcement remains hindered by slow mutual legal assistance processes, conflicting foreign privacy regulations, and limited technological capacity within investigative agencies. This article provides a critical analysis of India's jurisdictional struggles in darknet investigations, drawing upon case studies, legal frameworks, comparative international models, and institutional constraints. The paper concludes by recommending reforms intended to strengthen India's cyber- sovereignty, enhance investigative capacity, and develop a globally synchronized approach to combating darknet crime.

Keywords: Dark Web, Jurisdiction, Cybercrime, India, Tor, Cryptocurrency, IT Act, Evidence Law, International Cooperation.

Introduction

The dark web represents a concealed segment of the internet that operates through anonymity-enhancing technologies such as Tor and I2P. While these platforms serve legitimate purposes, including protection of political dissidents and whistleblowers, they also facilitate illicit markets trading in narcotics, weapons, stolen identities, ransomware-as-a-service kits, and child sexual abuse material. India's rapid digital transformation, accompanied by increased

ISSN: 2582-6433

internet penetration and data-driven governance, has simultaneously increased vulnerability to sophisticated cybercrimes emerging from the dark web.

Jurisdictional ambiguity lies at the heart of India's enforcement struggles. Traditional legal doctrines based on territoriality are fundamentally incompatible with anonymized, decentralized, cross-border darknet ecosystems. This paper critically examines the jurisdictional constraints faced by Indian law enforcement and evaluates the adequacy of domestic legal frameworks and institutional structures in addressing these new threats.

Literature Review

Academic scholarship on the dark web emphasizes its unique architecture of anonymity, encryption, and decentralization, which complicates attribution and forensic investigation (UNODC 2020). International research further highlights the challenges of cross-border cooperation, especially when crime involves servers scattered across multiple jurisdictions (Europol 2022). Indian scholarship has largely focused on cybercrime generally, discussing issues of privacy, surveillance, and data governance (Sukumar 2020), but there remains limited literature specifically addressing India's jurisdictional dilemmas related to the dark web.

Legal analyses have pointed to the limitations of the Information Technology Act, 2000—a pre- dark-web legislation—in regulating modern forms of digital criminality. Reports by CERT-In and the Ministry of Home Affairs indicate a growing incidence of darknet-linked crimes involving narcotics, identity theft, and financial fraud, yet without sufficient procedural clarity for investigating these offences beyond domestic borders.

This study fills a gap in the literature by offering a comprehensive, India-centered examination of jurisdictional constraints in darknet investigations.

Methodology

This research follows a doctrinal and analytical methodology, drawing upon statutory interpretation, case reviews, government reports, and comparative frameworks from international cyber governance. Primary sources include the Information Technology Act, 2000, the Indian Penal Code, the Digital Personal Data Protection Act, 2023, and relevant Indian case material. Secondary sources include reports from the NCRB, CERT-In, NCB, Europol, UNODC, and academic publications. This qualitative approach facilitates a detailed

ISSN: 2582-6433

analysis of how India's legal and institutional frameworks respond to emerging darknet challenges.

The Dark Web and its Legal Complexities in India

The architecture of the dark web is built to obscure location, identity, and communication routes. Tor-based onion routing passes user traffic through multiple global nodes, preventing the identification of true IP addresses and server endpoints. For Indian investigators, this creates uncertainty regarding the locus of criminal acts. When offenders operate from foreign territories and host their data on servers in yet another jurisdiction, traditional concepts of territorial jurisdiction become obsolete.

Indian law does not explicitly prohibit accessing the dark web. Instead, enforcement relies on applying various provisions of the IT Act, NDPS Act, POCSO Act, and IPC. However, these laws lack explicit clarity on darknet environments, leading to interpretive uncertainty during prosecution. The technical sophistication of darknet platforms further complicates this by rendering many traditional investigative techniques ineffective.

Jurisdictional Constraints Under Indian Cyber Law

Section 75 of the IT Act attempts to extend extra-territorial jurisdiction to cover offences committed outside India that involve a computer or network located within India. Although conceptually broad, its practical implementation suffers from structural and diplomatic hurdles. Foreign service providers may decline to share data, citing domestic privacy laws such as the EU's GDPR, which impose restrictions on cross-border data transfers. India's own Digital Personal Data Protection Act, 2023 modernizes domestic privacy regulation but does not clearly define protocols for cross-border criminal investigations, creating conflict between privacy protection and law enforcement needs. The absence of a unified global cyber legal system contributes to jurisdictional fragmentation, forcing Indian agencies to navigate complex foreign procedures to retrieve essential evidence.

Challenges in Identification, Attribution, and Evidence Collection

The fundamental obstacles in darknet investigations arise from anonymity, encryption, and decentralization. Tor conceals user identities and masks routing paths, making attribution extremely difficult. Darknet markets often operate on offshore servers that routinely delete logs or migrate to evade detection. Mutual Legal Assistance Treaties and Letters Rogatory remain

ISSN: 2582-6433

time- consuming, often resulting in loss of volatile digital evidence.

Cryptocurrency-based transactions introduce further complexity. Payment channels on the dark web rely heavily on Bitcoin, Monero, and other privacy coins. Offshore exchanges, particularly those in jurisdictions with lax regulatory standards, may refuse cooperation with Indian authorities. Even when cooperation is possible, tracing blockchain transactions remains technically demanding without advanced forensic tools.

Digital evidence collection suffers from lack of harmonized admissibility standards across jurisdictions. Foreign evidence may not satisfy requirements under the Indian Evidence Act, 1872, leading to courtroom challenges that undermine prosecution.

Institutional Gaps and Enforcement Challenges

India's cyber enforcement architecture is dispersed across multiple agencies including the CBI, NIA, NCB, ED, and state cyber cells. Coordination challenges and overlapping mandates often lead to fragmented investigations. The Indian Cyber Crime Coordination Centre (I4C), though promising, remains in early development and lacks specialized darknet-focused units comparable to Europol's EC3 or the FBI's Cyber Division.

Resource constraints further undermine investigative capacity. Many state-level cybercrime units lack access to darknet monitoring tools, advanced crypto-tracing platforms, and trained technical analysts. This skill deficit creates dependency on private cybersecurity firms or foreign agencies, which may not always be available or cooperative.

Constitutional and Legal Conflicts

The recognition of privacy as a fundamental right in Justice K.S. Puttaswamy v. Union of India (2017) imposes constitutional limitations on surveillance and interception. Darknet monitoring must comply with principles of necessity, proportionality, and legality, generating tension between privacy protections and security imperatives.

Encryption amplifies this conflict. Section 69 of the IT Act empowers authorities to demand decryption, but many darknet platforms utilize end-to-end encryption, multi-layer encryption, or privacy-enhancing cryptocurrencies that even service providers cannot decrypt. Furthermore, foreign VPN and hosting companies often refuse compliance due to conflicting

ISSN: 2582-6433

domestic laws.

Case Studies from India

Investigations into darknet-based narcotics trafficking in Bengaluru, Hyderabad, and Mumbai illustrate the jurisdictional difficulties in tracing foreign darknet markets, offshore crypto wallets, and international courier networks. The NCB has repeatedly encountered non-cooperative foreign crypto exchanges and hosting companies, slowing investigations and allowing suspects time to destroy evidence.

Large-scale data leaks affecting millions of Indian users have appeared on foreign darknet forums hosted in Eastern Europe and Russia. CERT-In advisories have had limited effect, as India lacks diplomatic and operational mechanisms to compel foreign compliance.

Cyber-terror cases involving encrypted darknet channels demonstrate India's reliance on foreign intelligence cooperation, which is inconsistent and often delayed. These case studies reveal systemic vulnerabilities in India's cross-border investigative capacity.

Comparative International Perspectives

Countries such as the United States and those in the European Union have developed specialized darknet task forces with strong international coordination. The takedown of AlphaBay and Hansa Market involved advanced infiltration, real-time intelligence sharing, and collaborative operations across multiple jurisdictions. These models demonstrate the importance of integrated cyber task forces, rapid cross-border evidence sharing, and standardized legal frameworks.

India lacks participation in the Budapest Convention, limiting its access to global cybercrime cooperation networks. While India cites sovereignty concerns, exclusion from this framework weakens its ability to engage in coordinated international action against darknet crime.

Discussion

India's jurisdictional limitations result from a combination of outdated legal frameworks, inadequate investigative infrastructure, slow international cooperation mechanisms, and the inherent architecture of the dark web. While the IT Act attempts to extend jurisdiction extraterritorially, enforcement is constrained by global privacy regimes, technological

ISSN: 2582-6433

anonymity, and diplomatic barriers.

A broader issue lies in the absence of harmonized global cyber governance. Without multilateral frameworks that facilitate real-time evidence sharing and coordinated operations, India's enforcement efforts remain fragmented and reactive. The increasing sophistication of darknet markets demands proactive, technologically advanced, and globally integrated strategies.

Conclusion

Darknet crimes transcend territorial boundaries, making traditional jurisdictional doctrines insufficient for modern cybercrime investigations. India's legal system, although equipped with theoretical extra-territorial provisions, struggles with technological anonymity, offshore servers, encrypted networks, and non-cooperative foreign jurisdictions. Strengthening domestic cyber capabilities, modernizing legal frameworks, joining or creating international cybercrime treaties, and establishing a specialized national darknet enforcement body are essential steps toward improving India's response. Without a harmonized, technologically adaptive, and globally connected investigative model, India risks remaining vulnerable to increasingly complex darknet threats.

References

- Arun Sukumar. 2020. "Cybersecurity in India: Future Challenges". Observer Research Foundation.
- CERT-In. 2021–2023. "Annual Cyber Security Reports". Government of India.
- Digital Personal Data Protection Act, 2023. Government of India.
- Enforcement Directorate. 2021–2023. "Cryptocurrency Investigation Briefings".
- Europol. 2022. "Internet Organised Crime Threat Assessment".
- Information Technology Act, 2000. Government of India.
- Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
- Ministry of Home Affairs. 2023. "Indian Cyber Crime Coordination Centre (I4C) Report".
- Narcotics Control Bureau. 2021–2023. "Darknet Narcotics Case Reports".
- National Crime Records Bureau. 2022. "Crime in India".
- UNODC. 2020. "Global Darknet Crime Trends Report".