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

EDITORIAL TEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

 ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

 ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

LEGISLATIVE FRAMEWORK IN COMBATING DARK WEB CRIMES

AUTHORED BY - MUTHULAKSHMI B
Sastra Deemed To Be University, Thanjavur

ABSTRACT:

The dark web's complicated terrain, classification, accessibility, and related illegal activity, as well as the unique difficulties it poses for Indian law enforcement. The dark web, a tiny but well-known section of the internet, uses encryption and anonymity technologies to facilitate both legal and illegal activity. The article describes the several browsers that are used to access the dark web, including Tor, I2P, and Freenet, and makes a distinction between the surface web, deep web, and black web. Effective intervention measures are urgently needed, as evidenced by the illicit activities that are common on the dark web, such as drug and people trafficking, information leakage, child pornography, and numerous forms of cybercrime. The study examines India's current legislative framework in light of these urgent concerns, summarising pertinent statutes such as the Prevention of Money Laundering Act, the Indian Penal Code, and the Information Technology Act. In order to effectively address crimes associated to the dark web, it highlights the need for extensive changes, public awareness campaigns, and improved international cooperation. Additionally, the value of international collaborations is emphasised, especially in light of India's joint initiatives with foreign law enforcement organisations via platforms like the Global Conference on Cyberspace and the QUAD. The study concludes by outlining the possible advantages for India of joining Europol's European Cybercrime Centre (EC3), such as access to real-time intelligence, coordinated operations, and cybersecurity best practices. This all-encompassing strategy seeks to improve national and international cybersecurity initiatives by giving India the instruments and frameworks required to address the complex problems presented by the dark web.

Key words: Dark web, Cybercrime, awareness, campaigns, challenges.

 ISSN: 2582-6433

I. RESEARCH GAP:

The primary research problem is the inadequacy of existing legal framework to effectively govern the use of dark web. Current regulations often fail to address the specific challenges posed by dark web.

II. RESEARCH PROBLEM

To identify the impact of dark web in the country and the need for legislative framework to address it.

III. RESEARCH OBJECTIVE

The objectives of this research are to identify and analyses the regulatory challenges faced by dark web. Specifically, the research aims to:

1. To trace the series of notorious event in the dark web
2. Assess the gaps in existing legal framework related to dark web
3. Recommend best practices for combating dark web crimes globally

IV. RESEARCH QUESTIONS

1. What are the key challenges posed by dark web?
2. How do current legal framework address issues posed by dark web?
3. What recommendations can be made to improve the legislative framework to combat the dark web crimes?

V. RESEARCH HYPOTHESIS

1. The problems posed by dark web outweigh its benefits.
2. Current legal frameworks are inadequate in combating dark web crimes.
3. Enhanced legislative framework can curb the notorious activities occurring through dark web.

VI. RESEARCH METHOD

The present study employs the secondary data collection method, which involves reviewing, analyzing, and scrutinizing previously published materials, including books, journals, and other written sources relevant to the topic. This work, which is entirely reference-based, relies on secondary research methods.

 ISSN: 2582-6433

Literature review: A comprehensive review of existing literature on legality of Dark Web, Onion Router and its role in accessing Dark Web, crimes against women and children perpetuated through Dark Web, International and National measures undertaken to combat and regulate the activities in this regard.

Analysis of regulatory framework: the review involved analyzing current legal frameworks such as Information Technology Act, Indian Penal Code along with International Cooperations.

Identification of Gaps: The literature review aimed to identify gaps in existing regulations related to dark web.

VII. LITERATURE REVIEW:

A study by Purbita MazumdaraIs on "The Dark web Illegal in India: A Comprehensive Study" examines the legal challenges surrounding the dark web in India. It explains that while accessing the dark web is not illegal, certain activities performed there, such as drug trafficking, child pornography, and weapons trading, are criminalized under Indian law. The dark web offers high levels of anonymity, making it difficult for law enforcement to track illegal activities. The paper argues that India's legal framework, including the Information Technology Act and the Indian Penal Code, needs stronger cyber laws and regulations to effectively address the increasing criminal use of the dark web. It concludes that while the dark web can be accessed legally, the intent and actions taken on it determine legality, and stronger legislative efforts are needed to prevent its misuse for illegal purposes.[1]

The paper "The Internet, Child Pornography and Cloud Computing: The Dark Side of the Web" by Mark O'Brien focuses on the challenges posed by technological developments like cloud computing and tools such as the Onion Router (TOR) in facilitating illegal activities on the dark web. The paper emphasizes the use of these technologies for the distribution and concealment of child pornography, which presents significant regulatory and legal hurdles. It argues that traditional policing and outdated regulatory practices are inadequate in addressing these issues due to the deep web's anonymity and encryption. The paper suggests that alternative regulatory models, including user-based self-regulation, could offer a more effective approach to combatting such illegal online activities.[2]

[1] **Mazumdar, P.** *Is the Dark Web Illegal in India: A Comprehensive Study*, 2 *Jus Corpus L.J.* 944 (2021).
[2] **O'Brien, M.** *The Internet, Child Pornography and Cloud Computing: The Dark Side of the Web?*, 23(3) *Info. & Commc'ns Tech. L.* 238 (2014).

 ISSN: 2582-6433

The paper "The Dark Web Ecosystem and the Risks It Poses to Women" by Riddhi Tripathi and Surya Dubey explores how the dark web's anonymity and encryption foster illicit activities, particularly targeting women. Women face threats like trafficking, blackmail, and privacy violations. Current cyber laws, especially in India, are insufficient to combat these crimes, and enforcement is challenging due to the anonymity of the dark web. The authors advocate for stronger regulations, better law enforcement training, and public awareness to protect women from these risks.[3]

The paper "An Untapped Network - A Legal Analysis on Dark Web and Deep Web in India" by S. M. Abinaya explores the distinctions between the surface web, deep web, and dark web, with a focus on the legal challenges posed by the dark web in India. The dark web, a hidden part of the internet, is often used for illicit activities such as drug trafficking, human trafficking, and cybercrimes. Despite its vast size and the increase in criminal activity, India lacks direct legislation addressing the dark web's illegal uses. The paper emphasizes the need for stronger laws and law enforcement capabilities to regulate and curb the misuse of the dark web in the country.[4]

The paper "Dark Web: A Web of Crimes" by Shubhdeep Kaur and Sukhchandan Randhawa provides a comprehensive overview of the dark web, focusing on its hidden nature and its association with various criminal activities. The paper discusses the origins of the dark web through technologies like Onion Routing, developed by the U.S. Navy, and highlights its use for illicit purposes such as drug trafficking, human trafficking, child pornography, fraud, and hacking. The anonymity provided by dark web browsers like TOR facilitates these illegal activities. The authors also examine different types of cyber-attacks linked to the dark web, such as DDoS, phishing, and ransomware, and the legal challenges faced by law enforcement agencies in regulating and combating dark web crimes. The paper stresses the importance of balancing the need for privacy with effective measures to curb the misuse of the dark web.[5]

The paper "A Shot in the Dark: Australia's Proposed Encryption Laws and the Disruption Calculus" by Brendan Walker-Munro examines Australia's proposed encryption laws and their

[3]**Tripathi, R. & Dubey, S.** *The Dark Web Ecosystem and the Risks It Poses to Women in Light of Contemporary Cyber Security Regulations*, 2 *Int'l J.L. Mgmt. & Hum.* 6, 3380 (2023)..
[4]**Abinaya, S.M.** *An Untapped Network – A Legal Analysis on Dark Web and Deep Web in India*, 2 *Indian J.L. & Legal Rsch.* 5, 1 (2023). .
[5]**Kaur, S. & Randhawa, S.** *Dark Web: A Web of Crimes*, 112 *Wireless Pers. Commc'ns* 2131 (2020).

 ISSN: 2582-6433

implications for law enforcement, national security, and privacy. It highlights the tension between the need for security and the challenges posed by encrypted communications, especially on the dark web, where criminal activities such as terrorism, drug trafficking, and other illicit behaviors can flourish under the cloak of anonymity. The legislation introduced by the Australian government seeks to compel companies to provide access to encrypted communications, but the paper argues that this approach is unlikely to be effective due to the nature of encryption and the global nature of technology companies. The author suggests a more holistic approach, including better regulatory tools and international cooperation, to balance privacy concerns with the needs of law enforcement.[6]

VIII. INTRODUCTION

The dark web is a section of the internet that can only be accessed via specialised software, such the Tor browser, and is not indexed by conventional search engines. It is present on darknets, which are overlay networks that allow users to interact and carry out operations in an anonymous manner. Techniques like onion routing, which encrypts user data and sends it via several servers, make it difficult to identify the original source and provide this anonymity. The dark web has genuine uses even though it is frequently linked to illicit operations including drug trafficking, the selling of firearms, and the sharing of stolen data. For example, it can give political dissidents in repressive governments a forum to exchange information and converse safely without being watched by the authorities. The phrase "dark web" is occasionally used interchangeably with "deep web," which refers to the entirety of the internet that search engines do not index; nevertheless, the dark web is merely a minority of the deep web. In conclusion, the dark web is distinguished by its anonymity and encryption, which permit both legal and illegal usage. The Surface Web, Deep Web, and Dark Web are the three primary categories into which the internet can be divided. Every one of these groups has unique traits and accessibility levels.

Surface Web

All publicly available web pages that search engines like Google, Bing, and Yahoo can index make up the Surface Web. It requires no special setup and is simple to use with standard web browsers. Just 4–10% of all digital material, including blogs, websites, news stories, and social

[6]**Walker-Munro, B.** *A Shot in the Dark: Australia's Proposed Encryption Laws and the Disruption Calculus*, 40 *Adel. L. Rev.* 783 (2019).

 ISSN: 2582-6433

networking platforms, is found on this portion of the internet.[7]

Deep Web

All areas of the internet not indexed by mainstream search engines are referred to as the Deep Web. A great deal of information is concealed behind paywalls, login forms, and other security precautions. Access cannot be found using standard search engines; required credentials or direct URLs are needed. Databases, private company websites, medical records, academic resources, and private emails are all part of the Deep Web, which makes up 90–96% of the internet.[8]

Dark Web

The Dark Web is a little portion of the Deep Web that has been purposefully concealed and is not visible in normal web browsers. It can only be accessed with specialised software, such as Tor or I2P. This area of the internet requires users to employ particular setups and tools, frequently using anonymity protocols. In repressive regimes, it encompasses unlawful activities like drug trafficking and criminal trading, but it also has valid uses for users who value their privacy. Though it only makes up 0.01% of all online material, the Dark Web is well-known for being connected to illegal businesses.[9]

IX. BROWERS TO ACCESS DARK WEB:

TOR browser

"The Onion Router," or Tor, is a specialised web browser made to give users privacy and anonymity when they access the internet. In order to accomplish this, online traffic is routed through a number of encrypted nodes, making it challenging to identify or track down the user. Tor, which was first created by the US Navy for encrypted communications, is now commonly used to access the dark web, which is made up of websites that are only accessible through the Tor browser and are not indexed by conventional search engines. Users need to download and install the Tor browser in order to access the dark web. They can join the Tor network, which is made up of many servers (nodes) run by volunteers that relay internet traffic, using this browser. Several levels of obscurity are created by encrypting each link, hence the term "onion

[7] *Types: Clear, Deep, Dark Web*, Martech Zone, https://martech.zone/types-clear-deep-dark-web/.
[8] *Surface Web, Deep Web, and Dark Web: Are They Different?*, CISO Platform, https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different.
[9] *Cybersecurity Spotlight: The Surface Web, Dark Web, and Deep Web*, CISA, https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web.

 ISSN: 2582-6433

routing." URLs that end in ". onion" are commonly seen on the dark web and can only be accessed with the Tor browser.[10]

I2P (Invisible Internet Project)

A decentralised, anonymous network layer called the Invisible Internet Project (I2P) was created to enable users to communicate privately with one another. I2P functions as a closed network, enabling anonymous user interaction within its ecosystem, in contrast to Tor, which links users to the wider internet. It makes use of a technique called garlic routing, which encrypts messages and routes them over several pathways, making it difficult for anyone to determine the data's origin or destination.I2P gives users access to "eepsites," or hidden websites, which are identified by URLs that finish in ".i2p." These websites can only be accessed over the I2P network and cannot be accessed with normal browsers. I2P allows users to exchange information and interact without disclosing their whereabouts or identities.

Freenet

A decentralised, peer-to-peer network called Freenet was created to make anonymous online conversation and data exchange possible. It is especially helpful in areas where free expression is prohibited since it enables users to access content without worrying about censorship. There are two ways that Freenet functions: Opennet, where users can connect to any node that is accessible, and Darknet, where they can only connect to peers they can trust. By hiding the names of users and the source of the shared data, this arrangement improves privacy and anonymity.

X. CRIMES IN DARK WEB

Drug trafficking

The illegal distribution and sale of restricted substances via anonymous online marketplaces is drug trafficking on the dark web. This approach, which frequently uses bitcoins for transactions, has grown in favour since it is thought to be anonymous and enables users to purchase narcotics without coming into direct touch with sellers. The dark web is a major issue for law enforcement organisations around the world since it promotes a variety of substances, such as fentanyl, methamphetamine, and cannabis.

[10] *How to Access the Dark Web Using the Tor Browser*, BleepingComputer, https://www.bleepingcomputer.com/tutorials/how-to-access-the-dark-web-using-the-tor-browser/.
4o

 ISSN: 2582-6433

Human Trafficking:

Traffickers use the dark web as a marketplace to take advantage of weaker people. It permits the use of coercion, fraud, and deceit in the recruitment, transportation, and exploitation of victims. Since traffickers frequently interact with cryptocurrency, it might be difficult for law authorities to track down their operations. The anonymity offered by the dark web makes anti-trafficking efforts more difficult because conventional investigative techniques could not work in this online environment.[11]

Information leakage:

Many websites, such as TOR, offer anonymity and are useful tools for activists, law enforcement, and whistleblowers. Additionally, hackers are now able to release private data on the dark web. An example is the 9.7 GB data dump of almost 32 million Ashley Madison users that was once made public by a hacking collective. Comparably, in 2017, more than 1.4 billion personal records were readily available due to a plain text leak on the dark web. Furthermore, some dark web hubs provide incentives for people to divulge company information.

Child pornography:

The large number of forums devoted to the sharing of child sexual abuse material (CSAM) on the dark web makes child pornography a serious and concerning problem. People involved in illegal activities, such as the distribution and possession of CSAM, are drawn to the dark web because of its anonymity, which is made possible by tools like TOR.

Carding and Payment Fraud:

There are many sites for exchanging credit card details that have been stolen and enabling illegal purchases using PayPal and Bitcoin. These transactions frequently take advantage of cryptocurrency' anonymity.[12]

Arm trafficking

The illicit sale and distribution of weapons, ammunition, and explosives through encrypted online marketplaces is a major and expanding aspect of arms trafficking on the dark web. At over 60% of these transactions, the majority of illegal firearms traded on the dark web come

[11] *Laws Relating to the Dark Web in India*, iPleaders (2021), https://blog.ipleaders.in/laws-relating-dark-web-india/.
[12] *Dark Web Facts*, Avast, https://www.avast.com/c-dark-web-facts.

 ISSN: 2582-6433

from the United States. Additionally, European markets make a substantial contribution, producing five times as much income as U.S. sales.[13]

Onion cloning

Cloning an onion is similar to utilising a proxy. The scammer duplicates the authentic website or page and changes the links to trick users into visiting their fake websites and stealing money.

Red room crimes

The term "Red Room" sites, which are known to exist on the dark web, describes purported platforms where people can watch live streaming of severe violence, such as torture and murder, for astronomical prices. Although these assertions are terrifying, there isn't much solid proof to corroborate their existence. Such live streaming is unlikely to happen successfully due to the TOR network's technological constraints, mainly its poor speeds, according to experts. The case of Australian Peter Gerard Scully, who was found guilty of horrendous crimes against minors, is one notorious instance that has brought attention to the dark web's potential for violent content. Scully ran a website called "No Limits Fun" (NLF) where he created and marketed videos showing children being severely abused and tortured, including the well-known movie "Daisy's Destruction." According to reports, this movie, which showed explicit scenes of child sexual abuse, sold for as much as $10,000 per view. Scully's actions were a part of a larger global child exploitation network that took advantage of the Philippines' most vulnerable youngsters. After being taken into custody in 2015, Scully was found guilty of his crimes in 2018 and given a life sentence. Given how far some people will go to produce and disseminate unlawful content online, his case has stoked conjecture regarding the existence of Red Rooms. Nonetheless, a lot of specialists consider the idea of Red Rooms to be mainly fictitious or overblown, frequently writing them off as urban legends or frauds spread on forums without solid proof.[14]

[13] *UNODC Analyses the Policy Implications of Illicit Firearms Trafficking on the Dark Web*, United Nations Office on Drugs and Crime (2021), https://www.unodc.org/unodc/en/firearms-protocol/news/unodc-analyses-the-policy-implications-of-illicit-firearms-trafficking-on-the-dark-web.html.
[14] *Kolkata Doctor Rape-Murder Case: Accused Sanjay Roy Was Drunk and Watched Porn, Says Bengal Police*, India Today (Aug. 11, 2024), https://www.indiatoday.in/india/story/kolkata-doctor-rape-murder-case-accused-sanjay-roy-liquor-watched-porn-bengal-police-2580653-2024-08-11.

 ISSN: 2582-6433

XI. MALWARE ATTACKS:

Data stealing trojans

Theft of Data Trojan horses are harmful programs meant to break into systems and compromise private data. They have the ability to disable antivirus software, intercept keystrokes, copy passwords from the clipboard, and move files to an attacker's email. The value of the stolen data can be much larger, even if hiring a burglar with these trojans costs about $10.

Ransomware

Malware that encrypts files or entire systems and prevents users from accessing them until a ransom is paid to decrypt them is known as ransomware. Ransomware cases typically cost around $270, which emphasises the financial strain on victims. Attackers frequently target businesses that are thought to pay quickly, such government institutions and medical facilities, who need instant access to their data. Law firms and other organisations that handle sensitive data may also choose to pay ransoms in order to stop breaches from being made public, which leaves them especially open to attacks using leakware. Attackers are using a variety of strategies to increase their control over victims as the ransomware assault scenario has changed. This covers not just encryption but also data theft and public disclosure concerns, which can force companies to respond to ransom requests faster. Increased cybersecurity and resilience plans are required as a result of the growing emphasis on ransomware as a major problem for organisations due to the ongoing rise in cyber-attacks.[15]

Botnet malware:

On the dark web, malware that builds botnets can be bought for as little as $200. Typically, a whole bundle that contains different modules and server applications costs between $1,000 and $1,500. The versatility of this kind of malware demonstrates how cybercriminals are expanding their attack tactics. Virobot is one example of a botnet ransomware that spreads to other victims by integrating itself into a spam botnet after infecting a device. Virobot uses RSA encryption to protect data on the targeted machine. Its keylogger function also records victims' private information and sends it to a command-and-control (C2) server. Virobot's botnet capability enables it to send spam emails to every contact on a compromised machine's Microsoft Outlook account. Virobot was initially discovered on September 17 and is currently still under

[15] *Global Ransomware Damage Costs Predicted to Reach $250 Billion USD by 2031*, Cybersecurity Ventures (2023), https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

 ISSN: 2582-6433

development.[16]

ATM malware:

The purpose of ATM malware, especially Trojan horses, is to steal money from ATMs, which have the capacity to store up to $200,000. Such spyware is among the priciest kinds of malware accessible, with a starting price of about $1,500. Multiple ATMs can be targeted by a single piece of software. Exploits, which exploit software or system flaws, are commonly available on the dark web and are regularly customised for different platforms. A vast user base and average pricing of $2,540 in 2017–2018 make Windows-based vulnerabilities particularly popular. The pricing range for MacOS exploits is $2,200 to $5,300. While individuals that obfuscate malware can make roughly $25 per month through subscriptions, malware developers usually charge $500 for their initial work.[17]

XII. LEGAL FRAMEWORKS FOR CYBERCRIME IN INDIA

Information Technology Act, 2000 (IT Act)

The Information Technology Act, 2000 is the primary legislation governing cybercrimes in India. Several provisions of the IT Act are relevant in combating illegal activities on the dark web:

- Section 66 (Computer-Related Offenses): This section criminalizes hacking, unauthorized access, and other illegal activities related to computer systems. Many dark web activities involve hacking or unauthorized access to data, making this a key provision in tackling dark web crimes.
- Section 66E (Violation of Privacy): The sale of personal data, which is prevalent on the dark web, can be prosecuted under this section. It penalizes the capture, transmission, and publishing of private images without consent.
- Section 67 (Obscene Content): Dark web platforms are frequently used for distributing obscene or sexually explicit content. Section 67 criminalizes the publishing or transmission of such material in electronic form, which includes dark web activities.
- Section 69 (Government Powers to Intercept, Monitor, or Decrypt): Section 69 of the IT Act allows government authorities to intercept and monitor online communication

[16] *Kaspersky Finds Botnet Prices Starting at $100 on Dark Web Market*, CXOToday (2022), https://cxotoday.com/press-release/kaspersky-finds-botnet-prices-starting-at-100-on-dark-web-market/.
[17] *Tyupkin Malware: ATM Security Malware*, Kaspersky, https://www.kaspersky.com/resource-center/threats/tyupkin-malware-atm-security-malware

 ISSN: 2582-6433

to protect national security and prevent offenses. This is critical for tracking and disrupting dark web activities related to terrorism, organized crime, and drug trafficking.

- Section 70 (Protected Systems): This section ensures the protection of critical infrastructure and computer systems that may be targeted by dark web hackers.
- Section 79 (Intermediary Liability): This section provides immunity to intermediaries (such as internet service providers and platform operators) from liability, provided they comply with government directives and do not knowingly host illegal content. This provision helps regulate online platforms, including those that might facilitate dark web activities.[18]

Indian Penal Code, 1860 (IPC)

In addition to the IT Act, several sections of the Indian Penal Code (IPC) are invoked to tackle crimes facilitated by the dark web:

- Section 420 (Cheating and Fraud): Many dark web crimes involve fraud, such as scams and fake services. Section 420 penalizes cheating and fraud, which can be applied to online transactions conducted through the dark web.
- Section 463 and 465 (Forgery): The dark web is used to sell forged documents, counterfeit currency, and fake identity credentials. These provisions of the IPC criminalize forgery.
- Section 468 (Forgery for Purpose of Cheating): This section specifically deals with forgery committed for the purpose of cheating, which can include the creation and sale of fake documents on the dark web.[19]

Prevention of Money Laundering Act, 2002 (PMLA)

The PMLA (Prevention of Money Laundering Act) is crucial in preventing financial crimes that are made possible via the dark web, especially when cryptocurrencies are involved:

- Tracking and Regulating bitcoin: The dark web mostly uses bitcoin transactions to sell illicit products and services. Financial institutions must notify the Financial Intelligence Unit-India (FIU-IND) of any questionable transactions under the PMLA. This information is used by law enforcement to monitor cryptocurrency transactions

[18]**Carr, N.G.** *Does IT Matter?: Information Technology and the Corrosion of Competitive Advantage* (Harvard Business Press 2004).
[19] **Malgi, S.** *Cyber Crimes under Indian IT Laws*, 3(6) *Int'l J. Sci. & Eng'g Research* 1 (2012).

 ISSN: 2582-6433

connected to crimes on the dark web, particularly those involving the financing of terrorism and money laundering.[20]

Narcotic Drugs and Psychotropic Substances Act, 1985 (NDPS Act)

India's legislative framework for preventing drug-related offences, particularly those made possible via the dark web, is centred on the NDPS Act:

Dark Web Drug Trafficking: Illegal drug sales take occur on the dark web, which is a major marketplace. The manufacture, distribution, and sale of narcotic narcotics and psychotropic substances are illegal under the NDPS Act, regardless of whether they take place in person online Criminal Investigations: Indian law enforcement has been keeping a closer eye on drug transactions on the dark web, and some successful investigations have resulted in the arrest of drug traffickers using these platforms.[21]

National Cyber Security Policy, 2013

The National Cyber Security Policy seeks to establish a safe online environment in India, while not being a law. It covers topics pertaining to cybercrime, such as those that come from the dark web

Cybersecurity Standards and Monitoring: The policy highlights the necessity of safeguarding government systems, enterprises, and key infrastructure against cyberattacks, many of which are orchestrated via the dark web. This entails encouraging collaboration amongst government entities and implementing global cybersecurity best practices.

Capacity Building: By offering education, resources, and experience, it seeks to increase law enforcement organisations' ability to combat cybercrimes, especially those involving the dark web.[22]

The Reserve Bank of India (RBI) Guidelines on Cryptocurrency

On the dark web, cryptocurrencies are frequently used as a medium of exchange for illicit transactions. The RBI published instructions in 2018 preventing financial institutions from assisting cryptocurrency transactions, but the Supreme Court overruled these rules in 2020.

[20]**Chowbe, V.S.** *Redefining the Fight Against White Collar Crime: A Moral and Value-Centric Perspective*, SSRN, https://ssrn.com/abstract=4761381 (2024).

[21]**Pathan, A.B. & Chakravarty, P.** *Assessing the Provisional and Conventional Acts to Control the Use of Narcotics Drugs and Psychotropic Substances for Individual's Well-Being: Implicating the Amendments and Laws Dealing with Misuse of NDPS*, 20(9) *NeuroQuantology* 1812 (2022).

[22]**White, J.** *Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies*, 7(4) *Global Sec. Stud.* (2016).

 ISSN: 2582-6433

The RBI has not legally legalised or outlawed cryptocurrencies.

- Cryptocurrency Regulation: In order to monitor and manage transactions on the dark web, India is now developing specific laws to regulate cryptocurrencies. In order to control digital currencies and prevent their usage in dark web-related activities, the government is anticipated to introduce the Cryptocurrency and Regulation of Official Digital Currency Bill.[23]

Indian Evidence Act, 1872

- Prosecution of cybercrimes, particularly those perpetrated on the dark web, depends heavily on the Indian Evidence Act. It regulates whether digital evidence is admissible in court:
- Admissibility of Electronic Evidence, Section 65B: This clause permits electronic documents, including messages and data from dark web services, to be admitted as evidence in court. It is a crucial instrument for the prosecution of cybercriminals who work behind the scenes on the dark web.[24]

XIII. INTERNATIONAL COOPERATION

Cybercrime frequently crosses national boundaries. International collaboration is essential. Interacting with foreign law enforcement organisations can yield important information and tools for combating crimes committed on the dark web across borders. India's strategy to combating dark web crimes can benefit from lessons learnt from nations that have effectively put policies in place. India's current cybersecurity collaborations are especially pertinent to reducing dark web activity since they foster information exchange, cooperative efforts, technological know-how, and legislative frameworks. These collaborations directly address the following dark web threats:

QUAD Cybersecurity Cooperation and Dark Web Curbing

The QUAD, which consists of the US, Japan, Australia, and India, has created a comprehensive plan to improve cybersecurity in the Indo-Pacific area, including dealing with dark web concerns. Here, the emphasis is on cyber defence, intelligence sharing, and teamwork in

[23]**Munjal, A.** *Cryptocurrency in India with Special Reference to Internet and Mobile Association of India v. Reserve Bank of India*, 1 *Int'l J. L. Mgmt. & Humanities* 905 (2023).
[24]**Vaidialingam, A.** *Authenticating Electronic Evidence: Sec. 65B, Indian Evidence Act, 1872*, 8 *NUJS L. Rev.* 43 (2015).

 ISSN: 2582-6433

identifying illicit activity on the dark web. Real-time intelligence sharing is one of the best strategies to counter the dark web. Members of QUAD share information about criminal networks operating on the dark web, including those engaged in terrorist financing, illegal arms sales, drug and human trafficking, and more. This facilitates prompt threat identification and aids in the coordination of international law enforcement activities. The majority of dark web transactions use cryptocurrencies like Bitcoin, which are more difficult to track down. The QUAD is working to improve member nations' capacity to monitor illegal cryptocurrency transactions. By utilizing cutting-edge tools and working together on financial intelligence, QUAD members can keep an eye on suspected blockchain activity that indicates the use of the dark web, enabling prompt action to freeze assets or apprehend individuals. The QUAD's collaboration in cybersecurity opens the door for cooperative law enforcement efforts to take down dark web marketplaces. These operations may entail coordinated efforts across several nations to guarantee that the owners and users of these illicit platforms face legal action in accordance with applicable laws. For instance, India gains access to the same strategies and investigative tools employed in the US's several well-publicized takedowns of dark web marketplaces through the QUAD.[25]

Limitations

The anonymity and encryption techniques like Tor that make it hard to track down criminal networks are the main reason why the QUAD's efforts to stop dark web activity are limited. The usage of cryptocurrencies like Bitcoin and more private coins like Monero makes it more difficult to keep an eye on illegal transactions, even with intelligence sharing. Furthermore, operators of the dark web are always improving their strategies, frequently surpassing the technological advancements of law enforcement. Coordinated actions are further hampered by jurisdictional concerns, as different nations have different legal systems that make simultaneous operations difficult. Lastly, the QUAD's ability to completely destroy illicit marketplaces is constrained by the size of the dark web and the resource-intensive nature of investigations.

Global Conference On Cyber Space (GCCS) And Dark Web Prevention

India may join with a worldwide network of nations to curb cybercrime, including dark web activity, through the GCCS platform. In order to create standardised legal frameworks that

[25]**Takahashi, K., Ide, T., Takahashi, I., Tokito, K., & Sasaki, T.** *Building Cooperation: Cyber, Critical Technology and National Security* (Quad Tech Network Series, Australian National University, 2021).

 ISSN: 2582-6433

address cybercrime, particularly that which occurs on the dark web, GCCS encourages collaboration across nations. India has sought to bring its cybercrime laws into compliance with international norms through its participation in GCCS, allowing for the cross-border prosecution of offenders operating on the dark web. India takes part in initiatives through GCCS to strengthen its law enforcement authorities' capacity to combat crimes committed on the dark web. This involves instruction in sophisticated cyber forensics to track down and disrupt dark web activities. Through international collaboration, methods such as deep web mining, metadata analysis, and machine learning algorithms to reveal hidden networks are exchanged and improved. Through GCCS, India can access state-of-the-art cyber defence tools created by other countries, which aid law enforcement in tracking actions that would otherwise stay anonymous and identifying hidden dark web sites (using Tor or I2P).[26]

Limitations

In order to effectively control dark web activity, the Global Conference on Cyber Space (GCCS) effort must overcome a number of obstacles. Cross-border prosecution is challenging due to national legal disparities, and criminals take advantage of legal loopholes in cybercrime legislation. Furthermore, operators of the dark web are constantly improving their strategies, frequently surpassing the forensics tools and procedures that are offered through GCCS collaboration. To properly utilise cutting-edge technologies like deep web mining and machine learning for detecting hidden networks, many law enforcement organisations lack the necessary resources and skills. While bureaucratic delays, jurisdictional problems, and differing levels of commitment from participating states impede global coordination, anonymity mechanisms like Tor and I2P further complicate efforts to take down black web sites.

Bilateral Cybersecurity Dialogues And Dark Web Intelligence

By encouraging direct collaboration in combating cybercrime, India's bilateral cybersecurity discussions with nations including the US, EU, and Japan are essential to reducing the dark web. These discussions include:

[26]**Bhatia, A., Kumar, A., Verma, P., Kumar, M., & Kumar, J.** *Cyber Threat: A Review on Dark Sides of Dark Web*, in *2023 3rd Int'l Conf. on Advancement in Electronics & Commc'n Eng'g (AECE)* 306-10 (IEEE, Nov. 2023)..

 ISSN: 2582-6433

United States

In terms of investigating crimes on the dark web, India and the US have a strong partnership. The United States has vast expertise in taking down the dark web (e.g., Operation DisrupTor and Operation Bayonet against AlphaBay). India gains access to the investigative methods and intelligence networks created by the United States to track illicit activities on the dark web through bilateral cybersecurity agreements. Advanced methods for tracking cryptocurrency transactions connected to the dark web have been developed by US law enforcement agencies such as the FBI and the DEA. By working with US agencies to use these technology, India's law enforcement may more effectively monitor money flowing through dark web portals. India receives access to dark web monitoring tools as part of this collaboration, which are used by US agencies to keep tabs on criminal activity, spot new illicit markets, and stop the sale of illicit commodities like weapons, drugs, or stolen data.

European Union (EU)

In order to prevent illicit data sales on the dark web, India is aligning its own data protection regulations with the strict data protection requirements established by the EU's General Data Protection Regulation (GDPR) through cyber dialogues with the EU. Due to GDPR's emphasis on holding companies responsible for data breaches, EU nations keep a close eye on data thefts, which frequently come via the dark web, and communicate intelligence about them to India. India benefits from collaboration with Europol through the EU, which has been crucial in thwarting extensive dark web activities such as the shutdown of Dark Market. India can also share intelligence on transnational dark web activity with Interpol, which collaborates closely with EU countries. These partnerships improve India's capacity to find and apprehend cybercriminals around the world.

Limitations

India has a number of obstacles in effectively reducing dark web activity in its bilateral cybersecurity discussions with the US, EU, and Japan. Law enforcement finds it challenging to stay up to date with the ever-evolving strategies used by criminals on the dark web to evade discovery, especially with the sophisticated tools these partner’s supply. Although methods for tracking cryptocurrency transactions are available in the US and the EU, using privacy-focused coins like Monero makes it more difficult to trace down illegal payments. Furthermore, the complete adoption of these monitoring systems is hampered by India's inadequate financial and technical capabilities. Additionally, jurisdictional difficulties hinder cross-border

 ISSN: 2582-6433

investigations, slowing down and decreasing the effectiveness of coordinated operations. It is also challenging to strike a balance between privacy and enforcement due to conflicts between dark web surveillance tools and data protection regulations like GDPR. Finally, the smooth execution of coordinated actions against illegal activity on the dark web is frequently hampered by fragmented international collaboration with varying goals and levels of commitment.[27]

XIV. RECOMMENDATIONS

Public awareness campaigns

People may refrain from committing crimes if they are made aware of the dangers posed by the dark web. Participation can be decreased by holding workshops and seminars to inform the public about the risks posed by the dark web and its link to illegal activity. Community efforts against cybercrime can be strengthened by collaborating with non-governmental organisations to raise awareness about online safety and the consequences of using dark web marketplaces.[28]

XV. CONCLUSION:

India must implement a proactive and all-encompassing plan to tackle such crimes because of the serious problems posed by the dark web. In order to successfully negotiate the intricacies of the dark web, this study emphasises the need for strengthened legislative frameworks, better law enforcement capabilities, and higher public knowledge. While possible participation in the European Cybercrime Centre (EC3) can further bolster India's capabilities, international cooperation is crucial for intelligence sharing and cooperative efforts through platforms like QUAD and GCCS. These efforts must, however, get beyond obstacles including disparate legal systems, changing criminal strategies, and the dark web's intrinsic anonymity. By prioritising public education and cultivating global collaborations, India can provide its law enforcement with the resources they need to successfully tackle cyber threats. In the end, a cooperative and multifaceted strategy would allow India to safeguard its digital environment and make a significant contribution to the worldwide battle against crimes connected to the dark web, opening the door to a safer online environment.

[27] **Remington, T., Spirito, C., Chernenko, E., Demidov, O., & Kabernik, V.** *Toward US-Russia Bilateral Cooperation in the Sphere of Cybersecurity*, Working Group Paper on the Future of US-Russia Relations (2016).
[28] *Ways to Protect Yourself from Cyber Crime*, Policy Bazaar, https://www.policybazaar.com/corporate-insurance/articles/ways-to-protect-yourself-from-cyber-crime/.
4o m

 ISSN: 2582-6433

REFERENCES:

- **Mazumdar, P.** *Is the Dark Web Illegal in India: A Comprehensive Study*, 2 *Jus Corpus L.J.* 944 (2021).
- **O'Brien, M.** *The Internet, Child Pornography and Cloud Computing: The Dark Side of the Web?*, 23(3) *Info. & Commc'ns Tech. L.* 238-55 (2014).
- **Tripathi, R. & Dubey, S.** *The Dark Web Ecosystem and the Risks It Poses to Women in Light of Contemporary Cyber Security Regulations*, 2 *Int'l J.L. Mgmt. & Humanities* 3380 (2023).
- **Abinaya, S.M.** *An Untapped Network: A Legal Analysis on Dark Web and Deep Web in India*, 2 *Indian J.L. & Legal Rsch.* 1 (2023).
- **Kaur, S. & Randhawa, S.** *Dark Web: A Web of Crimes*, 112 *Wireless Pers. Commc'ns* 2131-58 (2020).
- **Walker-Munro, B.** *A Shot in the Dark: Australia's Proposed Encryption Laws and the Disruption Calculus*, 40 *Adel. L. Rev.* 783 (2019).