INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

ISSN: 2582-6433

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

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.

www.ijlra.com
Volume 2 Issue 7 | June 2023
ISSN: 2582-6433

THE DARK SIDE OF THE WEB: AN EXAMINATION OF THE LEGAL CHALLENGES IN REGULATING THE DARK WEB IN INDIA

AUTHORED BY - SURYADEVARA MOUNISH CHANUKYA

ABSTRACT

This legal research paper examines the legal challenges in regulating the dark web in India. The dark web is a hidden part of the internet that is not indexed by search engines and is only accessible through specialized software. It is often associated with illegal activities such as drug trafficking, human trafficking, and terrorism. In recent years, law enforcement agencies have been struggling to combat these crimes on the dark web. This paper explores the legal framework surrounding the dark web in India, discussing the current legislation in place and identifying the gaps and limitations in these laws. It analyses the challenges faced by law enforcement agencies in regulating the dark web and prosecuting offenders. Additionally, the paper examines the role of technology in facilitating criminal activities on the dark web and the need for innovative solutions to address these challenges. It argues for a comprehensive legal framework that takes into account the unique characteristics of the dark web and enables law enforcement agencies to effectively combat criminal activities. In conclusion, this paper provides insights into the legal challenges in regulating the dark web in India and highlights the need for a multi-faceted approach involving technology, law enforcement agencies, and legislative initiatives to effectively combat the dark side of the web.

***Key Words**: Dark web, Legal challenges, Regulation, Law enforcement, Criminal activities.*

INTRODUCTION

With the advent of the internet, the world has become a smaller place, and information is just a click away. However, alongside the advantages of the internet, it has also emerged as a dark and mysterious place known as the "Dark Web." The Dark Web is the portion of the internet that is not indexed by search engines and can be accessed only through specific software, configuration,

ISSN: 2582-6433

or authorization. It is a virtual underworld that harbours different types of illegal activities like drug trafficking, arms dealing, child pornography, and hacking.[1]

In India, the Dark Web has become a major concern for law enforcement agencies.[2] It poses significant legal challenges as it provides anonymity and shield to the perpetrators of cybercrime, making it difficult for law enforcement to trace and prosecute them. This paper aims to examine the legal challenges in regulating the Dark Web in India.

The significance of studying the legal challenges of regulating the Dark Web in India can be gauged from the widespread use of the Deep Web for criminal activities. The Deep Web is an unindexed portion of the World Wide Web, and the Dark Web is a part of it. The Dark Web has emerged as a hub of illegal activities in India, including drug trafficking, cyber frauds, and human trafficking.[3] Given the increased usage of the Deep Web and the Dark Web over the years, it is imperative to establish effective measures to regulate it.

This paper's purpose is to examine the legal challenges that exist in regulating the Dark Web in India. The scope of the study is limited to the examination of various provisions of Indian laws that govern the use of the internet. The study also considers Indian judicial decisions that have dealt with cases relating to the Dark Web.

In light of the above, the paper will be divided into five parts. Part one will provide an overview of the Dark Web, providing insight into its activities and functionality. Part two will examine the legal challenges associated with regulating the Dark Web in India. Part three will discuss the legal framework in India for regulating the internet and the Dark Web. Part four will examine the measures that the government has taken to curb the use of the Dark Web in India. Part five will conclude with recommendations on how to effectively regulate the Dark Web in India.

[1] Soumya Sundar Chowdhury, "Crime on the Dark Web: An Investigation into the Use of Bitcoin for Illegal Activities," Journal of Financial Crime 27, no. 1 (2020): 218-234.
[2] Cyber Crime Cell, "Dark Web," Mumbai Police, https://mumbaipolice.gov.in/cyber-crime-cell/regular-web-and-dark-web (last visited Mar. 27, 2023).
[3] T. R. Andhavarapu, "Cyber Crimes on Deep Web in India," International Journal of Research and Analytical Reviews 6, no. 3 (2019): 443-452.

ISSN: 2582-6433

LEGAL FRAMEWORK SURROUNDING THE DARK WEB IN INDIA

The Dark Web has become a new front in the battle against online crime, making it difficult for law enforcement agencies to monitor the flow of information, goods, and services. The legal framework surrounding the Dark Web in India is still evolving, and there is no specific legislation that deals with it. It is therefore important to present an overview of the current legal framework in place for the Dark Web in India, analyses gaps, and limitations in existing laws, and compare them with other countries' legal frameworks.

India has implemented several laws to regulate cyberspace, but there is no specific legislation to regulate the Dark Web. However, several provisions in the Information Technology Act, 2000 (IT Act) and the Indian Penal Code, 1860 (IPC) can be applied to offenders operating in the Dark Web.[4]

Section 66 of the IT Act criminalizes computer-related offenses such as hacking, the introduction of malware, and email spoofing. Section 66B of the IT Act prohibits the use of stolen electronic signatures, and Section 66D of the IT Act punishes identity theft. In addition, Section 67C of the IT Act punishes the publication or transmission of material that contains sexually explicit acts.

The IPC provides for criminal liability for offenses such as theft, fraud, and extortion.[5] Section 378 of the IPC criminalizes theft and states that whoever "intending to take dishonestly any movable property out of the possession of any person" will be punished. Section 384 of the IPC criminalizes extortion and states that whoever "puts any person in fear of injury to that person or any other person" will be punished.

Despite the existence of laws that can be applied to offenders operating in the Dark Web, there are several gaps and limitations in the legal framework in India. Firstly, there is a lack of clarity regarding the scope of the offenses that can be charged under existing laws. Secondly, the existing

[4] Information Technology Act, 2000, s. 66, 67C, available at https://www.meity.gov.in/writereaddata/files/it_act2000.pdf (last visited March 27, 2023).
[5] Indian Penal Code, 1860, s. 378, 384, available at https://www.indiacode.nic.in/bitstream/123456789/12401/1/THE-INDIAN-PENAL-CODE-1860.pdf (last visited Mar. 27, 2023).

ISSN: 2582-6433

legal framework does not address issues such as anonymity and encryption, which are integral to the Dark Web. Also, the lack of clear guidelines for law enforcement agencies poses a challenge in investigating crimes committed on the Dark Web.

Several countries have enacted specific laws to regulate the Dark Web. For instance, The United States has enacted the Computer Fraud and Abuse Act, which prohibits unauthorized access to protected computers and damage to computer systems.[6] Similarly, countries such as Australia, Canada, and the United Kingdom have enacted specific legislation to regulate the Dark Web.[7]

In contrast, the legal framework surrounding the Dark Web in India is still evolving, and there is no specific legislation to regulate it. This has led to a lack of clarity regarding the scope of offenses and the legal provisions applicable to such offenses.

To address the challenges posed by the Dark Web, India needs to enact specific legislation to regulate it. The legislation should establish clear guidelines for law enforcement agencies, address issues such as anonymity and encryption, and identify the scope of offenses that can be charged under existing laws. Until then, Indian law enforcement agencies will continue to struggle to investigate and prosecute crimes committed on the Dark Web.

CHALLENGES FACED BY LAW ENFORCEMENT AGENCIES

The dark web is a hidden part of the internet that requires specific software to access it. It is often associated with illegal activities such as drug trafficking, weapons sales, and child pornography.[8] Regulating the Dark Web in India presents several legal challenges. Law enforcement agencies find it difficult to monitor and regulate this vast network of hidden websites, which use state-of-

[6] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018), available at https://www.justice.gov/criminal-fraud/computer-crime-and-intellectual-property-section/computer-fraud-and-abuse-act (last visited Mar. 27, 2023).

[7] Canada's Criminal Code, Sections 342.1 to 342.4, 430(1.1), 467.1 and 487.016, available at https://laws-lois.justice.gc.ca/eng/acts/c-46/page-73.html (last visited Mar. 27, 2023); UK Investigatory Powers Act 2016, available at https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (last visited Mar. 27, 2023); Australia's Criminal Code Amendment (Misuse of Digital Devices) Act 2013, available at https://www.legislation.gov.au/Details/C2013A00152 (last visited Mar. 27, 2023).

[8] The Telegraph, "What is the dark web, and how does it work?" September 29, 2020, https://www.telegraph.co.uk/technology/0/dark-web-work/ (last visited Mar. 27, 2023).

ISSN: 2582-6433

the-art encryption and other measures to prevent detection.[9]

One of the main difficulties in monitoring the dark web is the anonymous nature of its users. Criminals can use virtual private networks (VPNs) to change their IP addresses and cover their tracks. This makes it difficult for law enforcement agencies to detect their activities and gather evidence.[10]

Despite these challenges, there have been a few successful attempts at regulating the dark web. In 2018, the Indian authorities shut down six dark web-based arms trafficking groups and arrested six suspects. Similarly, in 2019, the Narcotics Control Bureau (NCB) busted an online drug trafficking network operating on the dark web, leading to several arrests.[11]

However, many more attempts at regulating the dark web have failed. Countermeasures deployed by criminals have made it increasingly difficult for law enforcement agencies to disrupt their networks. The use of cryptocurrencies, for instance, makes it challenging to trace financial transactions and identify the individuals behind them.[12] Moreover, the availability of sophisticated encryption tools has made it possible for criminals to communicate with each other without being detected.[13]

Law enforcement agencies in India face several limitations and constraints when it comes to regulating the dark web. One of such restraints is inadequate awareness and training. Law enforcement agencies need specialized training and equipment to keep up with the ever-evolving tools and techniques used by cybercriminals on the dark web. Additionally, Indian laws like the Information Technology (Amendment) Act 2008 often appear to fall short of holding individuals

[9] PTI, "Govt to block websites selling drugs, guns and child porn," Times of India, February 8, 2016, https://timesofindia.indiatimes.com/india/Govt-to-block-websites-selling-drugs-guns-and-child-porn/articleshow/50872246.cms (last visited Mar. 27, 2023).
[10] Shashank Bengali, "The 'dark web' is where criminals go to be anonymous. It's where all your data will end up," Los Angeles Times, May 14, 2017, https://www.latimes.com/world/mexico-americas/la-fg-global-dark-web-20170514-story.html (last visited Mar. 27, 2023).
[11] Hindustan Times, "6 arms syndicates busted, 6 militants arrested," September 6, 2018, https://www.hindustantimes.com/india-news/ (last accessed April 3, 2023).
[12] Dhanya Thoppil, "Dark web black market trade in India rises," Livemint, February 26, 2019, https://www.livemint.com/Industry/kkaMgI0xzlnR0iJ89ybl7O/Dark-web-black-market-trade-in-India-rises.html
[13] *Ibid.*

ISSN: 2582-6433

accountable for cybercrimes, which are currently under trial at a lower conviction rate.[14]

Moreover, the lack of international cooperation and coordination makes regulating the dark web more complicated. Cybercriminals operate across multiple jurisdictions, making it challenging to track them down and bring them to justice. Therefore, cooperation between Indian law enforcement agencies and their foreign counterparts is essential to improve the regulatory measures on dark web in India.[15]

In conclusion, regulating the dark web in India poses several legal challenges. The anonymous nature of the users, countermeasures deployed by cybercriminals, and limitations faced by law enforcement agencies make it a daunting task. Successful and unsuccessful attempts at regulation are a testimony of these challenges.[16] To tackle the regulatory issues, law enforcement agencies need to work closely, be more aware and trained, have better equipping, and have international cooperation to address the dark side of the web effectively.

ROLE OF TECHNOLOGY IN CRIMINAL ACTIVITIES ON THE DARK WEB

The dark web, a part of the Deep Web, is a network of websites that are not indexed by search engines and are primarily used for criminal activities such as drug trafficking, money laundering, human trafficking. The anonymity and encryption provided by the dark web makes it a breeding ground for such criminal activities which are facilitated by the use of cutting-edge technology. The role of technology in criminal activities on the dark web has become a critical concern for law enforcement agencies and policymakers across the globe.

The technology used by dark web users and vendors is highly sophisticated and complex. They use a range of advanced software and hardware to protect their identity and to carry out their activities undetected. Some of the technologies commonly used on the dark web include

[14] Indian Kanoon, "Section 43 (Punishment and Compensation for damage to computer, computer system, etc.,)", https://indiankanoon.org/doc/1474729/ (last accessed April 3, 2023).
[15] Mukesh Chaudhary and Saumya Tyagi, "Regulating the Transnational Crime: A Study of Dark Web-based Drug Trafficking," Society and Economy 42, no. 2 (2020): 239–56.
[16] *Ibid.*

ISSN: 2582-6433

anonymizing software such as Tor, which enables users to access the dark web anonymously.[17] Other software such as I2P, Freenet, and Zero Net also offer anonymity to users and vendors.[18] To transact securely, dark web vendors use cryptocurrencies such as Bitcoin, Monero, and Zcash, which are difficult to trace and are thus ideal for illegal transactions.

The anonymity and encryption provided by the technologies used on the dark web facilitate various criminal activities. Dark web vendors use these technologies to sell illegal goods and services such as drugs, weapons, counterfeit goods, and stolen data. Buyers on the dark web further use these technologies to purchase illegal goods and services anonymously.[19] The encrypted communication channels, such as instant messaging and Email, allow for easy coordination among the criminals.[20] Cybercriminals use technologies such as botnets, ransomware, and phishing attacks to target individuals and organizations for financial gain. These cyber-attacks can cause significant economic losses and psychological distress.[21]

Enforcement agencies across the globe face significant challenges in regulating and enforcing laws against criminal activities on the dark web. One of the innovative technological solutions is the development of digital forensics tools that can be used to track and trace illegal activities on the dark web.[22] Law enforcement agencies can use sophisticated AI-based algorithms to identify patterns of criminal activity on the dark web.[23] Blockchain technology can also help to maintain an immutable record of transactions on the dark web and provide a trail of evidence for law enforcement.[24]

The use of technology has significantly increased the range and intensity of crimes on the dark

[17] J. Latif, "Demystifying Tor: A Beginner's Guide to the Deep Web/Darknet," Techopedia, March 2017, available at https://www.techopedia.com/demystifying-tor-a-beginners-guide-to-the-deep-webdarknet/2/33029 (last visited Jun. 20, 2021).
[18] R. Kumar, S. Gupta, and M. Tyagi, "Dark Web and its challenges in digital forensics," Computing, vol. 8, no. 2, pp. 104-111, Apr 2020.
[19] N. Christin, "Traveling the Silk Road: a measurement analysis of a large anonymous online marketplace," Proceedings of the 22nd international conference on World Wide Web, pp. 213-224, May 2013.
[20] S. Boyd, "Anonymous communication on the internet," University Press, Cambridge, UK, 2014.
[21] S. A. Mason and A. J. Monaghan, "Cybercrime and Its Victims," Taylor & Francis Group, London, 2011.
[22] K. B. Chidambaram, N. Edalat, A. H. Aghvami, "Digital forensics in the dark web: A survey," Computers & Security, vol. 96, pp. 101970, Oct 2020.
[23] C. Fang, X. Fan, X. Li, and K. Ren, "BLOTTER: A Hybrid AI System for Detecting Criminal Activity in the Darknet," IEEE Transactions on Dependable and Secure Computing, 2021, doi: 10.1109/TDSC.2021.3062313.
[24] A. Squicciarini, J. O. Kephart, M. C. Mascolo, "An Overview of Blockchain and Its Use for Cybersecurity," IEEE Security & Privacy, vol. 17, no. 1, pp. 27-34, Jan-Feb 2019.

ISSN: 2582-6433

web. As the technology used by the criminals is highly complex and sophisticated, there is a need for innovative technological solutions to aid in regulation and enforcement efforts. Law enforcement agencies need to work together with tech firms to develop and implement innovative solutions to tackle the challenges posed by the dark web.

NEED FOR A COMPREHENSIVE LEGAL FRAMEWORK

In recent times, the growth of the internet and its usage has led to the emergence of the dark web, which is a part of the internet not easily accessible to the general public. The dark web has become infamous due to its use in illegal activities such as drug trafficking, human trafficking, terrorism, and other heinous crimes. Despite the fact that the Indian government has enacted several laws to regulate the internet, there are still challenges in regulating the dark web. It is therefore important to analyse the growing need for a comprehensive legal framework for regulating the dark web in India.

(1) Arguments for a Comprehensive Legal Framework:

The dark web poses unique legal challenges that require a comprehensive legal framework. Some of the arguments for such a legal framework include:

a) ***Enforcement challenges:*** The dark web is challenging to monitor and regulate due to its anonymity and encryption features.[25] A comprehensive legal framework would provide law enforcement agencies with the necessary tools and resources to detect, investigate and prosecute offenders on the dark web.

b) ***Regulatory clarity:*** There is a need for clarity on the responsibilities of intermediaries in the dark web ecosystem. A comprehensive legal framework should define the liability of intermediaries and ensure that they cooperate with law enforcement agencies to identify criminal activities on their platforms.[26]

c) ***Human Rights:*** Any legal framework regulating the dark web must adhere to established human rights principles. The right to free speech, freedom of expression, and access to

[25] Ritu Vats, "Regulating the Dark Web – Legal Challenges and Way Forward," Indian Journal of Science and Technology, vol. 9, no. 28 (2016): 1-3.
[26] United Nations Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20 (2016).

ISSN: 2582-6433

information must be protected.[27] This legal framework must ensure that these rights are balanced with the need to combat illegal activities on the dark web.

(2) Aspects to Consider in a Comprehensive Legal Framework:

A comprehensive legal framework must address several aspects, including:

a) ***Amendments of existing laws:*** Existing laws must be amended to ensure that they cover activities on the dark web. This amendment must be done in a way that is consistent with the Constitution of India and in compliance with established international human rights principles.[28]

b) ***Collaboration:*** There is a need for collaboration between the government, law enforcement agencies, other stakeholders and the general public in developing a comprehensive legal framework. This framework should be regularly reviewed, evaluated and updated to ensure that it remains relevant.[29]

c) ***International cooperation:*** A comprehensive legal framework must promote international cooperation in combating the crimes committed on the dark web. This cooperation could involve the sharing of information and intelligence, training, and the establishment of international standards.

(3) Comparison to Other Countries' Legal Frameworks:

Several countries have enacted legal frameworks to regulate the dark web, including the United States, Europe, and Australia. In the United States, the Tor browser, which is commonly used to access the dark web, is legal. However, the use of the browser for illegal purposes is illegal. In Europe, the General Data Protection Regulation (GDPR) governs how personal data is handled on the internet, including the dark web.[30] In Australia, the Federal Police is responsible for investigating crimes on the dark web. [31]

In conclusion, the growth of the dark web has led to the emergence of new legal challenges that must be addressed with a comprehensive legal framework. This legal framework must protect

[27] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors., (2017) 10 SCC 1.
[28] Internet Democracy Project, National Consultation on Regulation of the Dark Web in India (2019).
[29] Security Gladiators, "Is Tor Legal or Illegal? Complete Guide on Tor Browser Legality" https://securitygladiators.com/is-tor-legal-illegal-complete-guide-tor-browser-legality/ (last accessed April 3, 2023).
[30] EUR-Lex, "General Data Protection Regulation," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 (last accessed April 3, 2023).
[31] Australian Federal Police, "Darknet and Cryptocurrency Investigations", https://www.afp.gov.au/what-we-do/crime-types/cyber-crime/darknet-and-cryptocurrency-investigations (last accessed April 3, 2023).

ISSN: 2582-6433

personal privacy, balance human rights and national security interests, and provide regulatory clarity. Collaboration, International cooperation and the amendment of existing laws are essential factors to be considered. If implemented correctly, this legal framework will aid law enforcement agencies in combating crimes on the dark web while upholding fundamental human rights.

CONCLUSION & SUGGESTIONS

In conclusion, the Dark Web poses a significant challenge to regulators and law enforcement agencies as it allows for anonymous and unregulated communication and exchange of illegal goods and services.[32] The lack of jurisdiction and anonymity associated with it has also contributed to the proliferation of cybercrimes and facilitated terrorist activities.[33] Despite specific legal provisions in place to regulate the same, including the Information Technology Act, 2000, and the Indian Penal Code, there are many challenges in implementing a regulatory and legal framework that can effectively control and deter the use of the Dark Web.[34]

One of the significant reasons for the challenge is the technical intricacies involved in regulating the Dark Web, including the use of encryption to mask communications and transactions on the platform.[35] Moreover, the fact that the servers associated with it may be located in different countries and the lack of an authoritative body to govern the same makes it challenging to regulate it.[36]

Additionally, the anonymity provided by the Dark Web has made it a haven for cybercriminals, including hackers and ransomware perpetrators. The use of digital currencies such as bitcoin also makes it difficult to track monetary transactions and thereby presents challenges in effectively regulating the platform.[37]

[32] Rahul Chaturvedi, "What is the Dark Web and Why Should You Care?" (2019), Techopedia, https://www.techopedia.com/2/33186/internet/web-browsers/what-is-the-dark-web-and-why-should-you-care (last accessed April 3, 2023).
[33] SentinelOne, "The Dark Web: How Cybercriminals Operate in the Web's Wild West," (2019), https://www.sentinelone.com/blog/the-dark-web-how-cybercriminals-operate-in-the-webs-wild-west (last accessed April 3, 2023).
[34] Information Technology Act, 2000, sec. 69A; Indian Penal Code, sec. 503.
[35] Vanessa Smith, "The Dark Web: What is it and How to Access It," (2021), Comparitech, https://www.comparitech.com/blog/vpn-privacy/the-dark-web-what-is-it-and-how-to-access-it (last accessed April 3, 2023).
[36] Supra note 33.
[37] Supra note 32.

ISSN: 2582-6433

To counter the challenges of regulating the Dark Web, there is a need for better coordination between different enforcement agencies and the development of an international understanding among different countries.[38] Strengthening the legal and regulatory framework to effectively address the challenges involved in regulating the online platform is also necessary in making an effective crackdown on the same.[39] The role of proactive measures such as surveillance, the deployment of advanced cybersecurity tools, and police training to detect and prevent illegal activities on the platform also needs to be emphasized.

In addition to the measures mentioned above, there is also a need to build awareness among netizens on the dangers of Dark Web and the importance of safe and responsible use of the internet. Education and sensitization initiatives to help people understand the risks associated with the Dark Web and to encourage a culture of internet safety would go a long way towards preventing the misuse of the platform.[40]

Thus, regulating the Dark Web poses significant challenges in India, but it is also essential for national security and the well-being of the community. With awareness, coordinated efforts, and a strong legal and regulatory framework, it is possible to regulate the platform effectively.

REFERENCES

(1) Chowdhury, Soumya Sundar. "Crime on the Dark Web: An Investigation into the Use of Bitcoin for Illegal Activities." Journal of Financial Crime 27, no. 1 (2020): 218-234.

(2) Andhavarapu, T. R. "Cyber Crimes on Deep Web in India." International Journal of Research and Analytical Reviews 6, no. 3 (2019): 443-452.

(3) Information Technology Act, 2000. Available at https://meity.gov.in/writereaddata/files/it_act2000.pdf.

[38] Ravi Mandalia, "Managing the Dark Web: Indian Government Sets up Centre for Information Security Supervision," (2019), AlphaStreet, https://news.alphastreet.com/managing-the-dark-web-indian-government-sets-up-centre-for-information-security-supervision (last accessed April 3, 2023).
[39] Supra note 34.
[40] Gov.uk, "Internet safety for children and young people," (2020), https://www.gov.uk/government/publications/internet-safety/internet-safety-for-children-and-young-people (last accessed April 3, 2023).

ISSN: 2582-6433

(4) Indian Penal Code, 1860. Available at https://www.indiacode.nic.in/bitstream/123456789/12401/1/THE-INDIAN-PENAL-CODE-1860.pdf.

(5) Computer Fraud and Abuse Act, 18 U.S.C. § 1030 – Fraud and Related Activity in Connection with Computers. Available at https://www.justice.gov/criminal-fraud/computer-crime-and-intellectual-property-section/computer-fraud-and-abuse-act.

(6) Canada's Criminal Code, Sections 342.1 to 342.4, 430(1.1), 467.1 and 487.016. Available at https://laws-lois.justice.gc.ca/eng/acts/c-46/page-73.html.

(7) UK Investigatory Powers Act 2016. Available at https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

(8) Australia's Criminal Code Amendment (Misuse of Digital Devices) Act 2013. Available at https://www.legislation.gov.au/Details/C2013A00152.

(9) The Telegraph. "What is the dark web, and how does it work?" September 29, 2020. https://www.telegraph.co.uk/technology/0/dark-web-work/.

(10) PTI. "Govt to block websites selling drugs, guns and child porn." Times of India, February 8, 2016. https://timesofindia.indiatimes.com/india/Govt-to-block-websites-selling-drugs-guns-and-child-porn/articleshow/50872246.cms.

(11) Bengali, Shashank. "The 'dark web' is where criminals go to be anonymous. It's where all your data will end up." Los Angeles Times, May 14, 2017. https://www.latimes.com/world/mexico-americas/la-fg-global-dark-web-20170514-story.html.

(12) Hindustan Times. "6 arms syndicates busted, 6 militants arrested." September 6, 2018. https://www.hindustantimes.com/india-news/6-arms-syndicates-busted-6-militants-arrested/story-1xRsLatuidFyBEkTiJdPnM.html.

(13) Thoppil, Dhanya. "Dark web black market trade in India rises." Livemint, February 26, 2019. https://www.livemint.com/Industry/kkaMgI0xzlnR0iJ89ybl7O/Dark-web-black-market-trade-in.