DARK WEB AS RABBIT HOLE OF CRIMES AND A LOOPHOLE IN CYBER SECURITY IN INDIA

Ms. Usha S, B.A., LL.B., Chennai Dr. Ambedkar Government Law College,
Pudupakkam, Chengalpattu (Dt.), Tamil Nadu

ABSTRACT

Internet has now entangled with the human life. Every person depends upon internet for one use or another; as of 2024 about 68% of the world's population engaged in internet usage. The internet i.e., the World Wide Web (www) contains a hierarchy starting from the most commonly used surface web. The hidden point of the ice berg is the Dark Web: dark web deviates from the traditional usage as it requires full knowledge about its decryption and special search engines with VPN. Both the pros and cons of Dark Web arise from its anonymity.

This paper studies about the Dark Web through legal lens and legal intricacies associated with the usage of Dark Web. The usage of Dark Web is not illegal in India as there is no provision prohibiting the same. But, if the activities and the purpose for which it is used are illegal then there will be legal consequences. These illegal activities are hard to identify and trace because of the usage of VPN as India possess several free VPN providers.

The study apart from the privacy view also focused on the implication of consumer laws and cyber protection laws in India. The Author has used secondary research methodology for the findings. The research objective is to know the evolving types of cybercrimes in dark web, integration of consumer laws and the cyber security practices undertaken by the government for reducing the incidents of cyber-crimes. Towards the end, the paper aims to provide valuable suggestions for combating cyber-crimes in Dark Web through global collaborative practices, confining openly available VPNs, enacting provisions for regulating the usage of Dark Web and educating the users regarding the safe use of Dark Web to avoid being the target of cyber-criminals.

Keywords: Dark web, Privacy, Consumer law, Cyber security, Suggestions.

I. INTRODUCTION:

Internet has been becoming an inseparable part of human life. As per the world statistics, about 68% of the world population is engaged in usage of internet[1]. With these assembled multitude, people often need a hidden part of layer to ensure their privacy. The internet may be classified into three layers namely surface web, deep web and dark web[2]. Dark Web is known for its anonymity being provided to its users. However, with the providence of great anonymity there are wide range of crimes which are happening in dark that poises danger to cyber security and data protection. The paper is focused on the emergence of Dark Web into publicly accessible part of internet; crime associated with Dark Web and the challenges being faced in regulation of Dark Web in India. With these, the author has also made effort in providing valuable suggestions for combating the crimes and for cyber governance of Dark Web usage in India. Intersectional role of different Acts in interpretation of Crime has been given special consideration in the occurrence of Dark Web.

1.1. RESEARCH OBJECTIVES:

The paper focused on the Dark Web and the legal intricacies with the following objectives:

- To provide the information regarding the emergence of Dark Web and their evolution in becoming openly accessible layer.
- To know about the crimes happening in dark web and the efforts made to mitigate the same.
- To give an understanding about the legal intricacies of Dark Web governance and regulation.

1.2. RESEARCH METHODOLOGY:

The present work is an analytical study for which the author has relied upon secondary sources of research. The secondary sources of methodology include the published articles, journals and statistics. The study analyzed the technicalities, statutes and real time cases for the findings.

[1] World Bank Group, Individuals using the Internet, worldbank.org (July. 27, 2025, 15:00 PM) https://data.worldbank.org/indicator/IT.NET.USER.ZS.
[2] Kaur, S. & Randhawa, S. Dark Web: A Web of Crimes, 112 Wireless Pers Commun 2131, 2132 (2020), https://link.springer.com/article/10.1007/s11277-020-07143-2#citeas.

No primary sources have been used for the research. The author wholly relied upon secondary resources for the research.

1.3.LITERATURE REVIEW:

This literature review examines existing studies related to the legal intricacies involved in regulating the Dark Web. The exploration of this topic requires both the legally and technically sound knowledge. *Kaur S & Randhawa S (2020)* in their study dealt with the technical as well as the legal challenges in addressing the crimes occurring through Dark Web. *Rajamanickam D S & Zolkipli M S (2021)* explained the various dimensions of cybercrime and asserted that Dark Web serves as the gateway for cyber criminals.

It can be observed that IT Act, 2000 plays a pivotal role in the confrontation of cybercrimes. However, there is lack of new provisions for addressing the recently evolved technological crimes. In this regard, *Sneka E & Sowbarniga B (2024)* discussed the issue of gap between the modern cybercrimes and the traditional rigid laws, emphasizing the need for more flexible provisions to ensure effective cyber security in India.

Further literature highlights the conflict between fundamental rights – such as the right to privacy and the right to access the internet. However, limited scholarly attention has been given to the application of consumer laws to customers of the Dark Web. Therefore, the present study aims to examine this correlation, along with the issues relating to the violation of fundamental rights and legal intricacies in regulating the Dark Web.

II. EMERGENCE AND EVOLUTION OF DARK WEB:

The emergence of Dark Web is started through the browser named FreeNet in the 2000s which offered anonymity to its users while surfing on the internet. Though, it was emerged in 2000 the actual use came to view in the year 2002 when the U.S. Naval laboratory developed The Onion Routing System also known as “TOR” for the purpose of secret interaction between its forces[3].

The usage of Dark Web requires specialized browsers, encryption technique, Virtual Private

[3] Rajamanickam, D. S. & Zolkipli, M. F., Review on Dark Web and its Impact on Internet, 8 JICTIE 13, 14 (2021), https://doi.org/10.37134/jictie.vol8.2.2.2021.

Network (VPN) and routing algorithm[4]. Today, there are a number of browsers or networks that allow access to Dark Web: TOR browser, FreeNet, Whonix, 12P (Invisible Internet Project), TAILS (The Amnesic Incognito Live System) and Sub graph OS[5].

The users of Dark Web use Cryptocurrency particularly Bitcoin for the transaction that adds strength to the anonymity. The network that is developed for legal purpose of providing privacy however, resulted as a platform for conducting criminal activities like drug trafficking, data theft, child pornography etc., some of the marketplace that involved in these are Silk Road, Agora and other such. Silk Road and Agora was taken down through lawful means.

2.1. THE SILK ROAD TAKE DOWN:

Silk Road was a black market on the dark web that was created at 2011 by Ross Ulbricht as the maker of Dread Pirate Roberts.[6] Silk Road functioned as a platform for illegal drug transaction using the TOR network, where the buying and selling is done through Bitcoins and Cryptocurrencies. The FBI then with the help of other investigators found the email account of Ulbricht and traced him. In October 1, 2013, his laptop was taken away and he was given a life term sentence in 2015 by the judge.

Between these on 2013, Silk Road 2.0 was made by other such administers of the online market place which was also taken down by the U.S. Government. The Silk Road made about $13 million dollars' worth Bitcoin in the commission alone[7]. On January 21, 2025 President Trump granted a pardon to Ross Ulbricht[8].

2.2.THE BUDAPEST CONVENTION:

The Budapest Convention or the first Convention on Cyber Crime conducted on 2001, focused on addressing the growing threat of cybercrime at international level and called for collaboration between the parties of Convention. Convention categorized the cybercrimes into

[4] Kaur, S. & Randhawa, S. Dark Web: A Web of Crimes, 112 Wireless Pers Commun 2131-2158, 2137-2139 (2020), https://link.springer.com/article/10.1007/s11277-020-07143-2#citeas.
[5] *Ibid.*
[6] Federal Bureau of Investigation, Ross William Ulbricht's Laptop, fbi.gov (July. 27, 2025, 15:21 PM) https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop.
[7] *Ibid.*
[8] David Yaffe-Bellany, Ryan Mac, Trump Pardons Creator of Silk Road Drug Marketplace, doggett.house.gov (Jan. 21, 2025, 15:26 PM) https://doggett.house.gov/media/in-the-news/trump-pardons-creator-silk-road-drug-marketplace.

the following: Crimes against the confidentiality of data, integrity of data, and availability of data; computer-related crimes; content-related crimes and infringements of intellectual property rights.[9] Besides this, it also challenged the admissibility of electronic evidence in the courts of law. This became the first Convention to unite the countries in the bid to promote cyber security and information protection.

The Convention deals with such offences like child pornography and other crimes that are taking place as a matter of normalcy in the Dark Web. So, the agreement and the control of Dark Web are in strong relation with each other. It should be noted that India does not become the part of the Budapest Convention.

III. DARK WEB – AS A RABBIT HOLE:

Most of the people accessed the Dark Web information because of curiosity. The Dark Web is the market place of many illegal activities as a rabbit hole. Viewing Dark Web does not pose offense in India because there is no law provision against the use of same. Even the utilization of VPN also is not limited. However, Indian Computer Emergency Response Team (CERT-In) required VPN service providers to archive user information of users during 5 years period and even to pass the information at demand[10], it's effectiveness in the Dark Web governance is questionable.

3.1. CRIMES AND DARK WEB:

Cyber Crime is no less than a real-life crime. It is only the mode of the crime that changes but not the intention and the motive behind such actions. They have the similar outcomes of causing hardships to others whether in the form of emotional struggle, physical harm or financial attacks.

1. *Drugs and Narcotics Trafficking:*

Illegal Drug trafficking is a menace not only to the internal purview but also cross border transfers are being reported involving exchange of the drugs using the cryptocurrencies. India

[9] Sneka E & Sowbarniga B, Cyber Law and the Dark Web: Regulating Hidden Markets, 1 JLLRD 17, 22 (2024), https://www.jllrd.com/index.php/journal/article/view/28#:~:text=Ultimately%2C%20this%20paper%20advocates%20for,youth%20engagement%20in%20these%20illicit.

[10] Sunainaa Chadha, Explained: What the new VPN rules means for internet users in India, Times of India, May. 12, 2022(July. 27, 2025, 15:43 PM), https://timesofindia.indiatimes.com/business/india-business/explained-what-the-new-vpn-rules-means-for-internet-users-in-india/articleshow/91510719.cms.

Narcotics Control Bureau (NBC) has booked approximately 92 cases under Dark net and Crypto-currencies amidst the years of 2020-2024 (till Apr.) whereas 1025 cases under parcel/couriers have been reported by the entire Drug Law EnforcementAgencies.[11].

2. *Human Trafficking and Assassinations:*

Black Death is one of the places on Dark Web where the human trafficking takes place[12]. Trafficking is majorly perpetrated through labour exploitation, through sexual exploitation and organs trafficking. According to the National Crime Records Bureau (NCRB) Crime Report of 2021, it has come to light that approximately 2,883 cases are reported in the context of cyber-extortion.[13]. Apart form that, there are certain websites in Dark Web that provide assassination services for monetary gain.

3. *Child Pornography and Revenge Porn:*

Child pornography is a serious offence in India. Seeing, accessing, storing and transferring of child pornography is strictly prohibited[14]. Child pornography as a new commercial product on pay-per view basis is promoted by Dark Web. Approximately 7.5 per cent of Child sexual abuse Material (CSAM) are profitably traded [15]. In addition to these, there is also presence of revenge porn of women and coercion of minor girls is also found in Dark Web.

4. *Information Leakage:*

Information leakage in Dark Web includes not only those of individuals but also of big corporates who possess sensitive information of their customers. Among these information leaks in India was that of boAt info leakage in 2024 where the personal information of approximately 7.5 million customers got leaked on Dark Web by an Indian hacker going by the name ShopifyGUY [16].

[11] Press Information Bureau, Drug Trafficking in the Country, pib.gov.in, July, 24, 2024, 5:06 PM (July. 27, 2025, 15:44 PM) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2036398.
[12] Kaur, S. & Randhawa, S. Dark Web: A Web of Crimes, 112 Wireless Pers Commun 2131, 2140 (2020), https://link.springer.com/article/10.1007/s11277-020-07143-2#citeas.
[13] National Crime Records Bureau, Annual Report-2021 (July, 2, 2025, 15:57 PM) https://data.gov.in/.
[14] The Protection of Children from Sexual Offences (POCSO) Act, 2012, § 14, 15.
[15] Roberta Liggett O'Malley, Commercial Child Sexual Abuse Markets on the Dark Web, CINA Jun., 2018, 1, https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Liggett_Commercial_Child_Sexual_Abuse_Markets_Dark_Web.pdf.
[16] Naandika Tripathi, Hit with massive data breach, boAt loses data of 7.5 million customers, Forbes India, Apr., 6, 2024, 7:09PM, (July, 27, 2025, 17:07 PM) https://www.forbesindia.com/article/news/hit-with-massive-data-

5. *Arms Trafficking:*

Arms smuggling in Dark Web is an international menace. It creates terrorism inside the country. Europe is the biggest consumers of arms trade in the dark web, common consigned arms – traces to dark web arms-trade include the most widely arms in Dark web_Remarks: pistols, (84%), Rifles (10%), and Sub-machine guns (6%)[17].

6. *Malware Distribution:*

The Cyber-criminals in Dark Web also provide the service of malware distribution in exchange of monetary benefit. The most prominent ransomware group in India was LockBit 3.0 that caused 61.8 percent of all the attacks in the country followed by KillSec and Stormous [18].

3.2. THE DIPU SINGH CASE:

The first ever Dark Web drug trafficking case that has been caught by the Narcotics Control Bureau (NCB) was the Dipu Singh case in the year 2020. Dipu Singh was a Hotel Management student studying in Amity University, Lucknow; aged 21 that undertook illegal selling of drugs and other narcotics especially sex stimulative drugs which have been couriered in various countries especially US and UK. Under NDPS Act, he was arrested[19] and the raids revealed about 12,000 tablets of various psychotropic tablets at his residence and 55,000 tablets including *tramadol, zolpidem* and *alprazolam* have been seized in total[20]. Through the investigation, it has been found that Dipu Singh used TOR network for accessing Dark Web and engaged in Cryptocurrency (Bitcoins and Litecoin) transactions for maintaining the anonymity.

IV. INTERSECTION OF CONSUMER LAW AND DARK WEB REGULATION:

Law is the unavoidable tool in the enforcement of controlling measures of Dark Web.

breach-boat-loses-data-of-75-million-customers/92483/1.

[17] Alex Belomlinsky, International arms trade in the dark web, rand.org, 3 (July, 27, 2025, 17:10 PM) https://www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html.

[18] SOCRadar, India Threat Landscape Report, 2024, socradar.io (July, 27, 2025, 17:12PM) https://socradar.io/wp-content/uploads/2024/12/SOCRadar-India-Threat-Landscape-Report.pdf.

[19] The Narcotic Drugs and Psychotropic Substances Act, 1985, § 8.

[20] Staff Reporter, India's first 'darknet' narcotics operative held, The Hindu, Feb., 10, 2020, 11:50 AM, (July, 27, 2025, 17:21 PM) https://www.thehindu.com/news/cities/Delhi/countrys-first-darknet-narcotics-operative-held/article30778534.ece.

Nevertheless, there is no act that governs the Dark Web specifically, and the offenses related to the Dark Web are therefore banned in piecemeal legislation.

4.1. CONSUMERS OF DARK WEB:

As mentioned before, accessing Dark Web is not itself a crime. There are also some legal buying and selling transactions that happens in Dark Web which is not prohibited. The research area is whether such transactions and the customers of such website can be taken into account as a "consumer" as defined in the Consumer Protection Act, 2019[21].

There are customers of Dark Web who engage in reading of books, sharing of information and often used by whistleblowers, journalists and even government officials in sharing of confidential information as well as acquiring of sensitive matters.

The CPA included persons who engage in e-commerce[22] to be come under the term consumer. Nevertheless, no definitive information is available on the enactment of consumer laws against the customers and the electronic service providers on the Dark Web. The challenge is that the E-service providers are anonymous.

However, when the definition of the wording given in the Act is interpreted, they will include the use of Dark Web, and the consumers of the same shall be covered under the CPA. This is because the Dark Web is not legally defined as illegal in India and the second reason is the definition of consumers and electronic service providers that in a literal sense will repeat both of them. Nevertheless, it still lies in the hand of both Government and the Judiciary to interpret the coverage of this problem and to remove this ambiguity.

4.2. INFORMATION TECHNOLOGY ACT, 2000:

The Information Technology Act, 2000 forms a defining piece of legislation in punishing the cyber crimes committed in Dark Web.

Section 43 – This section defines the damage caused to the computer resource such as virus, stealing of information and such acts.

[21] The Consumer Protection Act, 2019, § 2(7).
[22] The Consumer Protection Act, 2019, § 2(16).

Section 65 -This section prohibits tampering with the computer source documents and it holds that it is now punishable by imprisonment up to 3 years or a fine up to 2 lakh rupees or both.

Section 66C- A person steals other persons identity; this creator will be punished with 3 years imprisonment along with a fine of up to 1 lakh rupees.

Section 66D- It allows punishment in punishing personation by which computer resources were involved and could be punished in terms of imprisonment up to 3 years and fine 1 lakh rupees.

Section 66E - It accords penalty in case of illegal access to the privacy of other person with the help of computer resource.

Section 66F - In this section, the attempt and dissemination of information to establish cyber-terrorism has been banned.

Section 67- The section prohibits transfer of obscene material in the electronic format which includes the child pornography. [23]

4.3. PROTECTION OF CHILDREN FROM SEXUAL OFFENCES (POCSO) ACT, 2012:

The POCSO Act takes stringent actions against the child harassment with distinct provisions against the different sexually oriented offences in mind targeting the children. It specifically makes child pornography illegal as well as the possession of child porn is punishable under this law[24].

4.4. BHARATIYA NYAYA SANHITA, 2023:

The Bharatiya Nyaya Sanhita, 2023 is the current law for India of the penal code. As discussed above if it is against any law then the acts done in the Dark Web will be punished. In the same manner, BNS prohibits sexual harassment, revenge porn, sharing obscene materials of women as well as children, kidnapping, cyber-terrorism, murder, cheating and cyber-stalking[25].

[23] The Information Technology Act, 2000, § 43, 65,66C, 66D, 66E, 66F.
[24] The Protection of Children from Sexual Offences (POCSO) Act, 2012, § 14, 15.
[25] Bharatiya Nyaya Sanhita, 2023, § 75, 77, 78, 87, 152, 292, 103, 318.

4.5. NARCOTIC DRUGS AND PSYCHOTROPIC SUBSTANCES ACT, 1985:

The most prevalent crime in Dark Web itself is Drug Trafficking as even the first instance of the Darknet crime exposure of India is based on Drug Trafficking (i.e., the Dipu Singh case). According to this Act, it is illegal to produce, sell and even possess drugs[26]. The Government often engage in operation for curbing the illegal selling of drugs in Dark Web.

4.6. ARMS ACT, 1959:

The Arms Act regulates the manufacturing, possession, trade and usage of arms and ammunition. The Act comes into the picture when there is Arms Trafficking in Dark Web. The Act prohibits the illegal manufacturing, sale and use of arms without permission from the necessary Government officials.

4.7. PREVENTION OF MONEY LAUNDERING ACT (PMLA), 2002:

The focus is not only curbing the crime and seizing the illegal materials from the Cyber-criminals of Dark Web but also the illegal earning generated through the crimes committed by them in the Dark Web marketplace. Most of the money involved in Dark Web are Cryptocurrencies. Thus, the illegal earning generated by them are seized by the Enforcement Department (ED).

4.8. DIGITAL PERSONAL DATA PROTECTION ACT (DPDP), 2023:

DPDP Act is more of new law concerned with the regulation of Data of customers handled by the industries. The Act calls for a comprehensive data security measures and obtaining the valid consent through electronic means. By the implementation of robust protective measures, the industries can eliminate the threat of data breach and identity theft by the Dark Web hackers.

V. DARK WEB IN CONNECTION WITH FUNDAMENTAL RIGHTS:

Between the Dark Web and the statutes in the parliament, there is a connotation not only circumlinked with the statutes shielded by the parliament but also, there is an association with the Constitution of India. There are Fundamental Rights of the people that cannot be breached but reasonable restriction may be affected during necessities. Dark Web relates to certain basic

[26] The Narcotic Drugs and Psychotropic Substances Act, 1985, § 8.

rights of the people and as such, it poses as a challenge to the Government that has minimal authority in regulation.

5.1. RIGHT TO PRIVACY:

Right to Privacy is one among the basic rights that uphold the independence of the population in India. The Right to Privacy is perceived as a momentous part of the Right to Life covered under Article 21[27] of the Constitution. Right to Privacy and Dark Web are closely interconnected. This right includes free from government surveillance and also the Dark Web. As there are also legal conversations and transactions that happen in the Dark Web; the individual has the full right to keep it private thus, falling under the ambit of Article 21.

Apart from that view, there are also people who engage in transmission of sensitive information in the Dark Web. These sensitive information holds the dignity of the person and the Right to Life also includes the Right to Dignity.

But what happens when the one transmitting and relaying the personal information is this Cyber-criminal? Then there is degradation of Privacy Rights to such individual whose information has thus been leaked to Dark Web. In such a way, Dark Web also has benefits and drawbacks.

5.2. JUSTICE K.S. PUTTASWAMY CASE:

The case law that dealt with the Right to Privacy is Justice K.S. Puttaswamy vs. Union of India delivered by the Honourable Supreme Court of India.[28] in which the court decided that, the right to privacy is a significant characteristic of the Right to Life. The court interpreted right to privacy into being the right of human being. Thereby, this right can't be violated for state welfare. As all rights are not absolute; there can be imposement of reasonable restriction on this right only in the matter of legitimate aims such as national security and after taking the test of proportionality.

5.3. RIGHT TO FREEDOM OF SPEECH AND EXPRESSION:

Article 19(1) (a) of the Indian Constitution gives the Right to Freedom of speech and

[27] India Const. art. 21.
[28] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

expression.[29]. This means people can express their criticism, thoughts, feelings, opinions and views on any issue through any medium[30]. Therefore, individuals sharing their views in the Dark Web will also be deemed as their right to freedom of speech and expression.

Even whistleblowers, journalists and government officials engage in posting the information on Dark Web hiding behind its encryption technology in order to protect their privacy and thereby keeping the anonymity of their profile. Whistleblowers often face life threats when their identity been revealed. Thus, Dark Web is useful to them; one such platform is the SecureDrop.

5.4. RIGHT TO UNDERTAKE ANY TRADE AND PROFESSION:

Every person who is a citizen of India has the fundamental right to carry on any trade, profession or occupation that they desire under Article 19(1) (g)[31]. Now, the trade includes the trade that occurs through electronic means. By this, the trade conducted in the Dark Web is regarded as a legal one. However, if the product that are being traded are illegal then, it will have the legal consequences.

5.5. ANURADHA BHASIN CASE:

In another seminal case by the Hon'ble Supreme Court of India Anuradha Bhasin vs Union of India & Ors.[32] Underlining the fact that right to trade, profession and occupation and right to internet is a fundamental right that cannot be endangered in the name of the unnecessary causes, the court restated that it is the responsibility of the state to safeguard the same.

Further in the case of Manohar Lal Sharma vs. Union of India & Ors.[33] the apex court strictly pronounced that the state officials can't use state security for irregulated surveillance over the e-commercial platforms.

VI. THE AADHAAR BREACH:

In 2023, the Resecurity reported that approximately 815 million Indian citizens aadhaar and

[29] India Const. art. 19, cl. 1(a).
[30] Muskan Sharma & Pushkar Bhandarkar, Freedom of Speech and Expression on Internet: An Emerging Right, Vol. 3 Iss. 4 IJLMH 381, 382 (2020) https://www.ijlmh.com/wp-content/uploads/Freedom-of-Speech-and-Expression-on-Internet-An-Emerging-Right.pdf.
[31] India Const. art. 19, cl. 1(g).
[32] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
[33] Manohar Lal Sharma v. Union of India & Ors., AIR 2021 SC 5396 (2021) (India).

passport data was released on Dark Web by a threat actor named pwn0001; The threat actor was supposed to sell the data to interested parties who would part with the sum of 80,000 dollar[34]. The information which the threat actor got accessed included the name, gender, age, aadhaar number, address, contact numbers and other sensitive information. For which UIDAI recommended "masked Aadhaar" showing only last four digit of the Aadhaar number[35].

VII. SUGGESTIONS IN GOVERNANCE OF DARK WEB:

Addressing and combating the threats arising from Dark Web will be a challenging one. The main barrier is the anonymity and technical aspect. With addition to that, there is also fundamental rights that comes in between in banning of Dark Web. however, there can be certain measures that can be adopted in reducing the criminal activities happening in the Dark Web.

1. International Collaborations:

As discussed before, the cyber-criminal activities in Dark Web are not only a national problem but that of an international one. Therefore, it demands collaboration and cooperation from the countries that face high risk from these illegal transactions. There is a need for new conventions and treaties as the present Budapest Convention and IT Act, 2000 are lacking the provisions for the newly emerged cyber-crimes[36].

While tackling cyber crimes there is also jurisdictional issues that arise between the countries, in order to address that, international collaboration is essential.

An international collaborative attempt also occurred between India and an international organization, i.e. the Operation CyberShield involving the Indian cybersecurity bodies, FBI and Interpol against a transnational cybercriminal syndicate that had long involvement in Dark

[34] HUMINT, "PII Belonging To Indian Citizens, Including Their Aadhaar ISs, Offered For Sale On The Dark Web", resecurity.com, Oct., 31, 2023, 20:29 PM, (July, 27, 2025, 17:33 PM) https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web.

[35] Nabeel Ahmed, How the personal data of 815 million Indians got breached | Explained, The Hindu, Nov., 07, 2023, (July, 27, 2025, 17:41 PM) https://www.drishtiias.com/daily-updates/daily-news-analysis/massive-aadhaar-data-breach.

[36] Sneka E & Sowbarniga B, Cyber Law and the Dark Web: Regulating Hidden Markets, 1 JLLRD 17, 24 (2024), https://www.jllrd.com/index.php/journal/article/view/28#:~:text=Ultimately%2C%20this%20paper%20advocates%20for,youth%20engagement%20in%20these%20illicit.

Web activities[37].

2. Operations by the Government:

India should conduct more Dark Web operations, currently, most of the operations focuses on narcotic dealings. India as a mixed economy, has to find its way between being liberal or authoritarian. Countries like USA focuses on hybrid way whereas, China easily imposes censorship and bans on illicit activities. The imposition of a ban would not suit the Indian scenario because of fundamental rights.

3. Confinement of Virtual Private Networks (VPN):

Virtual Private Network (VPN) is one attribute of Dark Web accessing that hides the location of the person accessing it and also the person providing the service. India didn't impose outright ban on both Dark Web and VPN usage.

The countries like Iraq, Turkmenistan, China, Oman, Russia, U.A.E. and Belarus have completely prohibited or controls the usage of VPN services[38]. However, India regulates the VPN service providers through making it mandatory for them to store the data of users for 5 years term and also to provide the information to CERT-In (Computer Emergency Response Team of India) on request. But, its contribution in regulation of Dark Web is still plausible.

4. Awareness Creation:

The Dark Web is still being attempted to be regulated by the Government. That said, the citizens have a responsibility to know about the operation of Dark Web as well. The user just needs a single click during the Dark Web usage to avail himself of the hazard. Hence, the same users of the internet who claims that it is his basic right must also contribute in safe browsing Dark Web.

VIII. CONCLUSION:

The Government does not openly prohibit Dark Web per se because Dark Web is also a section

[37] Kaliraj, Unveiling the Indian Footprint in Dark Web Marketplace: A Deep Dive into Illicit Cyber Activities, digialert.com, Nov., 24, 2023, (July, 27, 2025 17:48 PM) https://digialert.com/index.php/resources/blog/blog/others/unveiling-the-indian-footprint-in-dark-web-marketplaces-a-deep-dive-into-illicit-cyber-activities.

[38] Norton, "Are VPNs legal or illegal?", in.norton.com, Aug., 08, 2018, (July, 27, 2025, 17:53 PM) https://in.norton.com/blog/privacy/are-vpns-legal.

of the internet much like Surface Web and Deep Web. The right to access the internet and the right of the citizens to privacy is a constitutional right by the people and the Government cannot interfere with it. It is the responsibility of the Government to provide the safe surfing of internet and national security. There must be working on both sides in governing Dark Web illicit activities.

Therefore, besides international cooperation and various recommendations, people should also avoid indulging in this type of internet use to commit crimes.

REFERENCES:

1. Alex Belomlinsky, International arms trade in the dark web, rand.org, 3 (July, 27, 2025, 17:10 PM) https://www.rand.org/randeurope/research/projects/2017/international-arms-trade-on-the-hidden-web.html.

2. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).

3. Bharatiya Nyaya Sanhita, 2023, § 75, 77, 78, 87, 152, 292, 103, 318.

4. David Yaffe-Bellany, Ryan Mac, Trump Pardons Creator of Silk Road Drug Marketplace, doggett.house.gov (Jan. 21, 2025, 15:26 PM) https://doggett.house.gov/media/in-the-news/trump-pardons-creator-silk-road-drug-marketplace.

5. Federal Bureau of Investigation, Ross William Ulbricht's Laptop, fbi.gov (July. 27, 2025, 15:21 PM) https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop.

6. HUMINT, "PII Belonging To Indian Citizens, Including Their Aadhaar ISs, Offered For Sale On The Dark Web", resecurity.com, Oct., 31, 2023, 20:29 PM, (July, 27, 2025, 17:33 PM) https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web.

7. India Const. art. 21, 19 1 (a), (g),.

8. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India).

9. Kaliraj, Unveiling the Indian Footprint in Dark Web Marketplace: A Deep Dive into Illicit Cyber Activities, digialert.com, Nov., 24, 2023, (July, 27, 2025 17:48 PM) https://digialert.com/index.php/resources/blog/blog/others/unveiling-the-indian-footprint-in-dark-web-marketplaces-a-deep-dive-into-illicit-cyber-activities.

10. Kaur, S. & Randhawa, S. Dark Web: A Web of Crimes, 112 Wireless Pers Commun 2131, 2132 (2020), https://link.springer.com/article/10.1007/s11277-020-07143-2#citeas.

11. Manohar Lal Sharma v. Union of India & Ors., AIR 2021 SC 5396 (2021) (India).

12. Muskan Sharma & Pushkar Bhandarkar, Freedom of Speech and Expression on Internet: An Emerging Right, Vol. 3 Iss. 4 IJLMH 381, 382 (2020)

https://www.ijlmh.com/wp-content/uploads/Freedom-of-Speech-and-Expression-on-Internet-An-Emerging-Right.pdf.

13. Naandika Tripathi, Hit with massive data breach, boAt loses data of 7.5 million customers, Forbes India, Apr., 6, 2024, 7:09PM, (July, 27, 2025, 17:07 PM) https://www.forbesindia.com/article/news/hit-with-massive-data-breach-boat-loses-data-of-75-million-customers/92483/1.

14. Nabeel Ahmed, How the personal data of 815 million Indians got breached | Explained, The Hindu, Nov., 07, 2023, (July, 27, 2025, 17:41 PM) https://www.drishtiias.com/daily-updates/daily-news-analysis/massive-aadhaar-data-breach.

15. National Crime Records Bureau, Annual Report-2021 (July, 2, 2025, 15:57 PM) https://data.gov.in/.

16. Norton, "Are VPNs legal or illegal?", in.norton.com, Aug., 08, 2018, (July, 27, 2025, 17:53 PM) https://in.norton.com/blog/privacy/are-vpns-legal.

17. Press Information Bureau, Drug Trafficking in the Country, pib.gov.in, July, 24, 2024, 5:06 PM (July. 27, 2025, 15:44 PM) https://www.pib.gov.in/PressReleasePage.aspx?PRID=2036398.

18. Rajamanickam, D. S. & Zolkipli, M. F., Review on Dark Web and its Impact on Internet, 8 JICTIE 13, 14 (2021), https://doi.org/10.37134/jictie.vol8.2.2.2021.

19. Roberta Liggett O'Malley, Commercial Child Sexual Abuse Markets on the Dark Web, CINA Jun., 2018, 1, https://cj.msu.edu/_assets/pdfs/cina/CINA-White_Papers-Liggett_Commercial_Child_Sexual_Abuse_Markets_Dark_Web.pdf.

20. Sneka E & Sowbarniga B, Cyber Law and the Dark Web: Regulating Hidden Markets, 1 JLLRD 17, 22 (2024), https://www.jllrd.com/index.php/journal/article/view/28#:~:text=Ultimately%2C%20this%20paper%20advocates%20for,youth%20engagement%20in%20these%20illicit.

21. SOCRadar, India Threat Landscape Report, 2024, socradar.io (July, 27, 2025, 17:12PM) https://socradar.io/wp-content/uploads/2024/12/SOCRadar-India-Threat-Landscape-Report.pdf.

22. Staff Reporter, India's first 'darknet' narcotics operative held, The Hindu, Feb., 10, 2020, 11:50 AM, (July, 27, 2025, 17:21 PM) https://www.thehindu.com/news/cities/Delhi/countrys-first-darknet-narcotics-operative-held/article30778534.ece.

23. Sunainaa Chadha, Explained: What the new VPN rules means for internet users in India, Times of India, May. 12, 2022(July. 27, 2025, 15:43 PM), https://timesofindia.indiatimes.com/business/india-business/explained-what-the-new-vpn-rules-means-for-internet-users-in-india/articleshow/91510719.cms.

24. The Consumer Protection Act, 2019, § 2(7), (16).

25. The Information Technology Act, 2000, § 43, 65,66C, 66D, 66E, 66F.

26. The Narcotic Drugs and Psychotropic Substances Act, 1985, § 8.

27. The Protection of Children from Sexual Offences (POCSO) Act, 2012, § 14, 15.

28. World Bank Group, Individuals using the Internet, worldbank.org (July. 27, 2025, 15:00 PM) https://data.worldbank.org/indicator/IT.NET.USER.ZS.