Journal of
Law and Legal Research Development
ISSN: 3048-5045

Cyber Law and The Dark Web: Regulating Hidden Markets

Sneka E[1] and Sowbarniga B[*]

[1] 5th year, BBA LLB(HONS.,), School of Law, SASTRA Deemed to be University, Thanjavur, India

Article History

Received: Sep-2024
Revised: Sep-2024
Accepted: Sep-2024
Published: Oct-2024

Keywords

Dark web
Silkroad case
Information Technology Act
Budapest Convention

Abstract

This research paper examines the intricate relationship between cyber law and the dark web, focusing on the challenges of regulating hidden markets that facilitate illicit activities. The dark web, characterized by its anonymity and accessibility, has become a hub for criminal enterprises such as drug trafficking, human trafficking, and the sale of illegal goods. In India, a significant portion of the youth population—one of the highest in the world—actively engages with social media, online businesses, and digital transactions, making them a major demographic among dark web users. This interaction poses unique challenges for the Indian economy and business landscape, as it intertwines legitimate online activity with illicit behavior. This study aims to explore the effectiveness of existing legal frameworks, particularly within the context of India's Information Technology Act while also considering international conventions like Budapest Convention. Through a thorough literature review and analysis of current case studies, the paper highlights the limitations and gaps in existing laws that hinder effective regulation of dark web markets. Ultimately, this paper advocates for comprehensive legal reforms and innovative regulatory strategies to better address the complexities of the dark web, ensuring the protection of public safety and the integrity of digital commerce, while mitigating the economic risks associated with youth engagement in these illicit activities.

Corresponding Author:
Sowbarniga B
5th year, BBA LLB(HONS.,), School of Law, SASTRA Deemed to be University, Thanjavur, India
sowbi1807@gmail.com

1. INTRODUCTION

The dark web, a clandestine part of the internet that operates beyond the reach of standard search engines, has increasingly become a focal point of concern for governments, law enforcement agencies, and cybersecurity experts worldwide. While it offers a haven for privacy advocates and whistleblowers, it is equally notorious for facilitating a wide range of illegal activities, including drug trafficking, arms sales, and human trafficking. As more individuals, particularly the youth, gain access to the dark web—often through their engagement with social media, online businesses, and digital transactions—the potential for exploitation and criminal enterprise expands, raising urgent questions about the effectiveness of existing legal frameworks. In India, the rapid advancement of digital infrastructure and increasing internet penetration has further complicated the landscape of cyber law. With one of the largest youth populations globally, Indian young people are significant users of digital platforms, making them vulnerable to the allure of the dark web. The Information Technology Act of 2000, provides a foundation for addressing cybercrime. Additional legislation, such as Bharatiya Nyaya Sanhita 2023, the Narcotics Drugs and Psychotropic Substances Act, 1985, the POCSO Act, 2012, the Unlawful Activities (Prevention) Act (UAPA), and The Prevention of Terrorism Act, 2002, regulates cybercrimes that occur within the dark web. However, these laws often fall short in dealing with the complexities associated with dark web markets. The anonymity afforded by the dark web challenges traditional law enforcement methods, making it difficult to track, prosecute, and deter illegal activities effectively. This paper aims to analyze the regulatory environment surrounding the dark web in both the Indian and international contexts. By examining the limitations of current legal frameworks and identifying specific challenges faced by law enforcement, the research seeks to highlight the urgent need for comprehensive reforms. Ultimately, this study advocates for innovative regulatory strategies and enhanced international cooperation to effectively combat the illicit activities thriving in hidden markets, ensuring the protection of public safety and the integrity of digital commerce, particularly in light of the significant impact on India’s youth and the broader economy.

1.1 Research Problem

The rising prevalence of cybercrimes on the dark web, coupled with significant youth involvement in key economic activities, poses a serious threat to India's economy, highlighting the need for effective regulatory measures.

1.2 Research Objectives

- To identify and analyze key gaps in both national and international legal frameworks that contributes to the proliferation of hidden markets on the dark web drastically affecting the growth of economy.
- To assess the initiatives taken by the Indian Government to address cybercrimes related to the dark web and evaluate their effectiveness in curbing such illegal activities.
- To propose a set of recommendations for a tailored legal framework that addresses the unique characteristics of the dark web in India.

1.3 Research Questions

The primary research problem revolves around the lack of an effective legal framework to regulate the illegal activities facilitated by the Dark Web. Traditional legal structures are often insufficient to handle crimes that take place in encrypted, anonymized environments where jurisdictional boundaries are blurred. The result is a thriving underground market with limited accountability and significant obstacles to law enforcement. This research addresses the following key issues:

a. How do hidden markets facilitate youth of India to contribute to the rise of cybercrimes dark web in India?
b. What is the economic impact of cybercrimes originating from the dark web on India's economy?
c. What are the current inadequacies in India's cyber law enforcement with respect to regulating the dark web?
d. What specific regulatory measures have the potential to mitigate the negative effects of cybercrimes on India's economic growth?

2. DARK WEB

The dark web is a part of the internet that is not indexed by traditional search engines and requires specific software, such as Tor, for access. Known for its high levels of anonymity, the dark web serves both legitimate and illicit purposes. While it offers a platform for whistleblowers and activists to communicate securely, it is more commonly associated with illegal activities, including drug trafficking, weapons sales, human trafficking, and the trade of stolen data. The structure of the dark web complicates regulatory and law enforcement efforts, as the anonymity it provides makes it difficult to identify and prosecute offenders. Existing legal frameworks, like the Information Technology Act in India, often struggle to keep pace with the evolving tactics used by cybercriminals. Furthermore, jurisdictional issues pose additional challenges, as crimes frequently cross international borders. The dark web also raises important ethical and societal questions about privacy and security. While it can protect individual freedoms, it can also facilitate harmful activities. Addressing the complexities of the dark web requires innovative regulatory strategies, enhanced international cooperation, and public education to balance the need for security with the protection of civil liberties.

2.1. *History of Dark Web*

Initially developed by the United States Department of Defense for anonymous communication, the dark web has evolved into a global platform for users seeking anonymity. It serves both legal and illegal activities. Utilizing a technology called "onion routing," the dark web shields users from surveillance and tracking by directing their data through a series of encrypted servers. When users access a site via Tor, their information is passed through thousands of relay points, obscuring their online activity and making it nearly impossible to trace. ARPANET, or the Advanced Research Projects Agency Network, was an experimental computer network developed in the 1960s that laid the groundwork for the Internet and eventually the dark web. It was designed to facilitate information sharing over long distances without relying on traditional phone connections. Initially aimed at academic use, it quickly gained military interest during the Cold War due to its decentralized structure, which protected against potential attacks that could disable a central hub. Funded by the U.S. Defense Department, ARPANET allowed researchers significant freedom to conduct experiments, including the first known illegal online transaction-a marijuana sale between Stanford and MIT students in the early 1970s. In 1983, ARPANET split into two networks: MILNET for military use and a civilian version that would evolve into the Internet. This evolution was paralleled by the rise of "data havens" in the 1980s, which allowed the storage of data in jurisdictions with lenient laws, reflecting growing concerns about online privacy that would later resonate with dark web users. ARPANET was a pioneering network that not only facilitated early internet communication but also introduced concepts of secure and anonymous exchanges, setting the stage for both the Internet and the dark web. Its evolution mirrored the rise of data havens, highlighting an increasing concern for privacy in the digital age. Ian Clarke, a University of Edinburgh student, launched Freenet as his thesis project. His goal was to create a "Distributed Decentralised Information Storage and Retrieval System" that would facilitate anonymous communication and file sharing. This foundational work led to the development of the Tor Project, which was introduced in 2002 and launched a browser in 2008, allowing users to browse the internet entirely anonymously and access sites within the dark web[1]. One of the earliest dark web markets was Silk Road, which became notorious as a platform for trading illegal drugs. Before its

[1] *Kastner, E. (2020). History of the Dark Web [Timeline].* *https://www.soscanhelp.com/blog/history-of-the-dark- web*

closure, Silk Road attracted significant attention from government agencies, the media, and law enforcement, especially after the FBI arrested its operators in October 2013. Despite its shutdown, the dark web continues to be used by individuals worldwide to maintain anonymity while accessing weapons, confidential or illegal information, and illegal drugs, as well as engaging in other criminal activities such as human trafficking, child exploitation, and terrorism. Between 2011 and 2017, some of the largest dark web markets included Silk Road, Silk Road 2.0, Agora, Evolution, Nucleus, Abraxas, and AlphaBay. The dark web contains approximately 500 times more data than what is accessible to users on the surface web, with the surface web holding around 19 TB of information compared to an estimated 7,500 TB in the deep web. Notably, 95% of deep web content is accessible to the public without requiring payment or a subscription.

2.1.1. *Silk Road: A Dark Web Case*

Silk Road was the first modern dark web market and an online black market launched in 2011 by Ross Ulbricht, who operated under the alias "Dread Pirate Roberts." Functioning as a hidden service on the Tor network, Silk Road allowed users to buy and sell goods and services anonymously. All transactions were made using Bitcoin, a cryptocurrency that helped maintain user privacy. The site became particularly notorious for its illegal drug marketplace, alongside various other illegal and legal listings. From February 2011 to July 2013, Silk Road facilitated sales totaling 9,519,664 Bitcoins. The FBI, collaborating with federal and state agencies, began investigating Silk Road after a tax agent discovered a mention of the site on an online forum on January 27, 2011. Eight months later, the same agent noted a job posting by the same user, instructing interested applicants to email an account linked to Ulbricht.

By tracing various network records obtained through court warrants, investigators identified Ulbricht as a suspect. On October 1, 2013, his laptop was seized. The FBI shut down the Silk Road website and arrested Ulbricht. The following month, Silk Road 2.0 was launched by former administrators of the original site, but it was also taken down the next year during Operation Onymous. In 2015, Ulbricht was convicted in federal court on multiple charges related to operating Silk Road and was sentenced to two life terms without the possibility of parole.

2.2. *Cybercrimes in The Dark Web*

Drug Trafficking: The dark web is a significant marketplace for buying and selling illegal drugs, often involving complex circumventing traditional regulations.

Human Trafficking: The anonymity of the dark web facilitates human trafficking operations, making it easier to exploit vulnerable individuals.

Fraud and Identity Theft: Cybercriminals use the dark web to steal personal information, including credit card details and social security numbers, for fraudulent activities.

Hacking Services: The dark web hosts a variety of services for hire, including hacking tools and paid cyber-attacks, enabling criminal enterprises.

Counterfeit Goods: Sellers offer counterfeit products, such as fake currencies and luxury items, exploiting the anonymity provided by the dark web.

Stolen Data Trade: Personal and financial information is frequently sold on the dark web, impacting individuals and organizations alike.

Malware Distribution: Cybercriminals distribute malware and ransomware through dark web forums, targeting unsuspecting users and businesses.

Illegal Streaming and Copyright Infringement: The dark web is a platform for illegal streaming services and the distribution of copyrighted material without authorization.

Online Extortion: Cyber extortion schemes, including ransomware attacks, are prevalent, where victims are threatened with data leaks unless a ransom is paid supply chains.

Terrorism & Weapon Sales: Firearms and other weapons can be acquired through various dark web platforms that could be brought by terrorists through cryptocurrency.

3. DARK WEB & INDIA

The dark web in India has emerged as a concerning space, particularly among the youth, who represent a significant portion of the population. This demographic is increasingly drawn to the anonymity and illicit opportunities the dark web offers, leading to a rise in cybercrimes such as hacking, identity theft, and the trafficking of illegal goods. As a result, these activities not only threaten individual security but also undermine the broader economic growth of the country. With a large youth population engaged in criminal activities, resources that could otherwise contribute to innovation and development are diverted toward combating these crimes. Additionally, the negative impact on businesses due to data breaches and financial fraud leads to reduced investor confidence, hindering job creation and economic stability. Thus, the intersection of youth engagement in dark web crimes poses a dual challenge of public safety and economic progress in India. Child pornography is also playing major part of dark web and it affects the economy in greater heights. Terrorist transactions on the dark web can significantly harm the Indian economy by funding violence and increasing security costs, which diverts resources from essential services. This instability undermines investor confidence, reduces spending, and disrupts trade, ultimately stunting long-term economic growth. Human trafficking on the dark web severely undermines India's economy by draining resources and disrupting legitimate labour markets, while also increasing costs for law enforcement and victim rehabilitation. The dark web has gone from strength to strength, and India is high on the list of users. According to a Statista survey in 2019, India accounts for 26 per cent of the global population using the dark web, the highest usage worldwide. Other surveys from 2022, 2023 has listed India among top 5 countries for highest dark web user population. India has the biggest marketplace of dark web users as compared to Australia and South America. According to the Arxiv, 18-25 years old were 35.9% and 26-35 years old were 34.8% of total dark web user's population. India's youth population between the ages of 18 and 35 is over 600 million, which is 43% of the country's total population. Hence, this clearly points the necessity for dark web regulation.[2]

3.1 Dipu Singh: First Narcotics Vendor in India

Dipu Singh, a 21-year-old hotel management student from Amity University in Lucknow, was arrested by the Narcotics Control Bureau (NCB) on January 31, 2020. Described as India's first narcotics vendor apprehended on the dark web, Singh allegedly masterminded the shipment of hundreds of drug parcels to countries like the US, UK, and several European nations using cryptocurrency and clandestine methods. Initially, Singh began by shipping erectile dysfunction medications and fitness supplements. However, recognizing higher profit margins in psychotropic drugs, he quickly transitioned to becoming a prominent figure in the dark web marketplace, with listings on major platforms like Empire Market and Majestic Garden. His operations involved secure communications via platforms such as Wickr and WhatsApp. His activities caught the attention of international authorities, leading to a global investigation called "Operation Trance," initiated in December 2019. The operation focused on tracking shipments of psychotropic drugs. In just one month, the NCB seized over 55,000 psychotropic tablets worth ₹45 lakhs from various locations, ultimately tracing them back to Singh. Singh's involvement in the drug syndicate began in 2018 when he was recruited by an operator of an online pharmacy. By early 2019, he was supplying illegal psychotropic tablets to international clients, completing over 600 drug consignments through the dark web[3]. While authorities hailed his arrest as a significant achievement, critics argue that Singh represents only a small player in a vast and growing market, where larger drug cartels operate with greater sophistication. It was not until 2020, the first drug vendor in dark web was caught. This highlights the ongoing challenges faced by law enforcement in combating the expanding scope of online drug trafficking.

3.2 Global Data Breach Impacting Internet Users

In 2022, a Times of India news article indicate that stolen data from approximately 5 million internet users worldwide is being sold online, with India being the worst affected country, accounting for around 600,000 compromised accounts. This alarming statistic was revealed by NordVPN, one of the largest VPN service providers globally. Following India, the other two countries most affected by this breach are Brazil and the United States. The stolen data encompasses a range of sensitive information, including user logins, cookies, digital fingerprints, and screenshots, all of which can be exploited for malicious purposes. Notably, the average price for an individual's digital identity on the dark web is approximately $5.95 (around ₹490), making this an accessible commodity for cybercriminals. This case highlights the urgent need for enhanced cybersecurity measures and public awareness regarding data privacy. As the market for stolen data continues to thrive, users must be vigilant about the information they share online and consider using protective measures, such as VPNs and strong, unique passwords, to safeguard their digital identities. The implications of this breach extend beyond individual privacy concerns, potentially impacting businesses and national security as well.

Overall, this incident underscores the critical importance of robust cybersecurity strategies and the ongoing challenges faced by individuals and organizations in the digital age.[4]

3.3 Major Data Breach of Aadhaar and Personal Information in India

In October 2023, one of the largest data breaches in Indian history was reported, revealing that the personal information of over 815 million Indian citizens is being sold on the dark web. This alarming disclosure came from US-based cybersecurity firm Resecurity HUNTER, which detailed the scope and implications of the breach. According to Resecurity, the datasets available for sale include critical information such as Aadhaar numbers, passport details, names, phone numbers, and addresses. On October 9, a threat actor known as 'pwn0001' posted a thread on Breach Forums, advertising access to the extensive collection of "Indian Citizen Aadhaar and Passport" records. Cybersecurity analysts investigating the breach discovered a sample containing 100,000 records of personally identifiable information (PII) pertaining to Indian residents. The investigation revealed valid Aadhaar Card IDs within the leaked sample, which were verified using a government portal that offers a "Verify Aadhaar" feature. Additionally, analysts communicated with the threat actor, who claimed that this data was derived from COVID-19 test records of Indian citizens and allegedly sourced from the Indian Council of Medical Research (ICMR). The actor expressed a willingness to sell the complete Aadhaar and passport dataset for $80,000 (over ₹66 lakh). However, the actor did not disclose the method used to obtain the sensitive data. Notably, the ICMR had been subjected to numerous cyber-attack attempts since February, with over 6,000 incidents reported that year. Central agencies and the council were aware of these threats and had urged the ICMR to take remedial actions to safeguard the data. This incident is compounded by a separate breach identified the previous month, where cybersecurity researchers found that the official website of the Ministry of AYUSH in Jharkhand had been compromised, leading to the exposure of over 320,000 patient records on the dark web. The breach, attributed to a threat actor named "Tanaka," revealed a database containing PII and medical diagnoses, as well as sensitive information about healthcare professionals, including their login credentials and contact details. These cases illustrate the significant vulnerabilities in data protection mechanisms in India and highlight the pressing need for enhanced cybersecurity measures. The breaches not only jeopardize individual privacy but also raise broader concerns about the integrity of national databases and the security of sensitive information. This situation underscores the urgent requirement for robust regulatory frameworks and proactive strategies to safeguard citizen data in an increasingly digital landscape.[5]

[2] *Tripathi, A. (2024). Unveiling shadows: Exploring the dark web's impact on Indian law and society. Manupatra.* https://www.manupatra.com

[3] *India Today. (2020, February 9). NCB arrests drug trafficker operating through darknet. India Today.* https://www.indiatoday.in/crime/story/ncb-arrests-drug-trafficker-operating-through-darknet-1644815-2020-02-09

[4] *Times of India. (2022, September 16). Data of 600,000 internet users in India being sold on dark web via bots: What are they and how they operate? The Times of India.* https://timesofindia.indiatimes.com/gadgets-news/data- of-600000-internet-users-in-india-being-sold-on-dark-web-via-bots-what-are-they-and-how-they- operate/articleshow/96084441.cms

[5] *Economic Times. (2023, July 21). Aadhaar data leak: Personal data of 81.5 crore Indians on sale on dark web, report. The Economic Times.* https://economictimes.indiatimes.com/tech/technology/aadhar-data-leak-personal- data-of-81-5-crore-indians-on-sale-on-dark-web-report/articleshow/104856898.cms?from=mdr

3.4 Massive Data Leak Affecting Millions of Users On Social Media Platforms

A significant data breach has exposed the personal profiles of approximately 235 million users across major social media platforms, including Instagram, TikTok, and YouTube. Security researchers from Comparitech identified that an unsecured database was the source of this breach, with the data made available on the dark web. The compromised data was distributed across several datasets, with two substantial datasets containing nearly 100 million records each, primarily scraped from Instagram. Additionally, around 42 million TikTok user profiles and nearly 4 million YouTube profiles were included in the leak. Alarmingly, one in five records contained sensitive information such as telephone numbers or email addresses, along with profile names, real names, profile photos, account descriptions, and engagement metrics like follower counts and likes. Paul Bischoff, Editor at Comparitech, noted that this information is particularly valuable to spammers and cybercriminals for phishing campaigns. While the data was publicly accessible, the structured nature of the leak significantly increased its value compared to isolated profiles[6]. The breach has been traced back to a company called Deep Social, which was banned by Facebook and Instagram in 2018 for violating data collection policies. Despite Deep Social's previous access being revoked, the legacy of its data scraping remains evident. Although the data marketing company Social Data later secured the database following the breach's disclosure, it denied any connection to Deep Social. This incident is part of a larger trend in data breaches, as evidenced by a recent incident involving the hacker group ShinyHunters, which released 386 million user records from 18 companies like BigBasket, photo editing app Pixlr, Delhi based cryptocurrency exchange and wallet, BuyUcoin, e-marketplace ClickIndia etc. The hacker is reportedly responsible for more than 44 public leaks in 2020, with several additional incidents yet to be documented. His databases reportedly hold information on over 1.25 billion people worldwide, including more than 200 million Indians. This situation underscores the ongoing risks associated with data privacy and the vulnerabilities of popular social media platforms, highlighting the need for enhanced security measures to protect user information.

4. HOW DARK WEB AFFECTS ECONOMIC GROWTH

Financial Losses: Cybercrimes such as fraud, data breaches, and identity theft result in substantial financial losses for businesses and individuals. These losses can divert resources away from productive investments and reduce overall economic output.

Reduced Business Confidence: The prevalence of cybercrimes can undermine trust in the digital economy. When businesses and consumers fear becoming victims of cyber-attacks, they may hesitate to invest in online platforms or adopt new technologies, stifling innovation and growth.

Increased Costs of Cybersecurity: As cyber threats rise; companies are forced to invest heavily in cybersecurity measures to protect themselves. While this is a necessary expenditure, it can lead to reduced funds for other growth-promoting activities, such as research and development, employee training, and expansion.

Disruption of Services: Cybercrimes targeting critical infrastructure, such as banking, telecommunications, and healthcare, can disrupt essential services. This disruption can result in lost productivity and can negatively impact overall economic stability.

Job Losses: Cybercrimes can lead to business closures, particularly for small and medium- sized enterprises (SMEs) that may lack the resources to recover from attacks. Job losses resulting from such closures can further hinder economic growth and increase unemployment rates.

Increased Regulation and Compliance Costs: The rise in cybercrimes can prompt governments to implement stricter regulations and compliance requirements. While these regulations aim to protect the economy, they can impose additional costs on businesses, particularly SMEs, which may struggle to meet compliance demands.

Impact on Foreign Investment: High levels of cybercrime can deter foreign investment, as investors may perceive an unregulated digital environment as risky. This can lead to a decrease in capital inflow, limiting the resources available for economic development.

Loss of Consumer Trust: Frequent cybercrimes, particularly those involving personal data breaches, can erode consumer trust in online transactions. A decline in consumer confidence can reduce overall spending, further impacting economic growth.

5. CYBER LAWS REGULATING DARK WEB IN INDIA

5.1. *Information Technology Act, 2000*

5.1.1 *Section 75: Extraterritorial Jurisdiction*

This section asserts that the provisions of the IT Act apply to offenses committed outside India if they involve computers, networks, or resources. This broad scope allows Indian authorities to take action against cybercriminals of any nationality, ensuring that individuals engaging in cyber offenses affecting Indian citizens or infrastructure are held accountable, regardless of their location.

5.1.2 *Sections 43 and 66: Hacking and Data Theft*

- Section 43: This section outlines various acts that constitute unauthorized access or damage to computer resources. It covers hacking, data theft, the introduction of viruses, and the disruption of computer systems. Offenders can face civil liability or criminal charges.
- Section 66: It penalizes similar activities, specifying that hacking or causing damage to a computer system can result in imprisonment for up to three years, a fine of up to ₹5,00,000, or both. This section is vital for addressing a wide range of cyber offenses, making it a cornerstone of the IT Act.

5.1.3 *Section 66B: Receipt of Stolen Property*

This section specifically targets individuals who receive stolen computer resources, mandating that the recipient must have known or had reason to believe the property was stolen. Penalties for violating this section can include imprisonment for

[6] *Bischoff, P., & Bischoff, P. (2021, May 30). Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok, and Youtube. Comparitech.* https://www.comparitech.com/blog/information- security/social-data-leak/

up to three years and/or a fine of up to ₹1,00,000, addressing the broader issue of trafficking in stolen digital goods.

5.1.4 *Section 66C: Identity Theft*

This section criminalizes the fraudulent use of another person's electronic signature, password, or other identifying information. It imposes penalties of up to three years of imprisonment and fines, protecting individuals from identity fraud, which is particularly relevant in the context of the dark web where personal data is often traded illegally.

5.1.5 *Section 66D: Cheating by Personation*

This section addresses the use of computers to cheat by impersonation. It penalizes individuals who mislead others by using technical devices for deceitful purposes, with similar penalties as Section 66C. This is critical in preventing scams and frauds that proliferate on the dark web.

5.1.6 *Sections 67, 67A, and 67B: Obscenity and Child Pornography*

- Section 67: Punishes the publishing or transmission of obscene material in electronic form, with penalties including imprisonment for up to three years and fines.
- Section 67A: Specifically targets sexually explicit content, imposing harsher penalties, including up to five years of imprisonment and higher fines for repeat offenders.
- Section 67B: Focuses on child pornography, carrying severe penalties, reflecting the urgency of combatting this egregious crime that often finds a market on the dark web.

5.1.7 *Section 43(h): Financial Fraud*

This section penalizes unauthorized alteration or manipulation of a computer or network to benefit financially at another's expense, such as changing electricity billing. This addresses various fraudulent schemes that can occur online, reinforcing the importance of safeguarding digital financial transactions.

5.1.8 *Section 65: Tampering with Computer Source Documents*

This section makes it illegal to intentionally conceal, destroy, or alter computer source documents. Violations can result in imprisonment for up to three years and/or fines up to ₹3,00,000. This section is crucial for maintaining the integrity of digital records and preventing manipulation of data, which is a significant concern in cybercrimes.

5.1.9 *Section 66E: Breach of Privacy*

Section 66E protects individual privacy by criminalizing the unauthorized capturing or distribution of private images. Penalties include imprisonment for up to three years and fines, addressing privacy violations that are rampant in the digital age, particularly on the dark web.

5.1.10 *Section 67C: Responsibilities of Intermediaries*

This section mandates that intermediaries (like ISPs and online platforms) retain specified data for a duration defined by the government. It penalizes those who fail to comply, ensuring that data can be accessed for legal investigations, thereby supporting law enforcement efforts against cybercrime.

5.1.11 *Section 66F: Cyber Terrorism*

This section addresses cyber terrorism, imposing stringent penalties on those who use computer systems to threaten national security, integrity, or public safety. Offenders can face severe consequences, including lengthy imprisonment, reflecting the seriousness of cyber threats against a nation.[7]

5.2. *Budapest Convention On Cybercrime*

The Budapest Convention on Cybercrime, adopted by the Council of Ministers, was opened for signature in Budapest on November 23, 2001, and came into effect on July 1, 2004. A notable aspect for India is the provision allowing non-member states to sign and ratify the convention (Article 37). For example, Montenegro became a non-member signatory in April 2005. The convention aims to establish a unified criminal policy to protect society from cybercrime by promoting appropriate legislation and international cooperation. Its three main purposes include defining material criminal law to harmonize legislative efforts, standardizing investigation measures and criminal procedures, and facilitating international cooperation. The convention categorizes offenses into four groups: crimes against the confidentiality, integrity, and availability of data; computer-related offenses like forgery and fraud; content- related offenses, including child pornography; and violations of intellectual property rights. In 2003, an additional protocol was signed to address racist and xenophobic acts committed via computer systems. The convention also addresses gaps in national laws, such as unauthorized access to computer systems, providing a framework for countries to follow. Crimes related to the dark web, such as the production and distribution of illegal devices or access codes, are covered under Article 8, which emphasizes the intention of the perpetrator. Offenses like child pornography and copyright infringements fall under Articles 9 and 10. Thus, the convention offers a valuable framework for regulating dark web crimes in India. Furthermore, it addresses extradition and mutual legal assistance through Articles 24 and 25-34, establishing a 24/7 network for support (Article 35). Article 40 allows nations to declare conditions related to their ratification, exemplified by Denmark's stance on child pornography laws. Given its comprehensive nature and broad signatory base, the Budapest Convention remains a critical legal instrument for combating dark web and cybercrimes, standing out among other international initiatives. Its extensive reach and initiatives for cooperation, such as the Commonwealth's Model Computer and Computer-related Crimes Bill, further enhance its significance in the global fight against cybercrime.[8]

6. LIMITATIONS IN THE LEGISLATIONS & THE CONVENTION

There is no specific legislation for regulating Dark web and it relies on provisions regulating cybercrimes. Indian

[7] *Government of India. (2000). The Information Technology Act, 2000 (No. 21 of 2000). Ministry of Law and Justice. Retrieved from* https://www.indiacode.nic.in

[8] *Ojha, S. (2020, June). Surge in Dark Web Crimes, the Indian Legal Scenario and 'International Cooperation' as the Way Forward. In Proceedings of the 17th International RAIS Conference on Social Sciences and Humanities (pp. 131-136). Scientia Moralitas Research Institute.*

legislation currently lacks specific provisions to effectively regulate the dark web, leaving significant gaps in addressing the rapidly evolving nature of cybercrime. The anonymity and secretive features of the dark web make it particularly challenging to identify and prosecute crimes, as traditional statutes do not account for the unique methods of concealment used by offenders. Existing laws, such as the Information Technology Act, are outdated and often fail to keep pace with advancements in technology and the innovation of criminal activities, resulting in inadequate responses to threats like human trafficking, child exploitation, and financial fraud. As cybercriminals continually adapt and exploit vulnerabilities, India's crime rate in hidden markets and on the dark web is rising uncontrollably. The Budapest Convention on Cybercrime, while a significant step in international law, is limited in its ability to regulate dark web crimes due to outdated provisions and a lack of specific focus on the unique challenges posed by the dark web. It primarily addresses traditional cybercrime, leaving gaps in tackling issues such as anonymity and decentralized activities that facilitate human trafficking and the distribution of illicit content. The convention relies on cooperation among member states, but inconsistent enforcement and varying domestic laws hinder effective collaboration, allowing cybercriminals to exploit jurisdictional loopholes. Additionally, the rapid evolution of technology and the rise of cryptocurrencies in illegal transactions outpace the convention's adaptability.

6.1 *Key Legal Issues in Regulating the Dark Web*

Anonymity and Identification: The dark web's primary feature is user anonymity, making it challenging for law enforcement to identify and apprehend offenders. Traditional identification methods, such as IP tracking, are ineffective on platforms like Tor, complicating investigations.

Jurisdictional Challenges: The global nature of the dark web means that criminal activities often span multiple jurisdictions. This raises complex legal questions about which laws apply, how to enforce them, and the difficulties of extraditing suspects.

Legal Frameworks: Existing laws often do not adequately address the unique characteristics of dark web activities. In many countries, including India, legislation like the Information Technology Act may lack specific provisions tailored to the intricacies of online marketplaces for illegal goods and services.

International Cooperation: Effective regulation requires collaboration among countries, yet differences in legal standards and enforcement practices can hinder cooperative efforts. Variations in laws related to privacy, cybercrime, and data protection complicate cross-border investigations.

Privacy vs. Security: Striking a balance between protecting individual privacy rights (Article 21) and ensuring public safety (also Article 21) is a critical legal challenge. Over-regulation could infringe on civil liberties, while under-regulation could allow criminal activities to flourish.

Regulation of Cryptocurrency: The rise of Cryptocurrency for transactions on the dark web poses regulatory challenges. These digital currencies provide anonymity for users, complicating efforts to trace financial transactions related to illegal activities.

Data Protection and Privacy Laws: The dark web often hosts stolen personal data, raising issues related to data protection laws. Ensuring compliance with such laws while investigating illegal activities can be legally complex.

Evolving Technology: Rapid advancements in technology, such as the emergence of decentralized platforms and advanced encryption techniques, outpace existing legal frameworks. Regulators must continuously adapt to keep up with these technological changes.

Law Enforcement Training and Resources: Law enforcement agencies often lack the specialized training and resources necessary to effectively tackle dark web crimes. This gap can hinder investigations and prosecutions.

Public Awareness and Education: A lack of public understanding regarding the risks and implications of the dark web complicates regulatory efforts. Educating users about the dangers associated with the dark web is essential for prevention and safety.

7. RECENT INITIATIVE TAKEN BY GOVERNMENT

The Indian government has long been in conflict with VPN services, as these tools allow users to bypass restrictions and access blocked content. In September 2021, a parliamentary standing committee on home affairs recommended a permanent ban on VPNs, citing concerns that cybercriminals use these services to evade restrictions and access the dark web. However, the committee did not acknowledge the widespread, legitimate use of VPNs by millions of Indians, including businesses. While the government did not impose an outright ban, it did follow the committee's suggestion to enhance surveillance and tracking of VPN usage. In response, the Indian government introduced a new policy in 2022 that requires VPN providers to store extensive user data for at least five years. This data includes user names, email addresses, phone numbers, the purpose for using the VPN, IP addresses used during registration and by the service, and usage patterns such as timestamps and subscription details. VPN providers are also obligated to submit this data to the Computer Emergency Response Team (CERT-In) upon request, and report cyber incidents such as data breaches, phishing, and unauthorized access[9]. Failure to comply with the new regulations can result in punitive actions, including fines, service bans, or even imprisonment. In addition to VPN providers, data centers, cloud service providers, and cryptocurrency exchanges are also required to collect and store user data in accordance with the law. Although the law was set to be enforced by June 2022, VPN companies have expressed strong resistance with some waiting to meet deadline to see what will happen when enforcements arrive, and with many choosing to shut down their physical servers in India, following the actions of similar providers in countries like Russia and

[9] *Chadha, S. (2022, June 1). Explained: What the new VPN rules mean for internet users in India. The Times of India.* https://timesofindia.indiatimes.com/business/india-business/explained-what-the-new-vpn-rules-means-for-internet-users-in-india/articleshow/91510719.cms

China. These companies, including NordVPN, ExpressVPN, and Ivacy, are holding firm on their commitment to not logging user data and are awaiting further developments in the enforcement of these regulations.

8. RECOMMENDATIONS

To effectively curb dark web crimes, India must introduce new provisions that specifically address the challenges posed by this hidden space, as existing laws remain inadequate in responding to the rapid pace of technological advancements. The current legal frameworks, such as the Information Technology Act (IT Act) and international conventions like the Budapest Convention, are outdated and fail to keep up with the evolving methods criminals use to exploit the dark web. The IT Act, for example, does not specifically account for crimes perpetrated through encrypted platforms and the dark web's anonymity features, leaving significant gaps in enforcement. Similarly, the Budapest Convention, while a valuable international agreement, has its own limitations when it comes to addressing the anonymity and decentralized nature of dark web crimes, and there is an urgent need for a more comprehensive and updated global framework to handle the complexities of modern cybercrimes. These outdated provisions hinder law enforcement's ability to track and prosecute dark web offenders, as criminals can easily circumvent existing regulations through technological tools that allow for near-complete anonymity. In this context, India needs to introduce new laws that specifically target dark web crimes, such as cyber trafficking, illicit trade, and hacking activities, while also ensuring these laws do not infringe on citizens' fundamental right to privacy under Article 21 of the Indian Constitution. The challenge lies in creating a legal framework that protects individuals' privacy but also enables effective enforcement against the illegal activities flourishing on the dark web. While the right to privacy is crucial, the government must ensure that measures to safeguard public safety and the right to life are not neglected, creating a balanced approach. A key aspect of tackling dark web crimes is regulating VPNs, which are commonly used to mask users' identities and facilitate anonymous access to illegal activities. The recent CERT-In law, which mandates VPN providers to store and submit user data, has proven ineffective in preventing dark web access, as many VPN services continue to operate without fully complying with these regulations. To address this, India must implement stricter enforcement of VPN regulations, ensuring that these services cannot be misused for criminal purposes. Given that dark web activities often cross-national borders, international cooperation is essential to overcome jurisdictional challenges. India should advocate for a more robust international legal framework, either through the enhancement of the Budapest Convention or the creation of a new agreement, to enable better cooperation in tracking and prosecuting dark web criminals who operate across multiple countries. This cooperation should also focus on the rapid pace of technological development, ensuring that international conventions remain adaptable and capable of addressing new challenges in cyberspace. Additionally, the anonymity that defines the dark web makes it difficult for law enforcement agencies to track and apprehend offenders. To counter this, India could establish a dedicated regulatory body tasked with monitoring dark web activities, employing cutting- edge technologies to uncover illegal activities without infringing on privacy. This body could work closely with national and international agencies to ensure that the dark web is constantly under surveillance, enabling more targeted interventions. Finally, improving these regulatory frameworks is not only vital for national security but also crucial for fostering India's economic growth. A secure digital environment, where cybercrimes—especially those originating from the dark web—are effectively controlled, will enhance trust in digital platforms, boost e- commerce, and encourage foreign investment. A strong legal infrastructure will contribute to the stability of India's digital economy, ensuring that technological advancements can be leveraged for growth without compromising safety. In conclusion, India must modernize its laws to address dark web crimes, strengthen VPN regulation, and foster international cooperation. These measures will not only protect public safety but also ensure that the country's digital economy can thrive in an increasingly interconnected and technologically advanced world.

9. CONCLUSION

The regulation of the dark web presents a complex challenge that requires a balanced and forward-thinking approach. The anonymity and decentralization inherent in dark web markets have made it a haven for illicit activities such as drug trafficking, human trafficking, and the sale of illegal goods. In India, where a significant portion of the population is engaged in digital transactions and online platforms, the dark web poses a unique risk to both public safety and the economy. Existing legal frameworks, including the Information Technology Act and international conventions like the Budapest Convention, are outdated and fail to address the rapid technological advancements and the evolving nature of cybercrimes. To effectively regulate these hidden markets, India must introduce targeted reforms that protect privacy while ensuring the safety of its citizens and the integrity of digital commerce. Strengthening VPN regulations, improving international cooperation, and creating dedicated bodies to monitor dark web activities are essential steps in combating these crimes. By updating legal frameworks, enforcing stricter controls, and fostering global collaboration, India can better safeguard its digital economy and mitigate the economic and social risks associated with dark web crimes.

10. CONFLICT OF INTEREST

Conflict of interest declared none

11. AUTHOR CONTRIBUTION STATEMENT

Study conception, design, data collection, analysis and interpretation of results, and manuscript preparation were performed by SE. Analysis, streamline processes and manuscript preparation were performed by SB.

12. REFERENCES

Ojha, S. (2020, June). Surge in Dark Web Crimes, the Indian Legal Scenario and 'International Cooperation'as the Way Forward. In *Proceedings of the 17th International RAIS Conference on Social Sciences and Humanities* (pp. 131-136). Scientia Moralitas Research Institute.