The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

LEGAL IMPLICATIONS OF THE DARK WEB: BRINGING THE DARK SIDE TO LIGHT FOR SOCIAL LEGAL ANALYSIS

~ Pranjal Arora

Abstract

The "Dark Web" is the foremost infamous and secretive zone of the web, where unbelievable unlawful action takes place. It serves a double reason, permitting clients to investigate the profundities of the Web namelessly whereas shielding touchy communications. The Dark Web moreover harbors a noteworthy sum of criminal action, extending from drug-related cybercrimes, such as hacking and character burglary to energize cure trades. In spite of the presence of the Dark Web, it remains an imposing danger to the internet's security, as information breaches and spills hold on. This research paper centers on the legitimate consequences and challenges related with the dark web's presence in India, centering on the legal framework in arranging illegal activities on the gloomy web. The reasonability of the current legal framework in arranging illegal works out on the dark web in India can be surveyed based on a legal and social approach that combines genuine, mechanical, and collaborative endeavors, while prioritizing all inclusive cooperation and open mindfulness to protect the web and the interface of its citizens.

Keywords

Internet,Web, Dark web, Illegal, IT Act, UAPA

Introduction

The way we have evolved from ancient times to bring ourselves into this modern world, the internet has also evolved over many years. It started as an invention that fascinated people, and soon after, people began using it to make their work easier and save time. As generations passed,

it became an integral part of our lives. Today, in this modern world, the internet isn't just for solving our queries but, in some cases, it is also used to mistreat others.

The internet can be divided into three stages: Surface Web, Deep Web, and Dark Web. What an ordinary person accesses on their browser is just a small portion, about 4 to 5 percent, of the entire internet. This part is called the Surface Web and is accessible to regular users, including websites like Google, Yahoo, YouTube, and more. The Deep Web, which is not accessible to the average person, contains hidden information for security reasons. It includes both illegal and legal activities performed anonymously.

The Dark Web, the lowest and most dangerous part, is not easily accessible to ordinary people. Unexpectedly, millions of people still use it every day. You can find a variety of illicit activities here, including buying narcotics, hiring hit men, and other illegal actions. The most notorious and mysterious area of the internet is known as the "Dark Web," where unfathomable illicit activity takes place.

The evolution of the internet from its humble beginnings to the complexity of today's online landscape illustrates a duality that mirrors human nature itself. It has brought about unprecedented convenience, knowledge-sharing, and opportunities for global collaboration. Simultaneously, it has unveiled darker aspects of human behavior, exploiting the same anonymity and connectivity to facilitate criminal endeavors.

As we continue to navigate this digital realm, it becomes imperative to strike a balance between preserving the positive aspects of the internet and addressing the challenges it poses. Education, cybersecurity measures, and law enforcement efforts are essential to ensure that the internet's evolution continues to empower while safeguarding society from its darker underbelly.

Silk Road, once a prominent and highly lucrative website on the Dark Web, stands as a testament to the immense financial potential of clandestine online marketplaces. While it is no longer operational, its impact during its active years was profound, accumulating an astonishing estimated revenue of $187 billion USD. This substantial figure underscores the scale of illicit trade that thrived in the hidden recesses of the internet. However, Silk Road's demise did not signal the end

of such activities on the Dark Web. Alternatives and successors have emerged, offering similar illegal commodities such as drugs, weapons, and more. These underground marketplaces continue to exploit the relative anonymity and encryption of the Dark Web to facilitate their transactions.

Beyond the realm of commerce, there exists a more disturbing facet of the Dark Web: the existence of disturbing and illegal content-sharing platforms known as "red rooms." These spaces are infamous for hosting live-streamed videos of heinous acts, including violence and other criminal activities. The existence of red rooms raises alarming ethical, legal, and moral questions regarding online freedom and responsibility. In a shocking twist, the mention of "Cannibal Cafe" highlights an even darker aspect of the Dark Web. This site, notorious for its disturbing content related to cannibalism, underscores the extent to which the internet's anonymity can be exploited for the propagation of depravity.

Silk Road's incredible revenue and subsequent closure represent just one chapter in the complex narrative of the Dark Web's illicit activities. Despite law enforcement efforts, alternatives have risen to take its place, perpetuating the challenges associated with illegal online commerce and disturbing content sharing. The Dark Web remains a volatile and evolving frontier where questions of ethics, legality, and digital responsibility persist.[1]

Research methodology

The social legal analysis approach used in this study of Legal implications of Dark web integrates legal, ethical, and sociological viewpoints. Data is gathered from legal statutes, case studies, and academic journals, giving a thorough picture of the legal ramifications of the Dark Web.

[1]Saha, S. et al. (2022) Dark web: The hub of crime, IJRASET. Available at: https://www.ijraset.com/research-paper/dark-web-the-hub-of-crime#:~:text=The%20dark%20web%20is%20a,to%20the%20dark%20web%20websites

Means to access and uses of Dark Web

While the name "Dark Web" might evoke a sense of mystery and illicit activities, it's important to clarify that using it is not inherently unlawful. The Dark Web indeed offers individuals a degree of privacy and maintains their anonymity, which contributes to its robust security features[2]

As previously discussed, the Dark Web is not readily accessible to the average internet user. It requires a separate browser known as TOR (short for "The Onion Router"). Once installed, TOR functions much like a regular browser, but with added layers of encryption and obfuscation, making it challenging to trace users' identities. This anonymity is a fundamental aspect of the Dark Web's design[3].

Interestingly, Tor originally emerged as a tool to protect sensitive government communications before finding wider adoption among the general public. Today, it serves a dual purpose, allowing users to explore the depths of the internet anonymously while safeguarding sensitive communications.

While it may seem strange, using the Dark Web is not illegal in many countries. Governments themselves utilize it for surveillance and intelligence gathering. However, it's essential to recognize that beyond its legal users, there is indeed an illegal side to the Dark Web. It hosts activities that include the illegal trade of drugs, weapons, counterfeit passports, pornography, and other harmful endeavors.

[2]BLOOMENTHAL, A. (2022) What is dark web and should you access it?, Investopedia. Available at: https://www.investopedia.com/terms/d/dark-web.asp
.

[3]Frankenfield, J. (2022a) What is tor? who uses it, how to use it, legality, and purpose, Investopedia. Available at: https://www.investopedia.com/terms/t/tor.asp

Governments around the world have taken notice of these illicit activities, leading to the discovery and shutdown of numerous Dark Web sites, such as Silk Road and AlphaBay. However, the Dark Web's existence continues to pose challenges for cybersecurity, as data breaches and leaks persist.[4]

In summary, the Dark Web is a complex and multifaceted realm. While it provides a level of privacy and security that has legitimate applications, it also harbors illegal activities. Law enforcement and governments grapple with the dual nature of the Dark Web, striving to maintain cybersecurity while curbing unlawful actions conducted in its shadows.

Legal challenges presented by Dark web for Law enforcement agencies

The Dark Web, hidden in the corners of the internet due to its security features, indeed harbors a significant amount of criminal activity. This is because tracing such activities becomes exceptionally challenging, posing several challenges for our legislation.

1. Firstly, anonymity is a formidable challenge for our legal systems. The Tor browser, which provides security to its users, ensures that they cannot be easily traced or identified. This poses a significant challenge for our legislation in determining who is engaged in illegal activities on the Dark Web and where these activities are originating from.
2. Secondly, the diversity of individuals involved in the Dark Web, engaging in various forms of trade or illicit activities from different countries, further complicates matters for our legislation.
3. The use of cryptocurrency, especially Bitcoin, for transactions on the Dark Web presents another major challenge. Bitcoin transactions are nearly untraceable, making it nearly impossible to determine where funds have gone or who sent them. If there were other means of financial transactions, the government might have been able to trace who sent money where.

[4]'Everything you should know about the dark web' (no date) Tulane. Available at: https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web#:~:text=Given%20its%20anonymous%20nature%2C%20the,and%20other%20potentially%20harmful%20materials.

4. Collecting evidence against the Dark Web, which remains a mystery for many, is indeed a challenge. Gathering conclusive proof of these activities is difficult, and it presents hurdles for any legal process against it.

As the Dark Web continues to grow and attract more users daily, preventing it or understanding its capabilities is far from easy. Despite our knowledge of the types of activities occurring on the Dark Web, these challenges have so far made our legislation largely ineffective in halting or curbing these activities.

Related acts/sections for Dark web

- Information technology Act,2000

As we all know, the Information Technology Act is an Indian law for electronic commerce, which encompasses things like online transactions and digital signatures. Similarly, it has some implications for the dark web.

The dark web, which is a hidden corner of our internet, also involves activities that are illegal, including digital signatures and online transactions. Information Technology Act and the dark web are related in some ways:

Securing personal data of every Indian is primarily the responsibility of the Information Technology Act, as it provides security akin to physical mail. What is happening in the dark web, where people's data is being saved, is against our Information Technology Act, and it is harmful.

The Act contains sections that deal with hacking, identity theft, and the like, which are also the kinds of illegal activities found on the dark web. Those engaging in such activities can be penalized under the Information Technology Act.[5]

[5] Sehgal, D.R. (2021) Laws relating to the dark web in India, iPleaders. Available at: https://blog.ipleaders.in/laws-relating-dark-web-india/

There is a term in the Information Technology Act called 'intermediary liability,' which means that an application is responsible for what data its users are using or what activities they are engaging in. Being an Indian law, the Information Technology Act can regulate what activities are happening in India on the dark web, and those involved may face legal consequences.

Section 66C: Identity theft
Section 66D: Cheating by personation by using a computer
Section 66F: Cyberterrorism
Section 67: Publishing or transmitting obscene material online

- Unlawful Activities (Prevention) Act, 1967

The Illegal activities (Avoidance) Act, frequently known as UAPA, is an Indian law that was ordered to halt unlawful activities that might undermine India's keenness and sway. Indeed whereas UAPA centers on terrorism-related activities, it may have impacts on the dim web within the setting of cyberterrorism and online radicalization. UAPA and the dim web may be related within the taking after ways:

1. Cyberterrorism:
The UAPA has clauses that address fear mongering in common, counting cyberterrorism. Cyberterrorism is the utilization of advanced apparatuses, such as the web and dark web, to dispatch attacks on imperative foundations, spread untrue data, or carry out other activities with the intention of hurting or ingraining fear. UAPA may be utilized against individuals or associations utilizing the dark web to commit cyberterrorist acts.
2. Online Radicalization:
The dim web may be utilized as a dissemination channel for radical philosophy and the selection of people in fear based oppressor bunches. UAPA empowers law requirements to require activity against people locked in in online selecting and radicalization efforts, indeed in the event that such people work on dark web spaces just like the dim web.
3. Cash and Bolster:

To back their operations, fear based oppressor bunches habitually search for cash and bolster through an assortment of roads, counting the dark web. UAPA may be utilized to target individuals or associations who lock in in shady web exchanges to donate money to these bunches.

4. Insights collection:

To distinguish conceivable dangers and follow the developments of individuals or associations suspected of being included in illicit exercises, law authorization specialists may screen the dim web for insights collection reasons. A legitimate premise for such reconnaissance and request is given by UAPA.

5. Removal and Worldwide collaboration:

In the event that individuals or associations included in illicit action on the dim web have joins overseas, UAPA can offer assistance with removal and universal collaboration to capture and arraign them.[6]

Section 39: Support to terrorist organizations

- Narcotics Drugs and Psychotropic Substances Act,1985

The Opiate Drugs and Psychotropic Substances Act, commonly known as the NDPS Act, is an Indian law sanctioned to direct and control operations relating to opiate drugs and psychotropic substances. It fundamentally centers on the generation, fabricate, ownership, deal, buy, transport, warehousing, utilize, utilization, consequence inter-State, send out inter-State, moment into India, trade from India, purport into India from a remote region, trade from India to a outside region or transshipment of opiate drugs and psychotropic substances.

Here's how the NDPS Act can be related to the dark web:

1. Unlawful Sedate Exchange:

[6] The Unlawful Activities (Prevention) Act, 1967 arrangement of sections (no date) Ministry of Home affairs . Available at: https://www.mha.gov.in/sites/default/files/A1967-37.pdf.

The dim web is known for facilitating illicit sedate marketplaces where opiates and psychotropic substances are bought and sold namelessly. The NDPS Act gives the legitimate system to combat such drug-related exercises, counting those conducted through the dark web.

2. Online Sedate Trafficking:

The act moreover covers online sedate trafficking, which incorporates exercises on the dim web. Individuals included in trafficking drugs on the dim web can be indicted beneath the NDPS Act on the off chance that they are found in ownership of illicit substances.

3. Cybercrime and dark Web:

In cases where the dark web is utilized for drug-related cybercrimes, such as hacking and character robbery to encourage medicare exchanges, the NDPS Act can be utilized in conjunction with other cybercrime laws to address these offenses comprehensively.

4. Universal Medicare Exchange:

The dim web empowers universal sedate exchange, and the NDPS Act can be conjured when drugs are imported into India from remote domains or traded from India to remote domains through these online channels.

5. Law Requirement and Dim Web Observing:

Law requirement organizations may screen the dark web to distinguish and track people or bunches included in drug-related exercises. The NDPS Act underpins these endeavors by giving a lawful premise for examination and indictment.[7]

Section 8: Prohibition of opium cultivation

Section 18: Punishment for contravention in relation to cannabis plant and cannabis

Section 21: Punishment for contravention in relation to poppy straw and opium

[7] Dark side of the dark net (no date) Legal Service India - Law, Lawyers and Legal Resources. Available at: https://www.legalserviceindia.com/legal/article-4113-dark-side-of-the-dark-net.html

Effectiveness of current legal framework in prosecuting illegal activities on Dark web

The viability of the current lawful system in arranging unlawful exercises on the dark web in India can be assessed based on a few components:

1. Enactment and Cybercrime Laws:
India has different laws, counting the Data Innovation Act (IT Act), the Opiate Drugs and Psychotropic Substances (NDPS) Act, and the Illegal Exercises (Anticipation) Act (UAPA), which can be utilized to arraign illicit exercises on the dark web. In any case, the adequacy depends on how well these laws are implemented and adjusted to the advanced scene.

2. Cybercrime Units:
India has built up specialized cybercrime units inside law requirement organizations to examine cybercrimes, counting those on the dim web. The adequacy of these units in following and indicting wrongdoers on the dim web depends on their preparation, assets, and collaboration with universal organizations.

3. Universal Participation:
Given the transnational nature of the dark web, worldwide participation is significant. India has been working with universal law requirement organizations to handle illicit exercises on the dark web, but the viability depends on the level of participation and data sharing.

4. Secrecy and Encryption:
One of the challenges in indicting dim web exercises is the utilization of encryption and anonymizing advances by guilty parties. Law requirement offices have to have the specialized capabilities to overcome these obstacles viably.

5. Mindfulness and Capacity Building:
Raising mindfulness among law requirements, the legal, and other pertinent partners almost the complexities of the dim web is basic. Capacity building and preparing programs are crucial to improve the viability of examinations and arraignments.

6. Lawful Challenges:
Legitimate challenges, such as jurisdictional issues and the tolerability of digital evidence, can prevent fruitful indictments. The legitimate framework has to advance to address these challenges satisfactorily.

7. Asset Assignment:
Satisfactory allotment of assets to cybercrime units and specialized agents is pivotal for compelling dim web authorization. This incorporates the arrangement of cutting-edge innovation and instruments for examination.

8. Public-Private Associations:
Collaboration between law authorization organizations and the private segment can offer assistance in recognizing and tending to dark web dangers. Private companies frequently have profitable data about cyber dangers and unlawful exercises.

It's imperative to note that the scene of the dark web and cybercrime advances quickly. In this manner, the adequacy of the lawful system in arranging illicit exercises on the dark web may be an energetic challenge. Law requirement organizations got to adjust ceaselessly to keep up with emerging threats and advances.

Suggestions and Conclusion

Certainly, here are a few recommendations and a concluding outline on the subject of the dark web in India:

1. Upgraded Cybersecurity Measures:
Reinforcing the cybersecurity framework at both government and private segment levels is basic. This incorporates customary security reviews, upgrades, and risk insights sharing.
2. Capacity Building:

Ceaseless preparation and aptitude advancement for law authorization organizations, judges, and lawful experts in managing cybercrimes and the dark web are basic.

3. Worldwide Collaboration:

India ought to cultivate more grounded participation with worldwide law authorization organizations to combat cross-border dark web exercises viably.

4. Open Mindfulness:

Advance open mindfulness approximately the dangers of the dark web, cybersecurity best hones, and detailing instruments for suspicious online exercises.

5. Private Segment Association:

Energize private division companies to contribute in the investigation and advancement of apparatuses to combat dark web dangers, and collaborate with law authorization.

6. Lawful Changes:

Frequently upgrade and revise existing laws to address advancing dark web challenges, whereas guaranteeing regard for security and gracious freedoms.

Conclusion:

The dark web presents complex challenges for India and the world at large. It may be a domain where illicit exercises, counting cybercrimes, medicate trafficking, and more, can prosper due to its secrecy and encryption highlights. To address these challenges viably, India needs a multi-faceted approach that combines legitimate, mechanical, and collaborative endeavors.

Whereas India has made strides in sanctioning and implementing laws related to cybercrimes and the dark web, it must proceed to adjust and advance its techniques. Universal collaboration, open mindfulness, and cybersecurity improvements are all significant components of handling the dim web successfully.

In conclusion, tending to the dim web's illegal exercises in India requires a proactive and multifaceted approach that considers both lawful and innovative measurements whereas prioritizing universal participation and open mindfulness to defend the internet and the interface of its citizens.