DARK WEB: A HIDDEN WORLD - ETHICAL AND LEGAL CHALLENGES IN COMBATING DARKWEB CRIME

Avni Kaushal, Babu Banarasi Das University (BBDU)

ABSTRACT

As we know the digital world has deeply become an intergral part of our everyday lives, fundamentally altering and shaping our behaviour, and influencing how we interact with each other and the world. It's fascinating to note that the dark web reportedly encompasses around 45% of the data found on the internet[1].

Technological advancements like Tor, bitcoin, and crypto currencies allow criminals to carry out activities anonymously, leading to increased use of the Darkweb. Thus this article explores the ethical and legal challenges of combating crimes on the Darkweb, including privacy, surveillance, and the balance between law enforcement and individual rights. The Darkweb, part of the deep web, can be accessed only through specialized computer software and used for illegal activities such as cybercrime, drug trafficking, exploitation, etc. The browser software used to access the dark web provides users with anonymizing and encrypting features, deliberately shielding their browsing behaviors, physical locations, and true identities. This ensures a heightened level of privacy and security for users navigating the dark web.

The dark web has transformed into a thriving hub for unlawful transactions, posing a considerable threat to cyberspace across several dimensions.

[1] techjury.net

"By failing to prepare, you are preparing to fail."

~ Ben Franklin

Introduction

The Internet is a complex network comprised of multiple interconnected computer networks and their extensive infrastructure. Within this framework, the web, commonly referred to as the Surface Web, holds within the easily accessible websites that are discoverable through widely-used search engines such as Google, Bing and Firefox. Beyond the Surface Web lies the Deep Web, which contains unindexed content that cannot be reached through conventional search engines. Within the deep web lies a section referred to as the "dark web," *It covers approximately 45% of the data on the internet*[2] which is intentionally concealed and can only be accessed using specialized software browsers like Tor (The onion router). The dark web is also known as the "*invisible web*" or the "*hidden web*." The use of anonymizers on the dark web creates a formidable barrier to tracking web patterns such as browsing history and location, making it a favored tool for individuals with nefarious intentions. Criminals leverage the cloak of anonymity to conceal their identities and perpetrate a wide array of illicit activities. It has evolved into a marketplace for unauthorized trade, including the sale of stolen data and other prohibited activities.

The Darkweb, also referred to as the Darknet, clandestine section of the deep web that is notorious for harboring illegal activities and clandestine operations. It is inaccessible through standard search engines and requires specific software or authorization to access. Originally designed for secure military and intelligence purposes, the Darkweb has unfortunately provided a platform for individuals to engage in a wide range of criminal activities, including but not limited to drug trafficking, weapons dealing, human trafficking, cybercrime, and the dissemination of extremist ideologies. As a result, it presents significant challenges to law enforcement agencies and poses serious risks to societal safety and security. The Darkweb has been predominantly recognized as a platform for facilitating crime-as-a-service. However, addressing the wide range of challenges associated with combating illicit activities and advancing cyber threat intelligence continues to be the primary focus of Darkweb research.

[2] techjury.net

History

The Tor network, originally developed by the U.S. government's Naval Research Laboratory, was initially intended to provide secure and anonymous Internet access for U.S. intelligence community members. It was later made open-source by the U.S. government in 2004, leading to the establishment of the Tor Project to ensure its ongoing development and maintenance.

The origins of the modern dark web can be traced back to the year 2000 when Ian Clarke, an Irish student, created Freenet. This platform allowed for discreet online communication through a decentralized network of users. However, the true turning point for the dark web came in September 2002 with the introduction of The Onion Router (Tor), which significantly raised its profile.

The dark web gained widespread attention in 2013 following the arrest of Ross William Ulbricht, who operated under the alias Dread Pirate Roberts, for running the Silk Road. This online marketplace facilitated the sale of illegal goods and services and relied on the use of Tor for its operations. The shutdown of the Silk Road brought the dark web and its illicit activities to the forefront of public consciousness.

Challenges

In the context of efforts to regulate internet usage, a commonly cited argument in favor of unrestricted access revolves around the potential infringement of basic rights. Notably, "*the Kerala High Court in India was the first to acknowledge internet access as a fundamental right, a position subsequently upheld by the Supreme Court.*"

Considering the integral role of the internet in our daily lives, imposing blanket restrictions on its usage is a formidable task. It's important to note that accessing the dark web is not inherently illegal, and any legislation aiming to govern access to it should be underpinned by clear guidelines and a justifiable cause in order to mitigate the risk of being invalidated on constitutional grounds.

Another issue that warrants consideration is the proliferation of Virtual Private Networks (VPNs). The popularity of VPNs stems from the enhanced privacy and security they afford users. While the use of VPNs is not inherently unlawful, questions may arise regarding the necessity for individuals to conceal their internet activities from being traced.

Despite these complexities, it appears improbable that VPNs will be outlawed in India in the near future. Apart from VPNs, challenges also encompass the inadequacy of infrastructure and the necessity for appropriate regulation of internet service providers (ISPs). Should the Central Government take a decisive stance, it may encounter difficulties in justifying such measures. Nonetheless, this should not imply a laissez-faire approach to governance. The statistics from the National Crime Records Bureau (NCRB) clearly illustrate a sharp rise in cybercrimes in India from year to year.[3]

Statics on dark web

State/UT-wise details of cases registered under cyber-crimes (involving communication devices as medium/target) for last three years

Sl. no	**State/UT**	**2020**	**2021**	**2022**
1	Andhra Pradesh	1899	1875	2341
2	Arunachal Pradesh	30	47	14
3	Assam	3530	4846	1733
4	Bihar	1512	1413	1621
5	Chhattisgarh	297	352	439
6	Goa	40	36	90
7	Gujarat	1283	1536	1417
8	Haryana	656	622	681
9	Himachal Pradesh	98	70	77
10	Jharkhand	1204	953	967
11	Karnataka	10741	8136	12556
12	Kerala	426	626	773
13	Madhya Pradesh	699	589	826

[3] cyberblogindia.in

14	Maharashtra	5496	5562	8249
15	Manipur	79	67	18
16	Meghalaya	142	107	75
17	Mizoram	13	30	1
18	Nagaland #	8	8	4
19	Odisha	1931	2037	1983
20	Punjab	378	551	697
21	Rajasthan	1354	1504	1833
22	Sikkim	0	0	26
23	Tamil Nadu	782	1076	2082
24	Telangana	5024	10303	15297
25	Tripura	34	24	30
26	Uttar Pradesh	11097	8829	10117
27	Uttarakhand	243	718	559
28	West Bengal	712	513	401
	TOTAL STATE(S)	**49708**	**52430**	**64907**
29	A&N Islands	5	8	28
30	Chandigarh	17	15	27
31	D&N Haveli and Daman & Diu	3	5	5
32	Delhi	168	356	685
33	Jammu & Kashmir	120	154	173
34	Ladakh	1	5	3
35	Lakshadweep	3	1	1
36	Puducherry	10	0	64
	TOTAL UT(S)	**327**	**544**	**986**

	TOTAL (ALL INDIA)	**50035**	**52974**	**65893**

Source: Crime in India published by NCRB.

Web-based onion services

In January 2015	
Category	**Percentage**
Gambling	0.4
Gun	1.4
Chat	2.2
New (not yet indexed)	2.2
Abuse	2.2
Books	2.5
Directory	2.5
Blog	2.75
Porn	2.75
Hosting	3.5
Hacking	4.25
Search	4.25
Anonymity	4.5
Forum	4.75
Counterfeit	5.2
Whistleblower	5.2

Wiki	5.2
Mail	5.7
Bitcoin	6.2
Fraud	9
Market	9
Drugs	15.4

- According to recent data, India has the largest user base on the dark web compared to Australia and South America. In fact, approximately 26% of all dark web users are located in India.

- According to ZDNet, a hacking group referred to as ShinyHunters made an attempt to sell the personal data of 73 million users on the dark web. This group successfully breached the security of approximately ten organizations, including well-known platforms such as the online dating app Zoosk, the printing service Chatbooks, and the South Korean fashion platform Social Share. The breach of these organizations potentially jeopardized the personal information of their users and customers.

- In April 2020, a cybersecurity firm, Cyble, reported that approximately 500,000 Zoom accounts were compromised and sold for a very low price, less than one rupee each.

- Research conducted by Arxiv indicates that approximately 70.6% of individuals using the dark web are male, while only 29.4% are female. These findings shed light on the gender distribution within the dark web user community.[4]

- In March 2012, a notorious Russian hacker named Yevgeniy Nikulin, along with three collaborators, orchestrated a sophisticated cyber attack to illicitly obtain passwords for a staggering 117 million email addresses from the renowned social media platform LinkedIn. Following their nefarious act, the perpetrators shamelessly offered the

[4] blog.ipleaders.in

exfiltrated data for sale on the clandestine corners of the internet known as the dark web[5].

- Then, in July 2016, a chilling revelation surfaced as a cache of approximately 200 million passwords belonging to Yahoo! accounts emerged in a similarly dubious marketplace, casting a dark shadow over the cyber security landscape.

- In 2013, Edward Snowden, a former contractor for the U.S. National Security Agency (NSA), exposed the extensive government surveillance practices that raised concern. To facilitate the release of 1.5 million classified government documents to journalists, Snowden employed Tor, an anonymity network. The publicity surrounding Snowden's actions resulted in a substantial surge of global interest in Tor, prompting a swift expansion of the network's user base.

According to the Arxiv, when looking at the category-wise statistics, we can summarize it as follows based on the table.[6]

Category Group	**Percentage of users using the dark web**
18-25	35.9%
26-35	34.8%
36-45	16.8%
46-55	8.8%
56-65	3.1%
Above 65's	0.6%

Legality of dark web in India

The dark web is not a safe place to surf on. While some sites may be legitimate, there is still a danger. It's important to understand the legality of accessing the dark web in India in detail. It's important to understand that the legality of the dark web is contingent upon its usage. It's

[5] www.britannica.com
[6] Dark web - Wikipedia

essential to recognize the fine line between 'legal' and 'illegal' activities when engaging with the dark web.

In India, simply accessing the dark web is not against the law. However, the actions carried out on the dark web could potentially breach different laws, including the Information Technology Act, 2000, and the Indian Penal Code. There have been arguments that the dark web upholds essential civil liberties such as free speech, privacy, and anonymity, which are protected under Article 19 and 21 of the Indian Constitution.

Article 19(1)(a) of the constitution guarantees all citizens the fundamental right to freedom of speech and expression. This right is considered the cornerstone of a democratic society, enabling individuals to articulate their thoughts and opinions without the fear of censorship or retaliation. It plays a crucial role in fostering an open and informed citizenry, thereby contributing positively to the growth and progress of the nation. However, it's essential to acknowledge that under article 19(2), reasonable restrictions can be imposed on this right to prevent its abuse and to uphold the rights of others.

Moving on to Article 21, which enshrines the right to privacy, it safeguards an individual's right to solitude and to keep personal matters and relationships confidential. While the right to privacy is paramount in a modern democracy, it's not absolute. Certain exceptions and reasonable restrictions can apply to this right, particularly in cases related to decency or morality, contempt of court, or incitement of an offense, where the greater good of society is at stake.

What activities are illegal when using the dark web?

- Child pornography is a serious crime punishable under Section 67(B) of the Information Technology Act, 2000 and Section 14 and 15 of POCSO Act, 2012. These are the sections that exclusively deal with the crimes of pornography related to children.

- Apart from this, the Indian Penal Code, 1860 describes the provisions for offences committed against minor girls. Section 366(A) deals with inducing, forcing, and seducing a minor girl for illicit intercourse shall be liable for imprisonment of 10 years and may also be liable to pay a fine.

- Section 372 and 373 of the Indian Penal Code deals with the buying and selling of girls

for prostitution. We have seen such kinds of illegal activities taking place. They directly or indirectly come under the ambit of human trafficking. Human trafficking is illegal.

- A lot of illegal activities related to child pornography are committed on the dark web. If you are traced promoting such actions, then you considerably land yourself in trouble. Apart from child pornography, buying guns and drugs, promoting illicit material is illegal.

- Under Section 24 of the Narcotics Drugs and Psychotropic Substances Act, 1985, whosoever engages in dealing with narcotic drugs outside India is liable to be punished under this Act. Now, suppose a person engages in external dealing in drugs on the dark web, then that would certainly be punishable even if the dark web is not illegal but the activity that you commit is illegal. Refer back to the case where five students were arrested while indulging in buying LSD dots drugs.

Loopholes of dark web

The legal framework in our country has several loopholes, particularly when it comes to addressing the challenges posed by the dark web. The Information Technology Act, 2000, which deals with cybercrimes in India, only contains six sections related to this issue.

It's crucial to understand that the dark web should not be accessed casually, as a single click can have serious legal ramifications. An article published by the Indian Express shed light on an incident where five students from Mumbai were apprehended for engaging in the purchase of drugs via the dark web. These students were found to have acquired 1,400 LSD dots valued at 70 lakhs.

A friend in the US, who was a member of a dark web syndicate, arranged for a cartel from a western European country to deliver LSD dots to an address in Mumbai. After the parcels were delivered, five students were arrested by the Mumbai DCP (Anti Narcotics Cell) Shivdeep Lande. According to Lande, making such arrests is challenging due to the intricate structure and high level of anonymity provided by the dark web, making it difficult to trace the criminals.

"In the case of the activists arrested by the Pune police, the authorities allege that they were affiliated with the banned CPI (Maoist) and used the dark web for communication. Similarly, in the Cosmos Bank fraud, a whopping Rs 94 crore was illicitly transferred with the aid of the

dark web. Internationally, the dark web is notorious for facilitating drug trafficking, child pornography, illegal arms trade, and the illicit purchase of login credentials for popular streaming services like Netflix. The use of the dark web presents unique challenges for law enforcement agencies in India, highlighting gaps in the country's cybercrime laws."

Better late than never

Changes required in India to prevent exploitation of dark web

In India, there are currently no specific laws or provisions dedicated to VPN usage. However, it's important to note that the legal and regulatory landscape surrounding VPN usage is subject to change. In contrast, some countries such as Iraq, Turkmenistan, and Belarus have implemented complete bans on VPN services, making it illegal to use them. Additionally, in the United Arab Emirates (UAE), Russia, and China, access to VPN services is heavily restricted. In the UAE, only banks and similar organizations are permitted to use VPN, and there are stringent limitations on personal use. In the cases of China and Russia, only government-approved VPN services are allowed, undermining the very purpose of using a VPN for privacy and security. It's essential to stay updated on the regulations and restrictions surrounding VPN usage.

We propose that India consider implementing a system to regulate the use of VPN services by potentially banning freely available and unregulated VPN services. Instead, the government could establish an authority for mandatory registration of VPN service providers, which would fall under *Chapter VI of the Information Technology Act, 2000.* Given the existing number of authorities, it is also recommended that a sub-committee be formed within an established statutory body.

Remembering the following text this research suggests:

When evaluating internet service providers (ISPs), it is crucial to assess whether they are taking adequate measures to identify and report suspicious user activity to the appropriate authorities. One potential strategy could involve mandating ISPs to create specialized teams responsible for detecting and containing potentially harmful user behavior. These teams would then be able to produce comprehensive reports based on their findings. It is important to stress the need to safeguard user privacy throughout this process, with only IP addresses being disclosed in the

reports.

As per our discussion, the report generated can be shared with a designated government or law enforcement unit. They can then conduct surveillance on the flagged users for a specific period. In cases where a user is using a VPN service, the government may request the service provider to decrypt the user's activities under the provisions of Section 69 of the Information Technology Act, 2000. This section allows the government to issue directives for the interception, monitoring, or decryption of information through any computer resource. Depending on the severity of the offense, the user may face prosecution and be prohibited from using VPN services for a specific duration. We believe that implementing such policies, even in their basic form, will significantly strengthen India's stance against cybercrimes on the dark web.