DOI: *https://doij.org/10.10000/IJLMH.114745*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 2

2023

The Dark Web Ecosystem and the Risks It Poses to Women in Light of Contemporary Cyber Security Regulations

RIDDHI TRIPATHI[1] AND SURYA DUBEY[2]

ABSTRACT

The twenty first century is driven by extreme technological spurt. The saying that "The future is at the moment," often proves that all is conceivable, everything is reachable and everything is a click away, connotes a both positive and negative effect. But with great power comes great responsibility. The layers of the Internet go far beyond the content of the external access of our day-to-day browsing. As common netizens, we use and access barely five per cent of the entire internet, leaving the remaining a vulnerable ground of threats. Unimaginable crimes are committed daily on the Dark Web, ranging from leaking personal data to a market for human organs. The worst affected are women, they are trafficked like commodities; private pictures leaked on social media platforms, often blackmailed, as they are an easy target for activities emerging from the dark web. There have been several occurrences through the years that reported the abuse of this platform for steering criminal acts under the radar. However, the nature and extent of the Dark Web was only taken seriously after the infamous Silk Road case. In this paper, the authors attempt to examine the concepts and reality of Dark Web, the danger it possesses to women in general, further the issues related to the Security of Women on the platform, extending to an analysis digital law in existence and their relationship with the disturbing truths of the Dark Web.

Keywords: *Dark Web, TOR, Privacy, Anonymity, I2P, Women.*

I. INTRODUCTION

In terms of criminal services and activities, the dark web is a rising asset. Security Mechanisms should be on the lookout for these issues and take action to solve them, TOR and other Dark Web networks have given bad actors various opportunities to trade "goods" both legal and illegal anonymously. Law enforcement and policymakers now have a hurdle in successfully combating harmful actors operating in cyberspace due to the developing technology with encryption and anonymity.

[1] Author is an Advocate in India.

[2] Author is an Advocate in India.

The impact of the Dark Web, specifically its privacy and anonymity, is discussed in this paper. Through the results, it is shown how many daily anonymous users there are on this Internet segment for both the Kosovo region and the entire world, as well as how much of an impact hidden services websites have on the Dark Web. The search engines Ahimia and Onion City were used to get the results for this section (for the Dark Web). We have come to the conclusion that anonymity is not entirely verifiable on the Dark Web, despite TOR's

Three aspects, including anonymity, privacy, and the potential for non-detection, are offered by specialised browsers like TOR and I2P. This paper, explains and navigates about the impact of the Dark Web on many societal realms concerning especially women and provide our findings. The Internet and the web are frequently confused as synonyms. These are really two distinct names that share certain characteristics. The vast infrastructure of several networks is part of the Internet. By establishing a network in which any computer may speak with other computers so long as they are linked to the Internet, it makes it possible to connect a million computers[3].

The sites' publishers on the Dark Web are anonymous and hidden. Users are accessed on the Dark Web to share data with little risk and to be undetected. The access of users anonymously is essential for the Dark Web, which recently it is supported by the encryption tunnelling for monitoring protection. The Dark Web content is supported by the Onion Routing (TOR). It is anonymous network and access by the TOR browser. The TOR project was launched in 2002 by the US Naval Research laboratory to enable online anonymous.[4]

Another network on the Internet, the Invisible Internet Project (I2P), is used for encrypted user traffic, anonymous communication, and other purposes. It makes networked networks more reliable and durable.[5] Because there is little chance of user identification on the Dark Web, both legitimate and illicit activity has flourished amid the traffic on this part of the Internet. [6]

A Supreme Court lawyer and cyber security specialist named Karnika Seth thinks the accessibility of self-destructive email and proxies, which aid people in generating phoney IDs, makes it more difficult to prove a specific accusation. It is challenging to find people since their true identities are not revealed. Thus, it is necessary to alter both the Indian Evidence Act of 1872 and the Information Technology Act of 2000[7].

[3] Chertoff, M. and Simon, T. (2015) The Impact of the Dark Web on Internet Gover, This report is available at: https://research.torproject.org/techreports/detector-2011-09-09.pdf.

[4] See, https://metrics.torproject.org/reproducible-metrics.html

[5] Ibid.

[6] Berghel, H. (2017) Which Is More Dangerous The Dark Web or the Deep State? Computer, IEEE Computer Society, 50, 86-91. https://doi.org/10.1109/MC.2017.215

[7] The dark web and how police deal with it, Mohamed Thaver, Mumbai, Updated: September 17, 2018, Indian Express

Vicky Shah, a specialist in cyber law, contends that rather than lagging behind the demand for additional legislation, we should have educated police who are knowledgeable about evolving digital developments.[8]

II. LAYERS OF THE INTERNET

The Surface Web

It is what user's access in their regular day-to-day activity. It is available to the general public using standard search engines and can be accessed using standard web browsers that do not require any special configuration, such as Mozilla Firefox, Microsoft's Internet Explorer or Edge, and Google Chrome.[9]

The Deep web

It refers to anything on the internet that is not indexed by and, therefore, accessible via a search engine like Google. Deep web content includes anything behind a pay wall or requires sign-in credentials. It also includes any content that its owners have blocked web crawlers from indexing. Medical records, fee-based content, membership websites, and confidential corporate web pages are just a few examples of what makes up the deep web. Estimates place the size of the deep web at between 96% and 99% of the internet. Only a tiny portion of the internet is accessible through a standard web browser generally known as the "clear web".[10]

As said, typical search engines are unable to reach the Deep Web since their material is not indexed there. Unlike the Surface Web, where the information is "static and connected to other pages," this information is dynamic. It's practically hard to gauge the depth of the Deep Web, according to academics.[11] Although some early estimates placed the size of the Deep Web at 4,000–5,000 times that of the surface web, the Deep Web is expanding exponentially and at a rate that is incomprehensible. This is because of how information is retrieved and displayed.[12]

The Dark Web:

The dark web is a subset of the deep web that is intentionally hidden, requiring a specific browser Tor to access, as explained below. No one really knows the size of the dark web, but most estimates put it at around 5% of the total internet. Again, not all the dark web is used for

[8] Ibid.

[9] Election Security Spotlight – The Surface Web, Dark Web, and Deep Web, Center for Internet Security, Inc. (CIS®) https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-the-surface-web-dark-web-and-deep-web)

[10] What is the dark web? How to access it and what you'll find, THE STATE OF CYBERSECURITY, By Darren Guccione, CSO, 1 JULY 2021.

[11] Bright Planet, Deep Web: A Primer, http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/

[12] Ibid.

illicit purposes despite its ominous-sounding name.[13]

Via decentralised, anonymous nodes on various networks, such as Tor (short for The Onion Router) or I2P (Invisible Internet Project), one may access the Dark Web. The U.S. Naval Research Laboratory initially developed Tor as The Onion Routing project in 2002,[14] as a tool for online anonymity in communication. Users of Tor access webpages "via a sequence of hidden networks. Instead of creating a direct link, virtual tunnels allow people and organisations to communicate information via public networks without risking their privacy. [15]

In order to prevent the originator of the traffic from being identified, users route their web traffic through the machines of other users. In essence, Tor creates levels (much like an onion layer) and directs traffic via those layers to hide the user identity. Dark web websites also use a scrambled naming structure that creates URLs that are often impossible to remember. For example, a popular commerce site called Dream Market goes by the unintelligible address of "eajwlvm3z2lcca76.onion."

III. TRAVERSING THROUGH THE DEEP WEB AND DARK WEB

Visitors frequently use directories like the "Hidden Wiki," which classifies websites in a manner like to Wikipedia, to traverse Dark Web sites. People may use search engines to look up information on the Dark Web in addition to wikis. These search engines might be more specialised or they can be more general, scanning the Deep Web.

A more comprehensive search engine like Ahmia, for instance, "indexes, searches, and classifies material uploaded on Tor Hidden Services." URLs of websites alter while using Tor. Websites often have a "onion" suffix at the end of their domain names rather than ending in.com.org,.net, etc., indicating a "hidden service." [16]

There are other ways than Tor and comparable networks to access websites with concealed information. Some programmers have produced programmes, such Tor2web, that access to content hosted by Tor without having to download and install the Tor programme.[17] Nevertheless using bridges like Tor2web does not give users the same level of anonymity, as Tor does. As a result, users of Tor2web or other bridges might be identified by law authorities

[13] What is the dark web? How to access it and what you'll find, THE STATE OF CYBER SECURITY,By Darren Guccione, Contributor, CSO, 1 JULY 2021.

[14] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," Proceedings of the 13th USENIX Security Symposium, San Diego, CA, August 9-13, 2004, https://www.usenix.org/legacy/events/sec04/tech/full_papers/dingledine/dingledine.pdf.

[15] Tor Project, Tor: Overview, https://www.torproject.org/about/overview.html.en

[16] InfoSec Institute, Diving in the Deep Web, March 14, 2013, http://resources.infosecinstitute.com/diving-in-the-deepweb/

[17] Kim Zetter, "New Service Makes Tor Anonymized Content Available to All," Wired.com, December 12, 2008.

more quickly than those who use software like Tor if they browse websites that hold illicit content, such those that house child pornography.

Process of sale on dark web

A major technological development that has contributed to the growth of the dark web Bitcoin, a crypto currency that enables two people to carry out a trustworthy transaction without knowing each other's identities, According to Privacy Affair's some of the prices for things that are regularly traded on the dark web are Mr as follows data by[18]

- Cloned credit card with PIN: $25 to $35
- Credit card details with account balance up to $5,000: $240
- Stolen online banking logins with at least $2,000 in the account: $120
- PayPal transfers from stolen accounts: $50 to $340
- Hacked Coin base verified account: $610
- Hacked social media account: $1 to $60
- Hacked Gmail account: $80
- Hacked eBay account with good reputation: $1,000[19]

IV. Legal issues with regulation of dark web

The legality of accessing the dark web in India presents particular difficulties for law enforcement agencies. According to NordVPN online marketplaces are selling 5 million internet users' stolen data, 600,000 of these people are from India, making it the nation most severely impacted. [20]

But nonetheless not all that exists on the dark web is unlawful; there's additionally a legal aspect to it. For instance, you may sign up for a "chess club" or "Black Book," a social network branded "the Facebook of Tor." Discussing of browsing the dark web legally from India, it must be noted that there aren't any explicit rules that forbid users from doing so. Although most of these websites don't have names that are legible, so you can't really tell what's on them or where they can go, it can also be deemed unlawful since you could inadvertently get into troubles.

Whereas the dark web is not prohibited, you have assumed accurately so far that it is not lawful.

[18] Dark Web Price Index 2021) Dark Web Price Index 2021By Zachary Ignoffo . 10 December 2022, https://www.privacyaffairs.com/dark-web-price-index-2021/

[19] Ibid.

[20] Data of 600,000 internet users in India being sold on Dark Web via bots: What are they and how they operate, TIMESOFINDIA.COM / Dec 8, 2022

Also, it isn't entirely legal. You might go to jail for a variety of causes, including the procurement of weapons such firearms, handguns, and weapons as well as the usage of narcotics. I'll provide a simple illustration to make a case for this. Realize from once that using the dark web is legal. Yet, you risk going to jail. A person's activities or intentions are taken into account when surfing the dark web. It simply affects whether you will face legal repercussions or if you may freely utilise it without incident.[21]

Criminal conduct can take place on the Deep Web and Dark Web just like it can on the Surface Web. Cyberspace is used by a variety of bad actors, including terrorists, criminals, and state-sponsored espionage. The internet may be a venue for discussion, planning, and action. In particular, they might utilize the Dark Web to facilitate their actions and lower the danger of being discovered. [22]

Although the focus of this section is on cybercriminals, the challenges discussed are undoubtedly relevant to other types of bad actors. Criminals operating in the twenty-first century increasingly rely on the Internet and cutting-edge technologies.

For instance, criminals may readily use the Internet to commit classic crimes like trafficking in sex and illegal substances.[23]

(A) Jurisdictional Border Issues

Physical Limits- Between nations, states, and other places, jurisdictional lines have been created for law enforcement purposes. Several law enforcement authorities have been given the right to dispense justice inside certain boundaries. When crimes transcend jurisdictional lines, one organization's control over criminal prosecution may no longer be absolute, and laws may not be uniformly applied.[24] These phenomena have long been recognised and used by criminals.

Thus, Boundaries between the physical and digital worlds are non-existent in the virtual world; the boundaries are not necessarily as distinct as they are in the actual world. Along with helping legal businesses expand, high-speed Internet connectivity has also given criminals a more advantageous operating environment where they can quickly take advantage of their victims.

The million dollar question that needs to be addressed is that, Do such illicit users of the illegal means require only the Dark Web to carry out their actions and exactly what they might be

[21] Is the Dark web Illegal in India: A Comprehensive Study Purbita Mazumdara.

[22] Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement, by Kristin Finklea and Catherine A. Theohary.

[23] Ibid.

[24] Daniel C. Richman, "The Changing Boundaries Between Federal and Local Law Enforcement," Boundary Changes in Criminal Justice Organizations, http://www.ncjrs.gov/criminal_justice2000/vol_2/02d2.pdf.

gaining from such abuse of technology? There are benefits and drawbacks both of them depending on the Dark Web's anonymity. The additional anonymity provided by the Dark Web may help criminals selling illegal items by improving their ability to elude law enforcement.

Yet they could have more problems attracting customers. In their analysis of the Dark Web, Trend Micro argues that "sellers suffer from lack of reputation brought on by greater anonymity. Being untraceable might have negative effects for a seller since they find it difficult to build confidence with their clients unless the market supports it.[25] In other words, if one is trying to sell things online and has not been verified, anonymity might be a hurdle.

(B) Payment on the Dark Web

The money that is frequently utilised in Dark Web transactions is bitcoin.[26] Of note, a number of digital currencies exist, though Bitcoin is the most prominent. These currencies include Ripple and Litecoin, among others.[27] It is a decentralised digital currency that conducts transactions between users with confidence.[28] People typically acquire bitcoins by "mining" them, receiving them as payment, or trading them for fiat money. Transactions are verified using the address for the transaction and a cryptographic signature.[29]

The use of bitcoin has increased privacy since the wallet and private key are not visible in the public ledger. There is no publicly available database of these digital transactions and hence such payments are not under scrutiny from legal monetization channels leading to flourishing payment gateways for illegal activities.

(C) Derailing by the Law Enforcement

Law enforcement can use the Dark Web's anonymity just like criminals can. It may make advantage of this to run internet sting operations, surveillance, and tip lines. According to reports, law enforcement has also been collaborating with businesses to create new technology to look into crimes and locate victims on the Dark Web.

They may use on more conventional crime fighting strategies in addition to creating technology to penetrate and deanonymize services like Tor; others have claimed that law enforcement may still rely on mistakes made by criminals or vulnerabilities in technology to target malicious actors.

[25] Vincenzo Ciancaglini, Marco Balduzzi, and Max Goncharov, Deepweb and Cybercrime: It's Not All About TOR, Trend Micro, 15 June 2019.
[26] Pierluigi Paganini, "What is the Deep Web? A First Trip Into the Abyss," Security Affairs, May 24, 2012
[27] See https://coinmarketcap.com/
[28] Timothy Lee, "12 Questions About Bitcoin You Were Too Embarrassed To Ask," The Washington Post, November 19, 2013
[29] See, https://bitcoin.org/en/ vocabulary/

As an example, in one of the most famous cases that brought the dark web in the main front media was when the FBI shut down Silk Road in 2013, which was at the time the "biggest criminal market in the cyber underworld.[30] According to reports, "mistakes" by the site's administrator were what ultimately caused it to shut down. Some people theorise that "federal agents discovered weaknesses in the computer code used to operate the Silk Road website and exploited those weaknesses to hack the servers and force them to reveal their unique identifying addresses. The servers might then be found by federal investigators, who could then request that local law police confiscate them. [31]

V. CYBER LAWS AND DARK WEB SECURITIES FOR WOMEN

Article 21 of the Indian Constitution grants citizens the Right to access the Internet. The Supreme Court has recognized this right as a fundamental one, essential for the exercise of freedom of speech and expression. Cyber security is important for everyone, including women who may be more vulnerable to online threats.

In many countries, there are specific laws and regulations that protect women from online harassment and abuse. For example, the Indian government has launched the Cyber Crime Prevention Against Women and Children (CCPWC) initiative to address online crimes against women and children.

The legality of accessing the dark web in India presents particular difficulties for law enforcement agencies, given the absence of stringent laws governing cyberspace in the country. The loopholes in the existing laws compound the unique challenges posed by the dark web.

Prohibition of dark web activities under Indian legislation:

According to Section 67(B)[32] and Sections 14 and Section 15[33], child pornography is a severe offence that carries harsh penalties. These are the only parts that address the crimes of pornography involving children.

In addition, the Indian Penal Code, 1860, outlines the punishments for crimes against young females. According to Section 366(A)[34], anybody found guilty of coercing, persuading, or enticing an underage girl to engage in sexual activity is subject to a 10-year jail sentence as well as a possible fine.

[30] Donna Leinwand Leger, "How FBI Brought Down Cyber-Underworld Site Silk Road," USA Today, May 15, 2014

[31] Ibid.

[32] The Information Technology Act of 2000

[33] The POCSO Act of 2012

[34] Indian Penal Code, 1860

Sections 372 and Section 373[35] address the purchase and selling of females for prostitution. Several types of illicit activity have been observed. They are included in the scope of human trafficking, either directly or indirectly.

On the dark web, there are many unlawful practises relating to child pornography. If you are discovered encouraging such behaviour, you might find yourself in serious difficulty. In addition to child pornography, selling criminal materials is prohibited, as is purchasing weapons and narcotics.

Anyone deals in narcotic drugs outside of India is subject to punishment under this Act, according to Section 24[36]. Now, if someone were to participate in external drug selling on the dark web that would undoubtedly be unlawful even if the dark web was legal but the behaviour was not.

In India, the Information Technology (IT) Act, of 2000 is the primary legislation that deals with cybercrime and related offenses. The Act was amended in 2008 to include new provisions for dealing with cybercrime, including those related to the dark web. Some of the key provisions of the IT Act that relate to the dark web include:

- Section 66F: This section deals with cyber terrorism and provides punishment for anyone who accesses a computer resource with the intent to commit a terrorist act. The punishment can be imprisonment for life or a term of up to 10 years, along with a fine.
- Section 67: This section deals with publishing or transmitting obscene material in electronic form. It provides for punishment for anyone who publishes or transmits such material, which can include content found on the dark web. A penalty of a maximum of three years in prison and a fine may be imposed.
- Section 69: This section deals with the interception and monitoring of computer systems. It allows the government to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary for national security or for investigating cybercrime.

Overall, the IT Act provides a framework for dealing with cybercrime in India, including those related to the dark web. It is important for individuals to be aware of these provisions and to take steps to protect themselves from online threats.

VI. Conclusion & suggestions

[35] Ibid

[36] The Narcotics Drugs and Psychotropic Substances Act, 1985

The violence against women and girls on the internet, through the dark web and social media has not received enough attention. The majority of domestic legislation that has been established in this regard nonetheless has common flaws. Some nations only partially address the problem through the eyes of children's rights and Internet safety, while others just pay attention to particular types of cyber violence. Instead of placing it in the context of a continuum of violence affecting women and girls in all spheres of life and failing to capture other effects of such acts, such as the social, economic, psychological, and participatory harm, the recognition and sanctioning of the harm perpetrated against women and girls online mainly focuses on protecting the person's safety, reputation, or property.

Furthermore, the relevant players in the judicial system and other professional groups, such as the medical industry and teachers, who lack adequate training, are not sufficiently aware of the extent of the issue. Additionally, law enforcement authorities do not always have access to the specialized knowledge and technological means needed to ensure the collection of evidence. Law enforcement officials frequently downplay the threat posed by online threats and occasionally choose not to look into them. The removal of offensive content from websites and social media platforms is not always successful. These sites shouldn't be locations where internet abuse spreads unchecked. Additionally, private businesses need to do more to fight these internet campaigns to silence women. combating the online component of violence against women and girls requires systematic and comprehensive responses from all actors involved.

The dark web is a place where crimes against women are more common. The absence of control and regulation on the dark web is one of these factors. Because of this, it is simpler for criminals to engage in unlawful behaviour without worrying about being detected or penalized.

Educating women about the hazards and perils of using the internet is one strategy to aid in the prevention of crime against women on the dark web. Women should exercise caution when disclosing personal information online and should refrain from opening attachments or clicking on links coming from unidentified websites.

The anonymity offered by the dark web is another factor. Criminals can percolate using aliases and conceal their identities using encryption, making it difficult for law enforcement authorities to find them.

Additionally, the main contributors to crimes against women on the dark web include poverty, illiteracy, and gender inequity. Due to these considerations, human trafficking and other forms of exploitation are more likely to target women who are weak.

Impunity has fatal consequences. It encourages abusers to do more harm by sending the message that women and girls can be abused online without suffering any repercussions from the law. As a result of impunity, women and girls lose faith in the national authorities and stop reporting threats and acts of violence against them because they don't believe they will receive appropriate support or because they are afraid of being judged and re-victimized.

The world needs to hear the powerful voices of women and girls. We all women and men have a responsibility to thwart attempts to drag them back into a silence-based culture. We require stronger, fearless voices to speak up and demand change. Science is required to address the digital aspect of violence at the same rate as innovation. As a result of new technologies, violence against women and girls will certainly take on various new forms. We must act quickly. Preparation and quick action are the only protection against the vices of the dark web.

*****