CYBER LAWS FOR DARK WEB: AN ANALYSIS OF THE RANGE OF CRIMES AND THE LEVEL OF EFFECTIVENESS OF LAW OVER IT

Written by **Sanidhya Mahendra**

5th Year B.A.LL.B.(Hons.) Student, Uttaranchal University, Dehradun, India

ABSTRACT

In the 21st century, when we say "The future is now", we mean that everything is possible, everything is accessible, everything is on our fingertips. This is because our entire world today is connected and controlled by the internet. This world wide connectivity offers us everything to use, like from shopping to travelling, from eating to feeding, and even for connecting to the people virtually, however the internet is not just limited to the millions of websites available for our daily use, rather it is far beyond that. We just access the 5 per cent of the entire internet and the rest of it is what may be a true horror for those who have been affected by it. This domain of internet is popularly known as the Dark Web. In this article the author has described the disturbing truths of the Dark Web. The author has described about its history and has pointed out the usage of the same by the criminals. The author further discusses the types of crime that are committed behind the veil of internet. The article thereafter defines the remedies available in various laws of India for the victims of cyber crimes. The author concludes the article with suggestions of improvement in the present laws.

KEYWORDS: Dark Net, Dark web, Deep Web, TOR, Onion, Cryptocurrency, privacy, anonymous, VPN, ARPANET, Crawlers, Silk Road, Phishing

INTRODUCTION

Today the most significant invention is the invention Internet, and it has taken the eyes of all the generation in one go. Internet is beneficial as it connects from one end of the world to the other. It brings all of us closer with just one click. Looking at the bigger picture like every other thing, it has all its advantages and disadvantages. If we primarily look into the various researches, it has been shown that Internet usage has been swiftly expanded in recent years.

Keeping in mind that Internet usage is increasing rapidly, people around are unaware of the deep Web and dark web present quietly. The part which can only be used with the help of special browsers. That part of the internet is kept out of reach of general public. This area of the internet is further divided into two groups. The deep web where majority of the passwords and user sensitive information of the websites and database of them are stored. The other part or the darker part known as Dark Web contains more severe contents.

The Dark Web came into the bigger picture after the Silk Road Incident. The combination of dark web and the currency used for it i.e. Cryptocurrency can even lead to hire murderer to murder someone. One can commit unimaginable crimes on the Dark Web. Some various examples are private photos, medical records, communication, shopping, banking, all the privacy at stake.

DARK WEB

A combination of websites encrypted and can't be arranged within standard programming and customary web crawlers like Google and Bing. Instead, they demand explicit programs for access like The Onion Network or all the more ordinarily TOR. The Dark Web, likewise called Darknet, comprises little networks like companion to-companion, distributed, and huge ones like TOR, I2P, which open organizations work. In TOR, the information is encoded in layers practically equivalent to the layers of an onion.

TOR, through encryption, keeps the characters and IP locations of individuals getting to the Dark Web untraceable. The TOR program ensures the client's personality by steering traffic through different IP areas and hand-off PCs. The visitor to a Dark website needs to utilize a similar encryption instrument as the webpage he needs to get to and realize where to discover the website, to type the URL and visit. Anybody can get destinations on the Dark Web, yet it is tricky to find out who is behind a website.

It is usually bewildered and utilized reciprocally with the Deep Web, which is a lot greater. Dark Web is a piece of the Deep Web. Yet, it likewise incorporates ordinary information concerning the report. It makes the right to security genuine. Just surfing on the Dark Web isn't unlawful, except if the illicit substance is gotten to. Email workers like SIGAINT, Proton Mail permit clients to send and get the mail without their area or personality being uncovered. Facebook has a variant of its website on the dark Web with the goal that it very well may be gotten to from nations like China and Iran where it is confined. The essential thought regarding this is the support of namelessness; for example, it's anything but a client's character and veiling IP addresses, making the area mysterious[i]

HISTORY OF DARK WEB

In 1969, the main message was sent between PCs associated with ARPANET, created by the Defense Advanced Research Projects Agency. Inside a couple of years, other cryptic networks show up close by ARPANET. During the 1980s, the normalization of the Web made the issue of storage of illicit data, and an answer came up as "data havens". Then, at that point, distributed data transmission came, which brought about decentralized data centers which could store unlawful documents and were secret phrase secured. In 2000, Freenet was created by Ian Clarke, a product that offered mysterious admittance to the darkest openings of the Web. In 2002, the U.S. Maritime Research Laboratory delivered TOR, a development that hid its clients' location and IP addresses. Initially made for government use, assurance of characters of American specialists working in suppressive nations like China, yet later on, came to be utilized by the everyday citizens. Wired magazine in 2005 assessed that about a large portion of 1,000,000 motion pictures was circulated on the Darknet ordinary. There was copyright encroachment of everything directly from Bollywood blockbusters to the Microsoft office. In January 2009, Satoshi Nakamoto acquainted the world with an untraceable type of digital money, Bitcoin. It right away got well known with individuals working on the Dark Web as it ensured obscurity. Silk Road, an online market for purchasing and selling medications on the Dark Web, became acclaimed in light of an article on a blog, and the worth of Bitcoin tripled. In 2013, Eric Eoin Marques, depicted by the Federal Bureau of Investigation to be "the biggest facilitator of kid pornography in the world", was captured. FBI closes down Silk Road and captures its designer, and about a month another online commercial center surfaces, Silk Road 2.0.

USES OF DARK WEB

An intelligent individual who craves to purchase illegal drugs won't look for them on the Surface Web. However, he will go to the Dark Web namelessly to secure his location and IP address. In like manner, the drug dealers would likewise not sell on the destinations, for example, Google, where they can be handily followed by law implementation.

People may impart through email, web talks or individual informing on the Dark Web. Clients explore the Dark Web through directories, for example, the "Covered up Wiki", where their classifications coordinate locales. It also tells which destinations are live and which dead and which ones are reliable.

It is utilized for sure just for criminal purposes. Informants use it, protection disapproved of residents just as by fear mongers, programmers, pedophiles, drug dealers. It is utilized to look after protection, sell unlawful merchandise, sell counterfeit visas and IDs, total deaths, discover programmers, and see kid erotic entertainment. It is its criminal side, for it is of worry to law authorization organizations and public arrangement creators.

Writers in vigorously blue-penciled nations like China utilize the profound Web to impart and trade data, with no dread of Government. The Dark Web gives them a road to get data out to the remainder of the world without censorship.

'Transfers' have been set up by TOR on PCs throughout the planet through which data passes. All traffic goes through at any rate three transfers before arriving at its objective. The last transfer is called exit relay.

Customary web crawlers utilize the way toward slithering. However, they don't assemble content from the Deep Web for reasons like unstructured, unlinked or transitory substance. The URL design is distinctive for the utilization of TOR. Rather than postfixes like .com, additions like '. onion' are utilized. It is used with the expectation of complimentary discourse, protection, namelessness.

TOR might be utilized for circumvention of censorship in nations where governments have forced guidelines. Political dissenters might likewise use it to conceal share theirs, simultaneously hiding their personalities. It is likewise utilized for delicate correspondences by people and organizations. Crooks fear-based oppressors just as state-supported covert agents may use it for coordination, post and activity. The Deep Web internet searcher for drugs is Grams.

It was seen through the examination of some instances that the ideal approach to crushing the online crooks might be customary law implementation, notwithstanding technology. Actual limits between the nations imply diverse requirement organizations. Yet, the Web has no limits, and when crimes on the web cross limits, law authorization offices of at least two nations became included, and the laws of various countries may not be steady. This irregularity in the rules of multiple countries is abused by the lawbreakers getting to TOR.

TYPES OF CRIMES THAT CAN BE COMMITTED THROUGH DARK WEB

1. Murder for Hire
2. Extortion
3. Blackmail
4. Illegal Drug Sales
5. Illegal Arm Sales
6. Sex Trafficking
7. Terrorism
8. Child Pornography

LAWS APPLICABLE FOR DIFFERENT OFFENCES COMMITTED

Section 75[ii]**:** Act to apply for an offence committed outer India: All the acts committed through the computer, computer network, computer sources, etc., outside India, Section 75 will be applied.

The section has a more extensive viewpoint, including cyber wrongdoing committed by cyber crooks of any nationality, any territoriality.

Hacking and Data Theft**:** Sections 43[iii] and 66[iv] of the IT Act punish various activities going from hacking into a Computer network, data burglary, presenting and spreading infections through Computer network, harming Computers or Computer network, or PC programs, disturbing any PC or PC framework or Computer network, denying an approved individual admittance to Computer network, harming or obliterating data living in a PC and so forth The punishment of the offence is the punishment of up to 3 (three) a long time or a fine of Rs. 5,00,000 (Rupees five lac) or both.

Receipt of taken property**:** Section 66B[v] of the IT Act recommends discipline for insincerely getting any seized Computer asset or specialized gadget. This segment necessitates that the individual getting the taken property should have done so deceptively or ought to be motivated to accept that it was taken property. Under Section 66B of the IT Act, this offence's discipline is the punishment of up to 3 (three) years imprisonment or a fine of up to Rs. 1,00,000 (Rupees one lac) or both.

Identity of crime and cheating by personation**:** Section 66C [vi] of the IT Act suggests punishment for identity robbery and gives that any individual who deceitfully or wrongfully utilizes the electronic mark, secret word or some other particular recognizable proof component of some other individual will be checked with the punishment of either depiction for a term which may reach out to 3 (three) year imprisonment and will moreover be responsible to fine which may stretch out to Rs. 1,00,000 (Rupees one lac).

Section 66D[vii] of the IT Act prescribes punishment for 'cheating by personation by utilizing Computer'. It gives that any individual who through any specialized gadget cheats by personation will be dismissed with the sentence of either a term which may reach out to 3 (three) years and will likewise be responsible to fine which may stretch out to Rs. 1,00,000 (Rupees one lac).

Obscenity**:** Sections 67[viii], 67A and 67B of the IT Act endorse punishment for distributing or transmitting, in electronic structure: (I) offensive material; (ii) material containing physically explicit demonstration, and so on; and (iii) material portraying kids in the physically explicit demonstration, and so forth separately. The discipline endorsed for an offence under segment 67 of the IT Act is, on the main conviction, detainment of either depiction for a term that may stretch out to 3 (three) years, to be joined by a fine that may reach out Rs. 5,00,000 (Rupees five lac), and in case of a second or resulting conviction, detainment of either depiction for a term that may reach out to 5 (five) years to be joined by a fine may stretch out to Rs. 10,00,000 (Rupees ten lac). The discipline endorsed for offences under areas 67A and 67B of the IT Act is on a first conviction, detainment of either depiction for a term that may stretch out to 5 (five) years, to be joined by a fine reach out Rs. 10,00,000 (Rupees ten lac) and in case of second or resulting conviction, detainment of either depiction for a term which may reach out to 7 (seven) years and with fine which may stretch out to Rs. 10,00,000 (Rupees ten lac).

***Section 43(h) of the IT Act*:** Section 43(h)[ix] read with area 66 of the IT Act punishes a person who charges the administrations benefited by an individual to someone else's record by altering or controlling any Computer or Computer Networks. An individual who changes the PC arrangement of an electricity provider and makes his Neighbour pay for his electricity utilization would fall under the area mentioned above 43(h) of the IT Act for which there is no identical arrangement in the IPC.

***Section 65 of the IT Act*:** Section 65[x] of the IT Act endorses punishment for messing with Computer source archives and gives that any individual who purposely or deliberately hides, annihilates or changes or purposefully or intentionally causes another to cover, obliterate, or adjust any Computer source code (for example a posting of projects, PC orders, plan and design and program examination in any structure) will be guilty with imprisonment for up to 3 (three) years or with a fine which may stretch out to Rs. 3,00,000 (Rupee's lac) or with both.

***Infringement of protection*:** Section 66E[xi] of the IT Act endorses punishment for breach of security and gives that any individual who deliberately or intentionally catches, distributes or transmits the picture of a private space of any individual without their consent, under conditions abusing the protection of that individual, will be rebuffed with imprisonment which may stretch out to 3 (three) years or with fine not surpassing Rs. 2,00,000 (Rupees two lac) or with both.

***Section 67C of the IT Act*:** Section 67C[xii] of the IT Act requires a 'representative' to save and hold such data as might be determined for such span and in such way and arrangement as the Central Government may endorse. The part further gives that any go-between who purposefully or intentionally negates this prerequisite will be given imprisonment for a term that may reach out to 3 (three) years and be obligated to a fine. A 'substitute' regarding a specific electronic record has been characterized in the IT Act to mean any individual who for someone else gets, stores, or transmits that record or offers any assistance concerning that record and incorporates telecom specialist co-ops, network specialist organizations, web access suppliers, web-facilitating specialist organizations, web search tools, online instalment sites, online-sell off-sites, online- commercial centers and cyber cafes.

***Cyber Terrorism*:** Section 66F[xiii] of the IT Act recommends punishment for illegal cyber threatening. Whoever, with a purpose to undermine the unity, integrity, security of India or to strike fear in individuals or any part of individuals, denies or makes the disavowal of access any individual approved to get to a Computer or endeavors to enter or get to a computer without authorization or surpassing approved admittance or presents or causes the presentation of any Computer, and through such lead causes or is probably going to make passing or wounds people or harm to or destruction of property or disturbs or realizing that it is probably going to cause damage or interruption of provisions or administrations vital for the existence of the community or antagonistically influence critical data foundation, is liable of 'cyber psychological oppression'. Whoever purposely or deliberately enters or gets to a system without authorization or surpassing approved admittance, and through such lead acquires admittance to data, data or PC database that is confined for explanations behind the security of the State or foreign relations, or any limited data, data or PC database, with motivations to accept that such data, data or PC database so got might be utilized to cause or prone to make injury the interests of the sway and integrity of India, the security of the State, amicable relations with unfamiliar States, public request, tolerability or morality, or comparable to the scorn of court, slander or incitement to an offence, or the benefit of any far off country, gathering of people or something else, is additionally liable of 'cyber terrorism''.

THE LEGALITY OF ACCESSING THE DARK WEB IN INDIA

It is not unlawful to get to Dark Web from India since TOR hides the IP address and location of the consumer. However, because of the location being covered up, it is difficult to know from which country a consumer is getting to the Dark Web, so the subject of the legitimateness of access in India won't emerge.

Simultaneously, it very well may be named as unlawful additionally since you may unintentionally fall into difficulty since a large portion of these web website doesn't have names which are comprehensible and consequently you don't have the foggiest idea what is there in it and where it could wind up with. However, it is recommended to avoid perusing such websites. Besides, you can be 100% detectable on the off chance that you are utilizing a famous VPN administration moreover. Protection programmers are amassing on the dark Web. Without much of a stretch, they can trace you on the off possibility that you are using Microsoft Windows, Unrooted Android or iOS. The main point here isn't to download a single thing from any website you find on the dark Web. You may likewise wind up in jail on the off chance that you attempt to purchase illicit arms, including unlawful seizing exercises, kid pornography, and so forth.

Likewise, there are websites on the dark Web showing horrendous pictures of dead bodies, torturing human bodies and living individuals. These pictures can make repulsiveness in your psyche, leaving you precarious for quite a long time or months. So, the dark Web illustrates to what degree individuals could turn sour, low or crumble themselves. Thus, this is something which neither you ought to investigate nor should you prescribe this to somebody.

CONCLUSION

Internet is perhaps the primary creations of the century, and the number of individuals getting to it is constantly expanding. The Web, a great many people know, comprises just 4 of the Web and is known as the Surface Web. If the Web is an iceberg, the Deep Web would be beneath the waterline, and it establishes around 90% of the Web with data sets like Westlaw and Lexis Nexis. The Dark Web, underneath the Deep Web, incorporates drug dealing, TOR encoded locales, unlawful data, and so forth and comprises around 4% of the Web. The Dark Web is an assortment of scrambled websites that can't be gotten through traditional web crawlers. It requires explicit programs for access like The Onion Network, wherein the information is encoded in layers practically equivalent to the layers of an onion. When an individual uses Dark Web, his location and IP address can't be followed[xiv]. It is utilized for legitimate just as criminal purposes. Informants could utilize it, protection disapproved of residents just as by fear mongers, programmers, pedophiles, drug dealers. It's anything but unlawful to get to the

Dark Web from India since TOR conceals the IP address and location of the client. Since the location being covered up, it's anything but conceivable to know from which country a client is getting to the Dark Web, so the topic of the lawfulness of access in India won't emerge. Like everything, Dark Web enjoys its benefits and weaknesses, and its utilization relies upon the client.

ENDNOTES

[i] https://blog.ipleaders.in/legality-dark-web-india/, Visited on 23rd June 2021.
[ii] Section 75, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[iii] Section 43, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[iv] Section 66, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[v] Section 66B, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[vi] Section 66C, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[vii] Section 66D, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[viii] Section 67, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[ix] Section 43(h), Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[x] Section 65, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[xi] Section 66E, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[xii] Section 67C, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[xiii] Section 66F, Information Technology Act, No. 21, Acts of Parliament, 2000 (India).
[xiv] https://blog.ipleaders.in/legality-dark-web-india/, Visited on 23rd June 2021.