

**DARK WEB: THE MISCALCULATED FIASCO AND FAILURE OF GOVERNMENT
TO THE CURB THE DIGITAL MENACE**

***PRIYA KOTWANI**

INTRODUCTION

Technology has expanded in every field imaginable. From brick phones to smart phones, cash to crypto currency, technology has evolved at a rapid pace. Only 15-20 years ago, computers were hardly affordable by families and today it has become sine qua non, particularly for primary education. However, as they say, *a double-edged sword cut both ways*, there is no doubt that technological advancement has also led to rise in cyber crimes. By becoming more and more massive these crimes are posing a serious threat to human life. Cyber crimes, generally includes hacking, cyber stalking, salami attacks, fraud, identity theft and many more. Further, in India we have Information Technology Act 2000, dealing with cyber crimes and electronic commerce. The act provides punishment for hacking, cheating using computer resources, publishing information which is obscene in electronic form etc.¹

The internet is colossal. Millions of websites, database, runs 24*7. The massive data on the web, has parts which are 'indexed' so that they may be found by users through search engines (Google, Bing, etc). And there are other parts of the web that aren't indexed, and therefore not easily available for public access, are known as the 'deep web'. This part was initially known as 'dark web', with the 'dark' being more an allusion to being kept away from the light of regular access than its now more nefarious association. It must be noted that it is near impossible to put a number to it, the estimates by unofficial mostly concur that the vast majority of the web is unindexed. Well, Internet can be imagined as an iceberg, where a small part of the ice is above the surface and is accessible to people every day like websites, images and videos but this forms just a small part of world web. Underneath the surface, the deep web makes up most of the internet. What happens under this surface? What kind of things a person can browse or sell? What's the reason of making these sites hidden from the eyes of people?

¹ Information Technology Act, S. 66,66D,67(2000).

USE OR MISUSE?

When someone speaks of *Deep web/Dark Web/Hidden Web* he/she thinks of a world characterized by the possibility to surf under some specific conditions. The dark web is only accessible by specific tools like tor (a software that gets you into the dark net). Generally, asking about dark web, a person shall be told that it is home to several nefarious things including buying and selling of drugs, child pornography, human trafficking and many more things that are illegal outside this surface. It must be noted that crime was never the primary use of dark net. Then why it was built? The Internet was originally funded by the department of defense. The dark web was just another tool used by governments to exchange documents secretly, for bank authorities to keep our credit card and other information safe, for journalists to bypass censorship of several states.

Therefore, the main purpose was never to increase crime but like any place where human beings congregate there is an activity which is not legal in the eyes of law. So is the dark web, where there is a black market where buying and selling of drugs takes place. The tool which was created for the security of government documents and general public of course has been misused nowadays. The increased popularity of dark webs only increased the illegal transactions taking place over there. In 2015, when Ross Ulbricht was sentenced to life imprisonment, did nothing but boosted the sale of drugs and other illegal weapons in the deep web market. A study by British Journal of Criminology provided some quantitative evidence showing that the dark web trade actually received a sales bump following the news of the arrest of creator of Silk Road. The Silk Road market that had been shut down at that time, gain so much popularity among the users that it got replaced, closed and again recreated with a different name. People were never discouraged from buying and selling of the drugs.

The saddest part is that there is no clear law in India for such trading. In our country, the transactions on the dark web belong to a legal grey area and are untraceable. Earlier, in 2017, a group of students got arrested in Hyderabad on charges of purchasing LSD on the dark web. Interestingly, the reason of their arrest was not because the transaction was made on the dark web; they were arrested because the use of LSD (also known as acid) is illegal under Indian law (Narcotic Drugs and Psychotropic Substances Act,1985).

A GLIMPSE AT BITCOIN

The crypto currency was first released in 2009- bitcoin. It was created by an unknown person or a group of people. The intention was to create a peer-to-peer electronic cash system that can be decentralized. Typically it is a type of digital currency which uses encryption techniques to regulate the generation of units of currency. The currency has a limited use, where economies like Japan and Russia have moved to legalize the use of Bitcoins, India has not recognized the crypto currency yet. Notably, there is no central authority to manage and loans out these coins. They are created through computer processing which also means that there is no central authority to issue 'clearing' for bitcoin transactions. This also means that it takes comparatively less time to transfer the currency. The ultimate is goal to keep our reserve coins in some type of wallet by using this alternative currency. And shop anywhere, bitcoins are accepted by using a unique ID.

Over the past few years the value of bitcoins has augmented so much that people have begun to invest on it as an asset. Though it was released in 2009 but it has gained a lot of popularity in past few years.

ANONYMITY WITH BITCOINS AND DEEP WEB

It appears from outside that these two topics probably do not have anything in common but bitcoins are the main source of transactions under the dark web. Yes!

The transactions in deep/dark web takes place through bitcoins, where your identity is untraceable. Bitcoin, is used on the dark web solely, for illicit purposes. It means that the popularity, investment and recognition to bitcoin can somehow increase the illegal trade in dark web. It is difficult to say that how things will turn out from this point but it's certain that the communities working over dark web has created some astounding system. Further, we cannot deny the fact that if the government has to regulate such market then, it is necessary that it recognizes the currency, only then it would be possible to keep a check on the activities and transactions taking place in a country.

Bedavyasa Mohanty, an Associate Fellow at Observer Research Foundation Cyber Initiative, says that there are Indian users transacting on the dark web using bitcoin and claims that this number is only likely to increase as accessibility increases. "Bitcoin cannot be tracked," says

Mohanty. “With the ledger and the blockchain, you can trace the trail of a certain bitcoin, but it is anonymised. You can’t point out who owns that bitcoin.” In nutshell, it can be said that number of transactions are made in dark web for n number of illegal activities using a currency which leaves no finger prints. Therefore, the dark web becomes more dangerous if combined with Bitcoins.

From the prospective of Indian law enforcement body, it is necessary to recognize the currency first, then, track down the owners and users of Bitcoins. Indeed, the chances of discovery are minimal, as the currency uses a system of public and private ‘keys’. But efforts could be made as country does not have any clear laws on crypto currency till now. It is the main currency used for trading purposes on dark web and the transactions are untraceable which makes people feel safe to do illegal trade activity.

ILLEGAL TRADE AND PROVISIONS IN INDIAN LAW

In India, The Narcotic Drug and Psychotropic Substances Act,1985 prohibits a person to manufacture, sell, purchase, possess, transport or store any Narcotic drug or psychotropic substances. It states that “No person shall—

(a) cultivate any coca plant or gather any portion of coca plant; or

(b) cultivate the opium poppy or any cannabis plant; or

(c) produce, manufacture, possess, sell, purchase, transport, warehouse, use, consume, import inter-State, export inter-State, import into India, export from India or tranship any narcotic drug or psychotropic substance, except for medical or scientific purposes and in the manner and to the extent provided by the provisions of this Act or the rules or orders made thereunder and in a case where any such provision, imposes any requirement by way of licence, permit or authorisation also in accordance with the terms and conditions of such licence, permit or authorisation: Provided that, and subject to the other provisions of this Act and the rules made thereunder, the prohibition against the cultivation of the cannabis plant for the production of ganja or the production, possession, use, consumption, purchase, sale, transport, warehousing, import inter-State and export inter-State of ganja for any purpose other than medical and scientific purpose shall take effect only from the date which the Central Government may, by notification in the

Official Gazette, specify in this behalf: 1[Provided further that nothing in this section shall apply to the export of poppy straw for decorative purposes.]²

The act further provides the powers of government to constitute any authority and punishment for the person found in possession, manufacturing or selling of the narcotic drug. It is the only act in India dealing with the narcotic drug and psychotropic substances. The act does provide for the offenders who are in possession of illicit substances but there is no provision under the act for buying and selling of such drugs on internet, specifically on Dark web. We might have heard few instances from last 2-3 years where people were arrested for buying and selling of drugs on the internet; for instances, if we take the example of that group of students who got arrested last year for purchasing LSD from dark web . Well, the reason of their arrest of not because the trading took place on dark web but because LSD is illegal under the above mentioned act.

Even under the Information Act 2000, there is no clear provision for such kind of trading. The IT Act deals with cyber bullying, hacking, cyber stalking, salami attacks, fraud etc and provides punishment for the same. But what about the illegal trading that is taking place on a daily basis at some place in the surface web which is note even traceable?

The number of offenders being arrested on such grounds is very less. Part of the problem is of course, that the Indian law does not recognizes the dark web as a separate entity from the surface web. There are thousands of active users from India itself, involved in illegal activities and nobody is there to stop them. The government is worried more about the economy of country, terrorism etc. They don't even think about what is growing out there on those chat rooms that is so immense and dangerous for the people and of course for the government as well.

The problem is not only the selling of drugs, dark web is full of such kind of illegal activities. Child pornography, illegal weapons and human trafficking; everything is so easy to browse on the dark web and there is no control over them. Buying a gun or cocaine has never been so easier, just by a click on mouse. How does commerce works on dark web? To access the dark web, a special browser is needed, like Tor browser. Users are the suppose to log in to these closed websites.

² The Narcotic Drug and Psychotropic Substances Act, S 8 (1985).

Once the order has been placed on the dark web portal, users are insisted on bitcoin payments to beat KYC norms which regulate ecommerce websites and further, ask for executing cross-border payments. And then, the delivery of goods takes place, complexity of which varies depending upon the good purchased. Things get a bit complicated when the trading is for arms and weapons, when such arms are to be shipped to abroad. So, the guns are disassembled into 5-8 pieces and then shipped separately. This is how commerce works over there. In a very smooth way just like normal shipping of anything we order from websites like Amazon or Jabong.

This is not enough, there is also a market for guidebooks on bomb making including some crude explosives. Even a person can hire someone for murder. One can easily find n number of discussions on Quora or yahoo on how to buy drugs from dark web or how to install tor and a lot more. This clearly indicates that the people of country are well aware of this kind of market and are keen to make transactions over there.

URGENCY TO MAKE AMENDMENTS IN EXISTING LAWS

The Narcotic Drug and Psychotropic Substances Act, 1985 is solely responsible for controlling and managing the manufacture, purchase, store, sell the illicit substances in country. The Indian Narcotics Control Bureau is official responsible for controlling the use of Narcotics in India. However, no legislation exists in India to control the illegal activities taking place over the deep dark web. There is no clear provisions dealing with such kind of activities and the result is, people are doing illegal trade on regular basis without any fear of the law and order.

Privacy is the basic feature of deep web. It was primarily designed to keep the privacy of individual. The deep web is used specifically by the government officials to keep the data and many records safe. A person cannot deny the fact that deep web is essential for the officials. Closed software like tor not only protects the government data but it also protects an individual's browsing activities just like they protect dark net sites like Silk Road. It also includes PGP and encrypted services that keep our emails and phone calls private. The desire for privacy on internet is becoming a big business now. We might have seen the changes on our Whatsapp or iMessages that are being encrypted now.

The Internet has become an essential element of our work culture. With the increasing use of technology, the dangers associated with it are also increasing. In such a situation, there is an urgent need of amendment in the existing laws. Over 30-40 years so many technological changes have been seen but the laws are still lagging behind. The IT Act 2000 is the only act dealing with cyber crimes which itself has many loopholes and therefore it does not fulfill the demand of present day situation.

BALANCE BETWEEN LAW AND TECHNOLOGY

In our families, we might have noticed that how clashes arises among the older and younger generations. There is lot of difference between thinking of both the generations; reason being the difference between the upbringing of both. So, for maintaining peace, both have to compromise and reach at consensus to further avoid clashes. Similar situation is with the law and technology. The development of science and technology has been immense. From last 30-40 years an individual has changed at so many levels. The work culture has developed so much. Type writer has been replaced by laptops and tabs, the use of internet has become so essential in work culture that people can't even think about working without these tools. The advancement also gave birth to dangers associated with it. The cyber crime rates have been increased which forced government to make separate laws dealing with crimes specifically taking place on the Internet and The Information Technology Act,2000 came into existence. At initial stage, the act was somehow beneficial but the level at which technology is mounting, there is a need to balance the provisions relating to such technology. A need to strike a balance between law and technology, they must go hand-in-hand, so that the crime rate can be decreased. Though, it is not humanly possible to take immediate actions and make provisions as it is a very lengthy procedure but efforts can be made to improve the situation. The government is more worried about the economy and other issues but this is an issue which cannot be ignored as it can pose a serious threat in future. The technology has gone so far and our laws are still lagging behind. The nationwide survey of cyber law indicates that there are only a few countries who have updated their laws in accordance with the present situation of their country. The cyber crimes have no longer confined to the developed countries alone, rather it has assumed a global dimension. The current legal techniques of investigating the crimes are inadequate. The problem is becoming more complex by each passing day as the technology is growing at a rapid pace.

The issue of illegal trading taking place at dark web is dangerous for society and therefore requires a separate provision dealing with the issue. But, the government at present has not even separated the deep web from surface web. Many police authorities are not even aware of such kind of criminal activity. It is evident from the above discussion that a clear cut edge between the two concepts has been faded away. Therefore, provisions related to such crimes and more accurate regulating authority is the need of this hour.

CONCLUSION

The emergence of new tech generation, the evolution of crypto-currency, the development of security tools has influenced the exponential growth of hidden drug market. The internet is getting vast by each passing day and therefore generating rapid change in the illicit drug market. This is also proving an accessible and efficient trade market for illegal activities. It is necessary to strike a balance between the law and technology. The traditional methods used by the authorities will not be sufficient to curb the issue. The policing techniques used by the law enforcement authorities are inadequate posing several challenges. The problems they face while handling such kinds of issues includes, location of servers their identity as the transactions are untraceable. The transactional nature of the deep web market pose very complex questions in mind while dealing with it, for instance; who will be responsible? The country where the server is located? Whether the police had adequate resources? The solution lies in answer to these questions which again is very complicated. In India, part of problem is that, the law enforcement body does not recognize dark web as a separate entity from the “surface” web, there are no special laws for it. It is necessary to make separate provisions for online illegal trading by amending the existing cyber laws. The Narcotic Drug and Psychotropic Substances Act, 1985 is solely responsible for controlling and managing the manufacture, purchase, store, sell the illicit substances in country. The Indian Narcotics Control Bureau is official responsible for controlling the use of Narcotics in India. Section 8 of the act deals with possession, selling , manufacturing or purchasing of narcotic drug but is not clear about how deal with cases falling under online trading of drugs. Therefore, there is a need to amend the act as well as per the needs of present day. Further, the transactions on dark web takes place through bitcoins, It has become the currency of choice in deep web market place. In a closed market, it increases the danger of physical exposure and arrest. It is important to control and regulate the transactions through

bitcoins by a separate authority in each country. In India, the crypto currency has not been recognized yet but people in the country are investing in the currency. It means that there is a possibility that no authority has been established to keep proper records of people using bitcoins specifically in dark web. Indian government must recognize the crypto currency first. And then shall appoint a committee that would be solely responsible for control and management of the affairs of bitcoins. It must also be noted that most of the police authorities in our country are not aware of such kind of trading. Awareness seminars for government authorities will also help in curbing the issue somehow. The skills and resources used by police officials must focus on high-level cyber crimes including weapon trafficking, cross-border cyber crime attacks, financial crimes. As outlined in a Computer's at Risk report by the US National Research Council from 1991 '*Tomorrow's terrorist may be able to do more with a keyboard than with a bomb.*³ The European Commission's efforts on cyber crime was indeed a laudable attempt as it laid down the guidelines to be followed by the member states on combating the cyber crimes. It further suggested the measures to be taken for restricting their cyber laws to meet the current needs of technological development. The convention also referred to the procedural aspects that must be considered while restructuring the existing laws as procedural aspect is one of the main hurdle in the cyber laws. It must be noted as every country follows different rules, some cyber crimes may not be the crime in different country. So, if a global approach is adopted; a uniform code or regulation dealing with all the cyber crimes might reduce the problems at a certain level. To curb this problem is not an easy task. It is not possible to eliminate the market in just one night. Therefore, the government must plan some strategies, prepare some short and long term goals and then work on it. For instance, the short-term goal could be creation of policy space to manage the dark web market rather than directly seeking to eliminate them. Longer term goals could be to re-evaluate the current system at both national and international level and including some penal provisions as well. At last, a sense of urgency is required towards the market that contains serious potential of destructing the peace in society.

³ D. Denning (2000) Cyberterrorism: The Logic Bomb versus the Truck Bomb', Global Dialogue. 2:4. *ibid.*