Effectiveness of Criminal Law in Tackling Cybercrime: A Critical Analysis
Ajoy P.B*1

1Research Scholar, National University of Advanced Legal Studies, Kochi, Kerala, India

DOI: 10.36348/sijlcj.2022.v05i02.005 | Received: 12.01.2022 | Accepted: 17.02.2022 | Published: 21.02.2022

*Corresponding author: Ajoy P.B
Research Scholar, National University of Advanced Legal Studies, Kochi, Kerala, India

Abstract
A significant number of nations around the world have enacted cybercrime laws for the purpose of controlling the occurrence of cybercrimes and mitigating its ill effects. However, in spite of enacting such cybercrime laws, available data show that the incidence of cybercrime is rapidly increasing. There are many factors that contribute to the failure of criminal law to fully control cybercrime. These factors include anonymity related issues, jurisdictional issues, extradition related challenges, problems associated with the law enforcement machinery, non-availability of data relating to cybercrime including non-reporting of cybercrimes, difficulties to identify, locate and arrest the cybercriminal, lack of experts, technology related issues, problems posed by international law etc. Since, at present, criminal law is not able to fully tackle cybercrime, there is a need to focus on cybercrime prevention strategies.

Keywords: Cybercrime, Extradition, Anonymity, Digital Evidence, Cybersecurity.

1. INTRODUCTION

Internet, as is known today, had its humble beginnings on 29th October 1969, when a message was sent over a leased telephone line from a computer located at the University of California at Santa Barbara, to a computer located at Stanford Research Institute covering about 350 miles (Kleinrock, 2010). Over the next half century, the internet grew in leaps and bounds and became a network of networks which is today made up of millions of computing/communicating devices which are interconnected together by means of various types of telecommunication systems (Froomkin, 2003). In 2018, which marks the 50th year of existence of internet, about 51.2% of the global population, which accounts to about 3.9 billion people had access to internet (International Telecommunication Union (ITU), 2018).

The explosive growth of internet has been of great benefit to mankind. Millions of people use the internet every day for a variety of purposes, like entertainment, social networking, learning, trading, etc. At the same time, a small percentage of internet users use internet for committing various forms of illegal activities/behaviour. Consequently, nation-states have enacted a number of cybercrime laws for curbing this illegal online activities/behaviour. However, these cybercrime legislations have not been able to effectively tackle cybercrime. This article seeks to identify some of the major factors that has rendered criminal law less effective in tackling cybercrime.

2. RESEARCH METHODOLOGY

Even though the writing of this article involved some amount of interdisciplinary research, the primary focus of the article is criminal law and criminology. Consequently, the primary method of research followed is doctrinal research. Secondary data has been used in this article and primary data has not been collected.

3. Cybercrime Statutes and Conventions

When cybercriminals began to extensively utilize the internet for committing various forms of deviant behavior like fraud, sale/distribution of child pornography, sale of guns/narcotics, causing damage to computer resources, etc.(Chawki et al., 2015), the nation-states around the world responded by criminalizing these deviant behaviors. For this purpose, they not only enacted criminal statutes but also entered into a number of cybercrime conventions. Some of the criminal statutes enacted are

(i) USA: Computer Fraud and Abuse Act, 1986.
The federal and state legislatures have also enacted several piece-meal legislations to deal with cybercrimes.

Published empirical studies point (Chawki et al., 2015) that the rapid rise in cybercrimes (Assarut, 2019) Also, a study published by Accenture Security in 2019, showed that there was a 50% increase in cyberattacks using mobile banking malware in the first half of 2019 compared to 2018 (Check Point Software Technologies Ltd., 2020).

Coming to India, the official statistics published by the NCRB (National Crimes Record Bureau) also show a significant rise in cybercrime with each passing year. India recorded 50,035 cases of cybercrimes in 2020 which represents a 11.85% increase of such crimes over the previous year. The rate of cybercrime (incidents/lakhs of population) in India also increased from 3.3% in 2019 to 3.7% in 2020 (National Crime Records Bureau, 2020). The following table illustrates the ever-increasing rate of cybercrime in India.

### Table 1: Total number of reported Cybercrimes in India (2011-2020)

<table>
<thead>
<tr>
<th>Year</th>
<th>No. of reported Cybercrimes</th>
<th>Increase over previous year</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>2213</td>
<td>-</td>
</tr>
<tr>
<td>2012</td>
<td>3477</td>
<td>57.12%</td>
</tr>
<tr>
<td>2013</td>
<td>5693</td>
<td>63.73%</td>
</tr>
<tr>
<td>2014</td>
<td>9622</td>
<td>69.01%</td>
</tr>
<tr>
<td>2015</td>
<td>11592</td>
<td>20.47%</td>
</tr>
<tr>
<td>2016</td>
<td>12317</td>
<td>6.25%</td>
</tr>
<tr>
<td>2017</td>
<td>21796</td>
<td>76.96%</td>
</tr>
<tr>
<td>2018</td>
<td>27248</td>
<td>25.01%</td>
</tr>
<tr>
<td>2019</td>
<td>44735</td>
<td>64.18%</td>
</tr>
<tr>
<td>2020</td>
<td>50,035</td>
<td>11.85%</td>
</tr>
</tbody>
</table>

The above quoted statistics clearly point to the fact that the incidence of cybercrime is rapidly increasing. This is happening, in spite of the fact, that nations across the world have enacted several cybercrime statutes. Consequently, through a process of logical reasoning it can state that criminal law has been ineffective to curb the surge of cybercrimes.

### 5. Factors/Challenges Inhibiting Criminal Law from Effectively Controlling Cybercrime

There are a large number of factors/challenges that inhibit criminal law from effectively tackling cybercrime. The most important of them are discussed below.

#### 5.1 Anonymity Related Factors

The technical features of internet enable criminals to commit cybercrimes in cyberspace anonymously without revealing their identity (Pont, 2001). The anonymity features of cyberspace are exploited by criminals to commit a wide variety of unlawful acts like fraud, sale or distribution of child pornography, sale of gems and narcotics etc. (Chawki et al., 2015). Many theories of cybercrimes including the Space Transition Theory developed by K Jaishankar suggest that anonymity is one of the most important factors responsible for rapid rise in cybercrimes (Jaishankar, 2007). People due to their social status and position do not indulge in crimes in the terrestrial space. However anonymity offered by cyberspace removes these restraints and they commit cybercrime (Assarut et al., 2019).

### 5.2 Jurisdictional Challenges

The world is currently organized on the principle of state sovereignty and independence within the territorial limits of a nation-state. This implies that each nation-state has the authority and jurisdiction to make and prescribe laws, enforce them and also adjudicate disputes arising out of the enactment and
enforcement of laws (Houck, 1986). Consequently, the criminal justice system developed by each nation-state is enforceable only within the territorial limits of that state.

Cyberspace is however not limited by the geographical borders of nation-states. Crime committed by criminals in cyberspace transcends nation-states and territorial boundaries. A cybercriminal sitting in the comforts of his home located in one country can commit a cybercrime, the effect of which could be felt in any other country in the world (Ajayi, 2016). When the victim of the cybercrime is located in another country, many complex issues relating to jurisdiction arises. The victim’s country would face a large number of legal and practical hurdles in enforcing its criminal laws against the perpetrator of the cybercrime.

5.3 Extradition Related Challenges

Extradition is a formal process by which a person usually accused of having committed an offence, is surrendered by one state to another state (Bassiouni, 2014). Relatively very few conventional crimes involve extradition as there is always some degree of physical proximity between the criminal and the victim (Chawki et al., 2015). However, that is not the situation so far as cybercrimes are concerned. Technologies associated with cyberspace enable a criminal to commit crimes at locations thousands of miles away from his location, at other jurisdictions (Brenner, 2004a). Consequently, relatively large number of cybercrimes are perpetrated across national borders. Hence extradition is a real issue in the enforcement of cyber-criminal laws.

Under the international law, there is no instrument or customary law that oblige a sovereign nation to automatically return criminals including cybercriminals for trial (Ajayi, 2016). Extradition is made possible through bilateral and multilateral treaties between nations. In the absence of such treaties, extradition is possible only by following the procedure prescribed in the national legislation of the country from where the extradition is sought. Such national legislations usually require the requesting state to approach a designated court/judicial tribunal. Either way, the extradition process is lengthy and cumbersome (Bassiouni, 2014).

5.4 Challenges Posed by the Existing Law Enforcement System

The current criminal investigation system/law enforcement system including the operational procedures has been evolved to deal with traditional crimes. The same system is now being employed to deal with cybercrimes and cybercriminals. However, the existing system is not able to tackle/deal with cybercrime as cybercrime does not possess many of the features of real-world conventional crime (Brenner, 2004b). For example, real world crimes are on most occasions one-to-one crimes due to its corporeal nature. (Jetha, 2013) However, there is no such assumption in case of cybercrimes. In fact, cybercriminals can multiply the number of times a cybercrime is committed in a given duration of time by using automation techniques. The traditional system of investigation/prosecution is not equipped to deal with crimes of such large scale and can very easily get overloaded (Brenner, 2004b).

5.5 Challenges in Apprehending the Cybercriminal

Experience of law enforcement officers reveal that apprehending a cybercriminal is not an easy task (Brenner, 2004a). The unique technical features of cyberspace enable criminals to hide their identity and physical location at the time of commission of offences (Pont, 2001). This anonymity makes it extremely difficult for law enforcements officials to trace the culprit. Additionally, the criminal may also make use of technology to assume the identity of an innocent person for the purpose of confusing investigators (Brenner, 2004a). Further, in case of cybercrimes there is no need of any physical proximity between the criminal and the victim. The nature of cyberspace is such that it allows a criminal located in one place to commit cyber-crimes like online fraud, intellectual property related offences, hate speech etc., the effect of which can be felt many thousand miles away (Brenner, 2004b). The lack of physical proximity between the cybercriminal and the victim as well as the huge physical distance between the place of investigation and the location of the cybercriminal has made it extremely difficult for law enforcement officers to apprehend the cybercriminal.

5.6 Factors Relating to the Scale of Commission of Cybercrimes

Technologies associated with cyberspace permits a large number of crimes to be perpetrated in an extremely short period of time. Further, many cybercrimes like online fraud can be automated enabling the cybercriminal to multiply by many times the number of cybercrimes that can be committed in a given period of time (Brenner, 2004a). Automation also permits the perpetrator to start the process of victimization and there after let the automated systems complete the process without any further involvement of the perpetrator (Brenner, 2004b). In this way, offenders can use technology to exponentially increase the number of cybercrimes that can be committed in a given period of time (Brenner, 2004a). The existing criminal justice system is not equipped to tackle such issues.

5.7 Factors Relating to the Nature of Evidence

Physical or tangible evidence, which is common in case of real-world crime, is rare in cybercrime prosecution. Since cybercrimes are committed in cyberspace which is a virtual environment, the evidence that is required to be presented in a court of law to secure the conviction of a
criminal is for most part intangible digital evidence (Brenner, 2004a). The collection of such evidence presents new challenges to investigating agencies which were hitherto accustomed to the collection of tangible evidence. Digital evidence is difficult to handle and can be easily altered or erased (Casey, 2011). Digital evidence is usually voluminous requiring investigators to spend substantial time processing the evidence to identify evidence which is relevant to the case (Brenner, 2004a). Presently, a large segment of the law enforcement officers is not trained to deal with digital evidence.

5.8 Factors Relating to Search and Seizure Procedures
Most of the cybercrime related laws enacted by nation-states around the world do not lay down any special procedure for search and seizure of digital evidence. Consequently, law enforcement officers rely on the traditional procedural law of search and seizure for collecting digital evidence. However, when the law that was evolved to address actions taken in physical world is extrapolated to deal with conduct that occurs in the cyberspace, numerous challenges arise (Brenner & Schwerha IV, 2002). For example, unlike real world physical evidence, digital evidence is extremely difficult to handle and can be easily corrupted (Casey, 2011). Consequently, digital evidence must be properly collected and preserved. This involves huge investments both in equipment and training of law enforcement personnel. Currently, most countries around the world are not in a position to make such huge investments.

5.9 Challenges Posed by the Lack of Effective Reporting and Dearth of Data
One reason that is significantly contributing to the difficulty in enforcing cybercrime laws is the lack of reporting of cybercrimes by victims particularly by businesses and corporates. The Commercial Victimization Survey (CVS) conducted in United Kingdom in 2013 is reported to have found that just 2% of online crime incidents were reported by businesses to law enforcement agencies. This was considerably lower in comparison to the reporting rates of other crimes like vehicle theft (100%), burglary (80%), etc. In case of general public, as well, the trend is no different. The Crime Survey for England and Wales (2007) reveal that only 1% of adult internet users reported hacking/authorized access to data.

The lack of effective reporting of cybercrime has resulted in the lack of sufficient data/statistics relating to cybercrime. Consequently, the public/businesses are not aware of the extend of cybercrime (Ajayi, 2016). Further, the non-availability of data regarding cybercrime has made it difficult for cybercrime law enforcement policy makers to draw up long-term plans for dealing with cybercrime.

5.10 Challenge Posed by the Lack of Effective/Adequate Legislation
The non-enactment of adequate cybercrime legislations by nation-states has also contributed to the failure of criminal law to tackle cybercrime. A study conducted in 2015 showed that only 79 of the 201 countries in the world have enacted cybercrime legislations. This implies that only about 40% of the countries in the world have enacted cybercrime laws. More importantly 47 of the 79 countries which enacted cybercrime laws are European nations (Ajayi, 2016). This alarming situation has helped cybercriminals escape prosecution by basing their illegal action in a safe haven country which has not enacted cybercrime laws (Goldstone & Shave, 1998). Further, the extradition of such a perpetrator is not possible due to the principle of double criminality, according to which extradition is permissible only if, the alleged deviant behavior is an offence in both the requesting state and the requested state (Williams, 1991).

5.11 Challenges Posed by the Lack of Experts in Prosecuting Cybercrimes
There are no special courts to try cybercrimes. The same criminal courts that deal with the trial of real-world crimes also conducts trial of cybercrime cases. Consequently, the prosecution of both real-world crime cases and cybercrimes cases are conducted by the same public prosecutor. The qualification to be appointed as a public prosecutor is usually a minimum prescribed period of practice of law. For example, in India an advocate with minimum seven years of practice can be appointed as a public prosecutor. No special technical qualification is prescribed. However, the prosecution of cybercrimes requires special skill and knowledge (Brenner & Schwerha IV, 2002). Consequently, ordinary prosecutors would find it difficult to conduct cybercrimes cases as they do not have expertise/knowledge regarding technical aspect of internet/information and communication technology. This is a serious handicap which is most likely to affect the conviction rate.

5.12 Challenges Posed by Ill-Equipped and Ill-Trained Law Enforcement Agencies
Investigation of cybercrimes involves the use of technology. Costly equipment and gadgets have to be used by the investigating agencies to trace cybercriminals. For this purpose, law enforcement officers have to properly trained in the use of technology and various equipment and gadgets. Only a few agencies like the FBI in USA have the financial resources to purchase costly gadgets and sufficiently train its workforce in the use of technology. However, due to lack of funds, vast majority of the law enforcement officers in most other countries around the world are not properly trained in the investigation of cybercrimes (Ajayi, 2016).
5.13 Challenges Posed by the Easy Availability of Devices/Tools and Access/ Instructions to Commit Cybercrime

An important reason for the failure of cybercrime statutes to control deviant behavior in cyberspace is the easy availability of technical devices like computers, hand-held devices, etc. necessary to commit cybercrime (Gercke, 2012). In the initial days of internet, a lot of technical knowledge was also required to commit cybercrimes (International Telecommunication Union (ITU), 2013). However, today specialized software tools which facilitates commission of cybercrimes are readily available. Consequently, the need of the cybercriminal possessing technical knowledge is greatly reduced (Gercke, 2012). Most of these specialized software tools not only help the cybercriminal commit cybercrime, but also helps him hide his identity. Most nation-states are yet to enact laws prohibiting the use of such specialized software. So long as technology is permitted to assist cybercriminals commit cybercrimes, there will always be a steady growth in cybercrime.

5.14 Challenges Due to the Limitations of International Law

The international law as it exists today is based on the concept of sovereignty of nation-states. Consequently, international law has no enforcement mechanism and it relies on the nation-states themselves for enforcement (Payandeh, 2010). Transnational cybercrimes are growing exponentially primarily due to the inability of international law to deal with the situation. For example, the Council of Europe’s Convention on Cybercrime has come into force in 2001. However, the Council of Europe cannot compel the state parties to enforce those provisions within its territories. The Council of Europe cannot also compel any state party to provide international assistance in the investigation of cybercrimes as provided in the Convention. Consequently, the non-binding nature of international law coupled with the lack of enforcement mechanism has prevented the proper enforcement of cybercrime laws (Ajayi, 2016).

6. CONCLUSION

A large number of factors including those described above have cumulatively made it difficult for criminal law to effectively curb cybercrimes. All this point to need to establish an International Court or Tribunal for the investigation and prosecution of transnational cybercrimes particularly those of a grave nature. There is no international consensus at this point of time, facilitating the creation of such an international tribunal/court. Even as such an international mechanism is being thought of, there is a need to adopt cybercrime prevention strategies to reduce cybercrimes. Various methods, technical or otherwise, that help reduce the opportunity to commit cybercrime should also be encouraged. Creating awareness regarding cybercrime among citizens, cybersecurity measures, private policing of the internet etc. are some of the most important cybercrime prevention strategies adopted in actual practice.

7. REFERENCE


