JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

JUDICIAL ENDEAVOUR ON JURISDICTION OF CYBER CRIME

SHWETANK AVIKAL

Department of Faculty of Management Studies , Graphic Era Hill University, Dehradun, Uttarakhand, India 248002

ABSTRACT

Defining cyber jurisdiction in a dispute involving many nations is complicated by the breadth of cyber law. Further complicating matters is the fact that a website, app, product, or material may be lawful in one jurisdiction but unlawful in another, and that the persons involved may or may not be residents of either nation. The study aims to analyze the first international convention to deal with the problem of cybercrime as well as several significant ideas of jurisdiction. Issues Facing the Courts, sentencing by the Judiciary, Trends in Indian Law, Due to the gravity of the societal impact of crime, judges weighing jurisdictional issues cannot afford to ignore them. As a result, the decisions of the courts play a crucial role in determining the best course of action going forward in such situations of comparison.

KEYWORDS: Cyber Crime, Jurisdiction, Technology, territorial sovereignty, international cooperation.

INTRODUCTIONS

Cybercrime is on the rise in today's globe. Yet, India does not have a cyber law policy in place. The online purchase was simple and quick to complete. There is a serious issue with India's lack of forensic investigation and with the country's improper cyber regulations. These days, most people can't function without some kind of technological assistance. Criminal activity of late has resulted from technical means. One easy way to define computer wrong, often known as cyber-crime, is as any illegal act that has been committed with the use of a computer or the internet. The widespread availability and pervasiveness of the internet, computing, and mobile technology has fundamentally altered the structure of modern civilization. It's hard to believe that just twenty years ago, the vast majority of people still didn't have a mobile phone, and personal computers were still a pricey luxury item. People did not have access to email, and texting was not common. Dial-up modems and Ether net cabling made it possible for anyone to access the Internet, and residents were compensated on an hourly basis for their online time.

The proliferation of cybercrime cases in India has presented regulatory agencies with a new front of complexity. The expansion of IT has pushed the number of real people beyond the actual bounds. All things considered, it's fair to say that every argument has two sides. The new ultra-modern global city that has emerged at breakneck speed comes with infinite potential benefits and downsides.

Throughout the course of more than a century and a half, India's criminal justice system has improved, earning it a reputation as one of the world's most sophisticated.

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

Parliament (administrators), police (law masters), investigators, legal counsel, and appointed authorities are all vital institutions concerned with the administration of criminal justice. They have access to a wealth of valuable opportunities, but their cooperation is based on a set of regulations that prevents them from encroaching on one another's territory and ensures that they always operate in concert.

The significance of information, communication, and technology in people's daily lives is vital. Everything from an individual's financial transactions to a country's national security is dependent on the internet. In a similar vein, criminals are abusing this technology to perpetrate crimes. Several frustrating events occur in cyberspace, which may provide offenders with opportunities to engage in numerous cybercrimes. There are several possible actions that might be classified as cybercrime.

Cybercrime may also be understood in a more general sense as "any criminal behavior by means of, or in connection to, a computer system or network," which would include illegal acts including possession and providing or distributing information over computer networks." Nowadays, cybercriminals may easily interrupt any computer or network, regardless of its location, with only a few mouse clicks. In order to counter such threats, states need the authority to extend their jurisdiction beyond their borders, and hence have the ability to execute legal processes inside their borders. One of the most important areas of study in international law is that of state jurisdiction. With no physical boundaries in cyberspace, the location of an attack makes no difference.

LITERARTURE REVIEW

Dr. Sudhir Kumar Sharma (2017) The advancement of computer technology has improved the quality of human existence by increasing precision, velocity, and productivity. The prevalence of cybercrime is a major impediment to national progress. With cybercrime on the rise, it's imperative that we all implement cyber security measures. In a normal situation, an individual might be worried about the methods and equipment used to combat cybercrime. This study highlights the role of legislation against cybercrime in attaining cyber security in a roundabout way, and focuses on the legal reaction to cyber security.

Ms. K. Roopanjali (2018) Salmond, an acclaimed English legal scholar, is correct in his assessment that the law seeks to steer the course of social development. The result of progress and development in society is the betterment of society as a whole. There is a clear path that can be traced back to the beginning of human civilization that reveals how the development of law has progressed. As civilization progressed, people settled down and learned to work together to form communities, which in turn promoted the formation of states. There was demand for managing the direct of individuals bury se; along these lines, State formed the fundamentals of administration which subsequently came to known as "law". As a result, legal development is a process that has followed changes and developments in society. For the most part, laws are enacted to solve societal problems, making law a fluid concept subject to evolution in response to societal demands. Technological progress has helped human civilization thrive and flourish, but it has also given rise to new problems that humans have never faced before. Digital crime is one such murky area that has emerged in the last few of decades

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

Abidi, Dr. (2018). The increasing susceptibility of societies to cybercrime is a side effect of the phenomenal development of information society and its reliance on Internet use throughout the globe, and in India in particular. As the Internet has no physical boundaries, cybercrime may happen anywhere in the world. The "Digital India" paradigm is part of India's grand plan to transform the country into a "information society," in which all levels of government, businesses, and citizens rely only on the Internet for everything from routine tasks to highly confidential dealings and data storage. Because of this, cybercriminals may easily target India. Because of the Internet, data and information may easily be transferred from one network to another. Security concerns have risen to the forefront for administrators as data and information are transmitted across networks in different places. Administrators have had to take significant measures to safeguard the system from unauthorized access or virus assaults due to the development of cybercrime. Cybercrime has skyrocketed in India since 1998, and its rise has followed an exponential pattern. Although India has made strides in combating cyber threats and has been included to the list of Fully Updated Countries, much more has to be done to stem the tide of rising cybercrime and safeguard vulnerable machines. The computer and the network are being rescued with the use of data mining tools. There has been some cybercrime-related litigation and court judgements across the globe. As the number of cybercrimes committed and reported in India continues to rise at an alarming rate, so too will the number of cases involve cyber litigation.

Xiaobing Li, (2018) Cybercrime jurisdiction is the primary focus of this essay. This article presents a new theory of cybercrime jurisdiction and proposes a system for establishing it, based on the principles of "priority of power," "territorial superior rights," a negotiated system for resolving disputes over criminal jurisdiction, and a civil jurisdiction of computer cybercrime.

Hifajatali Sayyed (2019) The prevalence of cybercrime is rising rapidly. A few clicks from anywhere in the world may have an effect on any computer system. The primary question that has to be answered is whether or not the state that felt the effects of the act has jurisdiction over the conduct itself if it was done outside of the state's borders. Jurisdiction is an essential topic to consider in this context since it relates to the sovereign rights of a state over its own territory. This paper seeks to explore numerous major theories of jurisdiction and the Budapest Agreement on Cyber Crime, 2001, the first international treaty to address the problem of cybercrime. It makes an attempt to centre emphasis on international cooperation as a viable technique for combatting cybercrimes.

CHALLENGES BEFORE THE JUDICIARY

Since most of our day-to-day activities, including business, banking, currency exchange, data correspondence, legislative and non-administrative authority exchanges, scholastic pursuits, and so on, are now conducted online, thanks to the proliferation of PC networks and the Internet, online culture has become an integral part of modern existence. At this point in time, anybody who wants information or media may get it on the internet. Yet despite this technology's many benefits, there are also certain drawbacks that provide legitimate cause for worry to law-requirement agencies and legal functionaries alike. Abuse of PC networks for illegal activities

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

thereafter gave rise to a wide range of internet inquiries, comparisons, debates, and so on. While it's true that questions have been around since the dawn of human civilization, the nature, scope, and treatment of debates surrounding digital interactions are vastly different, making them a genuine test for the official court systems.

The variables which hamper legal condemning in cybercrime cases are as per the following:

- They are so transnational that they don't recognize national or even regional boundaries;

- Differences between national legal systems, approaches, and norms regarding the adjudication of digital-related disputes; and,

- Confusion as to what constitutes cybercrime and what kinds of activities fall within that umbrella.

Due to the immaterial nature of cybercrime, physical violence or the presence of a suspect are not necessary. Because to these factors, the traditional adversarial structure of suit fails miserably to fulfill the objective of equity in matters such as cybercrime.

"The Internet and other data developments have brought with them problems that were not anticipated by the legislation. It also didn't account for problems that may arise if government officials, who may lack scientific aptitude or expertise, tried to deal with the new situation. Our legislature's inability to predict how new technologies would affect crime rates quickly became a matter of central attention. While updates to the Data Technology Act of 2000 have included new cybercrimes and associated punishments, the Act's enforcers still face a number of challenges.

JUDICIAL SENTENCING

A cursory examination of the Indian judicial system would reveal that the age, sex, educational background, mental edge, and growth of the accused are all factors that influence legal condemnation as a whole. The denouncer's mental process, the circumstances under which the violation was committed, and the consequences on the accused or the public all play a role in the denunciation. In most cases, leniency in sentencing is warranted because of the offender's youth, lack of criminal history, or both, whereas harsh punishment is warranted because of the seriousness of the crime, the offender's history of repeat offenses, or both. All the same, these are only theories, and they shouldn't stop the authorities from being vigilant in prosecuting the criminals. Juries weighing punishment have little room to ignore crime's broader impact on society. Hence, the decisions made by the courts in such circumstances become crucial in determining the course of action to be taken in the future.

Cybercrime is on the rise despite the fact that the available case law is undoubtedly more insufficient compared to traditional crimes. This is because PCs are becoming more user-friendly. The courts have often shown a tendency to see digital criminals as

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

guilty of planned crime and an expected risk to society, and hence they are unlikely to decrease the sentence of such people.

Although it may be justified to impose a lengthy term due to the seriousness of the offense or a shorter one due to the remorse or restitution of the offender, Leon Radzinovicz argued that a penalty disproportionate to the crime is distasteful.

As cybercrimes may cause considerable damage, the general trend is to impose strict punishments. Whether or whether societal safety or criminal prevention should take precedence in cybercrime sentencing is the central question. Without any specific step in his regard, the general trend is apparently toward cybercrime prevention and control through a harsh stance toward punishing digital offenders. The response of the legal executive and its approach to resolving the digital concerns by providing medical relief to the survivors of such abuses is reflected in the case law referred to in the following pages.

Judicial trend in India

Very Few Indian case law existed on the subject of digital jurisdiction of the courts prior to the development and passage of the Information Technology Act, 2000 on October 17, 2000. One unintended consequence of data innovation's rise as a more efficient means of communication in the new millennium has been an uptick in cybercrime that has bypassed the courts in search of resolution.

A case in point is P.R. Transport Agency v. Union of India and Others. Including judicial wards where better-off communities have reached an agreement through electronic mail. In this case, the offending party had its offer for 40000 metric big loads of coal from the Dobara colliery accepted during an online coal closeout staged by Bharat Cooking Coal Ltd. (BCCL) at several locations. On July 19, 2005, the BCCL informed prospective buyers through email of their acceptance of their offer. The aggrieved party had previously set aside 81.12 Lakhs of funds with a cheque payable to BCCL; BCCL had accepted and paid the check but had failed to deliver the coal. The dissatisfied party was informed via email that the e-closeout stands dropped "due to certain specialized and unavoidable circumstances" on BCCL's part. The aggrieved party discovered that BCCL had abandoned its e-closeout of offer of coal because another party had submitted a better bid for the same quantity but hadn't been taken into account earlier due to a flaw in the PC's software or the maintenance of its data. P.R. Transport, the aggrieved party, took the respondent to the High Court of Allahabad to determine whether or not it was within its rights to rescind the agreement.

The BCCL objected to the Court's regional ward on the grounds that the High Court of Allahabad was not the appropriate venue since the alleged wrongdoing did not occur inside the state of Uttar Pradesh. The aggrieved parties argued that the Court had jurisdiction since they had received electronic notification of receipt of the sensitive document in Chandauli, Uttar Pradesh. Supreme Court concluded after hearing both sides that once an email is acknowledged, the message is saved in the "worker's memory," which might be anywhere in the globe, and can be accessed by

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

the recipient account holder from anywhere in the world. As a result, neither the sending nor the receiving of an email is tied to a certain time.

One's place of business is deemed to be the point of origin for an electronic report under Section 13 (3) of the Information Technology Act, 2000. Wherever the offending party (in this case, P.R. Transport) does business is taken to be the place where it received the sensitive information. Allahabad High Court was accorded jurisdiction since both Varanasi and Chandauli are in the state of Uttar Pradesh. Reasonable play and equity, which are always dependent on the following considerations, may be assumed to apply to the legal pattern of the exercise of venue by courts in cybercrimes if this option is selected.

a. The extent to which criminal activity or deliberate disruption have an impact on State endeavors;

1. The level of discontent with the State's authority;

2. obtaining the state's advantage in resolving the dispute;

3. the responsibility of the state to protect the interests of aid organizations; and

4. The presence of a democratic assembly.

The legislation mandates that the State provide access to the site and interact with the ward in some kind in order to aid them online.

JURISDICTION CONFLICTS

a) Negative conflicts

Nonetheless, a negative jurisdiction conflict may emerge, in this case neither country claims jurisdiction over the cybercrime, despite the fact that the laws for cybercrime jurisdiction are frequently rather broad, at least in a number of states and countries. Due to the nature of most cybercrimes, such as hacking and denial-of-service assaults, they might be prohibited under the laws of most nations. This is due to the fact that different nations might assert their right to prosecute a crime depending on factors like where the computer was located, how far-reaching the consequences were, or where the victim happened to be from. Nevertheless, a number of factors, such as the seriousness of the offence, the degree of the damage, and the offender's links to the country, must be taken into account, will determine whether or not they will assert jurisdiction to adjudicate. The issue is considerably murkier when viruses and certain content-related violations are involved. These crimes often don't target individual computers, people, or nations, and they often take place simultaneously in a wide variety of locations (or "in Cyberspace"). Specifically, If the perpetrator is a resident of a nation recognised for being a cybercrime freehaven and the crime is committed while they are in that country, a negative jurisdiction conflict may occur. For the most expansive jurisdiction claims, such as West Virginia's or Singapore's, there is often something on which to establish jurisdiction, such as the effect within an area or the transit through of data. The real question is whether a state will ever have a compelling enough interest in asserting jurisdiction; for instance, when it comes to

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

viruses or websites hosting hate speech, individual countries may not feel they are sufficiently harmed to claim jurisdiction, perhaps because they believe another country will surely assert jurisdiction. Further study is necessary to examine such cases and assess potential remedies for nations to consult with one another in the event of a potentially detrimental jurisdiction clash.

b) Positive conflicts

Positive jurisdiction disputes, which occur when many countries assert their authority over the same cybercrime, are more significant than negative conflicts. This is a plausible scenario, since cybercrimes often transcend international boundaries, and many nations have expansive jurisdiction laws, therefore there are likely to be many countries with authority to pursue any particular offense. For example, In the example above, at least three nations may lay claim to jurisdiction: the Netherlands, Belgium, and Utah. Other countries, such as West Virginia or Singapore, might lay claim to jurisdiction if the data transfer occurred via their territory. If a virus such as the "love bug" or the "Blast worm" were wreaking havoc inside their borders, several countries may want to claim ownership of it. The federal government of the United States, the states of Wyoming and Texas, Belgium, Germany, and maybe other nations may assert jurisdiction over a Wyoming-hosted website that connects to child pornography on a website in Texas. The reasonableness level is meant to mitigate the effect of such cases across many countries. The mere fact that data passed through a country's territory is insufficient to establish jurisdiction if, for example, that country has suffered much less damage than another or the data just passed through the area without causing any damage. As a result of its malleability, the reasonableness threshold might be interpreted differently by different national courts, permitting jurisdiction claims despite tenuous ties to the country. Yet, in many cases of positive disputes, there will be no resolution at all based on the reasonableness criterion since it will be unclear whether country demonstrably has the closest tie to the crime or has clearly experienced the greatest damage.

THEORIES OF JURISDICTION:

States need to establish a nexus between themselves and either the accused or the crime in question in order to exercise jurisdiction over the matter. The various states have developed their own ideas for establishing legal authority.

Nationality Theory: The perpetrator's nationality is essential to this explanation. There are strict regulations placed on citizens of all countries. The State has the authority to punish its citizens for crimes committed elsewhere in the world. This is addressed under Section 4 of the Indian Criminal Code, 1860, which states that the law applies to Indian nationals everywhere in the world. Section 4 of the Indian Penal Code uses the terms "outside and beyond India" to make it clear that an Indian citizen who commits a crime outside of Indian territory is still liable to Indian law.

Passive Nationality Theory: Victim nationality is the focus of the Passive Nationality Theory. Although it shares the same premise that the government should have complete power over a nation's affairs, this ideology takes a more nuanced and nuance-avoiding approach. According to this view, the state of residence of the victim is the proper venue for addressing a certain crime. It's reasonable, as it's the state that

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

has the most say over its citizens if they commit a crime abroad. Similarly, when a citizen is threatened while traveling abroad, it is the responsibility of the state to intervene. Several countries argue that implementing this approach would be a breach of international law since it would interfere with the internal affairs of other countries.

Protective Theory: Under this view, a state may assert its authority over an offensive conduct that threatens its national or international interests. Almost everywhere in the world, foreign nationals are subject to home state jurisdiction for crimes committed abroad that threaten national security. The international community has to agree that these actions amount to crimes. There is now a greater opportunity for transnational criminal activity. In order to avoid legal repercussions that would result from a rigid application of the territoriality and nationality principle, criminals undertake their incriminating projects in separate areas. The threat has been detected, and states have recognized the need for increased security. If the State wants to apply the protective principle safely and without violence, it must always communicate with the international community.

Universality Theory: According to this idea, any state may claim jurisdiction over criminal acts, regardless of whether or not such acts really affect the asserting state. A state may assume jurisdiction if it has the criminal in custody and the offense is considered particularly egregious on a global scale. Universal jurisdiction was expanded to include crimes of war, crimes against humanity, some terrorist actions, hijacking and sabotage of aircraft, apartheid, torture, and other abuses of human rights.

ISSUES OF JURISDICTION:

Jurisdiction has been broken down into two distinct parts:

1. Prescriptive Jurisdiction:

Freedom to define one's own laws in whatever area a state so desires is what this term refers to. The basic rule is that a state has limitless prescriptive jurisdiction, meaning it may pass laws governing any situation that arises, regardless of where it takes place or the citizenship of the people involved.

2. Enforcement Jurisdiction:

The presence of prescriptive jurisdiction is essential for a state to be able to enforce such laws. According to the principle of the Sovereign equality of States, a state cannot, in practice, impose its jurisdiction over individuals or events physically located inside the territory of another state, even though that state's prescriptive jurisdiction extends to such locations.

JURISDICTION ACCORDING TO BUDAPEST CONVENTION ON CYBER CRIME:

According to the Budapest Convention on Cybercrime, a state's enforcement authority is presumed to be absolute over all things and individuals located inside its own territory. The first international convention aimed at addressing cybercrime, the

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

Budapest Convention on Cyber Crime seeks to promote uniformity in State legislation and seeks collaboration among member States.

Its primary goal is to standardize laws against cybercrime so that they can be effectively enforced. establishing appropriate regulations and a framework for global collaboration. Article 22 of the Convention addresses the issue of jurisdiction over cybercrimes by requiring each Party to adopt laws establishing jurisdiction over the offence when it is committed in its territory, on board a ship flying the flag of that Party, on board an aircraft registered under the laws of that Party, or by one of its nationals, if the offence is punishable under criminal law where it was committed or if it is committed outside the territory of that Party.

Using just the Convention, parties may establish jurisdiction based on territoriality and nationality considerations. It also recognises the aut dedere aut judicare principle, which states must use to bring people guilty for serious international crimes to justice even if no other country has requested their extradition. The basic principle is the need that any wrongdoing be dealt with severely. It imposes a duty on the state even if the crime occurred outside of its borders or if the offender and/or victim are not citizens of that country.

It necessitates that the alleged offender be present within the territory of one Party State, that the offended State make a request for extradition, and that if the Party within whose territory the alleged offender is located is constrained by domestic law not to extradite, the requested Party has the duty to prosecute and the legal ability to undertake investigations and proceedings within its own borders.

CONCLUSION

Cybercrime refers to any illegal behavior that takes place on the internet. Cyber laws provide protection against and deterrence of cybercrime. Cybercrime is exacerbated by the open nature of the internet and the absence of security measures in place to secure personal information. crimes carried out by cybercriminals. However, The vast majority of crimes go unreported, and of those that are accounted for, only a tiny percentage result in resignation because the police and investigative authorities are typically uninformed of the facts of these transgressions and lack adequate proof against the accused. Justice Yad Ram Meena, Chief Justice of the Gujarat High Court, recognized the challenges faced by law enforcement and forensics experts when investigating cybercrime and proposed the establishment of a scientific science university within the state to better equip investigating authorities and judges with the knowledge and resources they need to effectively resolve cases involving cybercrime and other financial and technological offenses. The most expedient and efficient legal strategy for prosecuting such attacks would be to extend the extraterritorial scope of domestic criminal legislation related to cybercrimes.

REFERENCES

1. Dr. Sudhir kumar sharma (2017) cyber security: a legal perspective issn 0974-2247

ISSN- 2394-5125 VOL 07, ISSUE 02, 2020

2. Ms. K. Roopanjali (2018) legal implications of cybercrimes in india issn: 2581-5369

3. Abidi, dr. (2018). Cyber-crimes in india: judicial endeavours. Law review. 38. 10.29320/jnpglr.38.1.7.

4. Xiaobing li, yongfeng qin,research on criminal jurisdiction of computer cybercrime,procedia computer science,volume 131,2018,pages 793-799,issn 1877-0509

5. Hifajatali sayyed (2019) jurisdictional issues in cybercrimes issn 2455-2437

6. Krishna kumar, cyber laws, khanna publication (new delhi) 2nd ed, p.124, 2017

7. Adv.prashant mali, cyber law, india express, 3rd ed., p23, 2016

8. Ahamad m, amster d, barrett m, cross t, heron g, jackson d, king j, lee w, naraine r, ollmann g, ramsey j, schmidt ha, traynor p (2008). Emerging cyber threats report for 2009, georgia tech information security centre. Georgia inst. Technol. 9p.

9. Ajayi efg (2015). The challenges to enforcement of cybercrimes laws and policy. International journal of information security and cybercrime, 4(2):33-48. Available at: http://www.ijisc.com/year-2015- issue-2-article-4/

10. Ajayi efg (2016). The impact of cybercrimes on global trade and commerce. Available at ssrn: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2810782 or http://dx.doi.org/10.2139/ssrn.2810782

11. Paganini p (2013). Infosec institute 2013 cost of cybercrimes http://resources.infosecinstitute.com/cybercrime-and-theunderground-market/

12. United nations office on drugs and crime (2014). United nations convention against corruption. Available at: https://www.unodc.org/documents/brussels/un_convention_against _corruption.pdf.

13. Hawes j (2014). "2013 an epic year for data breaches with over 800 million records lost." Naked security, february 19, 2014. Available at: https://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-fordata-breaches-with-over-800-million-records-lost/

14. Mcguire m, dowling s (2013). Cyber-crime: a review of the evidence summary of key findings and implications home office research report 75, home office, United Kingdom, october. 30p.

15. Halder, d., & jaishankar, k. (2016). Cybercrimes against women in india. New delhi: sage publishing. Isbn 978-9385985775.