RES MILITARIS
Social Science Journal

A STUDY ON JUDICIAL APPROACHES TO THE JURISDICTION OF CYBERCRIME

Lizzie Albert[1], Dr. Pelasur Chandrakumar Swamy[2]
[1] Research Scholar, Department of Law, Himalayan University, Arunachal Pradesh.
[2] Research Supervisor, Department of Law, Himalayan University, Arunachal Pradesh.

Abstract
In a multi-nation dispute, the scope of cyber law makes it challenging to define cyber jurisdiction. Things get much more complicated when you consider that the same website, app, product, or material can be perfectly legal in one country but utterly illegal in another and that the people involved might not even be citizens of either country. The study's goals are to examine many essential concepts of jurisdiction and the first international convention to address cybercrime. Issues In the face of judicial sentences, Indian legal currents, justices considering questions of jurisdiction cannot afford to turn a blind eye to the societal effects of crime. So, in cases like these, the choices made by the courts are quite crucial for figuring out what to do next.
Keywords: Cyber Crime, Jurisdiction, Technology, Territorial Sovereignty, International Cooperation.

Introductions:

In today's world, cybercrime is becoming more common. Currently, there is no cyber law policy in effect in India. It didn't take long at all to finish the internet purchase. India has some significant problems with its cyber rules and its forensic investigation capabilities. Most individuals nowadays rely on technology to get things done. Technical means have recently been used in criminal conduct. The term "computer wrong," frequently shortened to "cybercrime," refers to any unlawful activity using computers or the internet. The advent and pervasiveness of computing, mobile devices, and the internet have radically changed the foundations of contemporary society. It's hard to imagine that even only twenty years ago, most people still didn't own a cell phone, and PCs were considered a luxury good. Neither email nor texting were widely available. Thanks to dial-up modems and Ether net wiring, anyone could get online, and locals could earn money for every hour they spent online.

A new layer of complexity has emerged for regulatory bodies in India due to the increasing number of cybercrime cases. Due to the proliferation of IT, the number of actual humans has beyond all reasonable expectations. I think it's safe to state that any dispute has two sides. There are endless possible advantages and disadvantages to the new ultra-modern global city that has sprung up at a dizzying rate.

India has a reputation for having one of the world's most advanced criminal justice systems, thanks to its systemic improvements over the past 150 years. Essential institutions involved in the administration of criminal justice include parliament (administrators), police (law masters), investigators, legal counsel, and appointed authorities. Their cooperation is predicated on rules that guarantee they never work in isolation and prohibit them from invading each other's domain despite the abundance of beneficial chances at their fingertips.

Information, communication, and technology significantly impact everyday life. The Internet is crucial for every aspect of life, from personal finance to national security. The criminal element also uses modern technology for illicit purposes. Many annoying things happen online, which could allow criminals to commit many cybercrimes. Several different kinds of behavior could be considered cybercrime.

Another way to look at cybercrime is "any criminal behavior using, or in connection to, a computer system or network." This would encompass all sorts of illegal activities, like sharing or disseminating information over computer networks and using computers themselves. With the click of a mouse, hackers can now compromise any network or computer, no matter where it is located. To fight against these kinds of dangers, states require the power to carry out legal procedures within their boundaries and the right to extend their jurisdiction outside. The study of state jurisdiction is a crucial subfield in international law. Since cyberspace has no natural borders, it doesn't matter where an attack occurs.

Literature Review:

Dr. Sudhir Kumar Sharma (2017) The development of more accurate, faster, and more productive computing has raised the standard of living for all humans. A big roadblock to national progress is the prevalence of cybercrime. The prevalence of cybercrime is growing, so everyone must take precautions to protect themselves online. A typical person could be concerned about the tools and strategies used to fight cybercrime. By concentrating on the legal response to cyber security, this study draws attention to the indirect function of cybercrime legislation in achieving cyber security.

Ms. K. Roopanjali (2018) An esteemed English legal professor named Salmond is accurate in saying that the purpose of the law is to direct society's progress. When people work together to improve society, everyone benefits. A straight line beginning with the dawn of human civilization shows how the rule of law has evolved. People learned to live in communities and work together as civilization advanced, which paved the way for establishing states. The need to regulate the burial practices of individuals prompted the state to develop the administrative principles that would later be referred to as "law." Consequently, societal changes and advances have accompanied the path of legal evolution. Law is a notion that can change and adapt in response to society's needs because it is often passed to address societal concerns. While technological advancement has undoubtedly contributed to human civilization's success and prosperity, but it has also brought forth unseen challenges. Cybercrime is a new, hazy sector that has grown in the previous several decades.

Abidi, Dr. (2018). A consequence of the remarkable growth of the information society and its dependence on Internet use worldwide, including in India, is the growing vulnerability of societies to cybercrime. Cybercrime can occur globally since the Internet has no geographical limitations. In its ambitious goal of becoming a "information society," in which all tiers of government, companies, and individuals depend only on the Internet for mundane chores, sensitive transactions, and data storage, India has instituted the "Digital India" paradigm. This makes India an easy target for cybercriminals. The ease of data and information movement between networks is attributable mainly to the Internet. As more and more data and information is sent over various networks in different locations, managers are becoming increasingly concerned about security. The rise of cybercrime has forced administrators to take drastic steps to protect the system from intrusion and virus attacks. There has been an exponential growth in cybercrime in India since 1998. There is still a long way to go before we can stop the rise of cybercrime and protect vulnerable machines, notwithstanding India's inclusion on the list of Fully Updated Countries and its progress in this area. Using data mining technologies, the computer and network are being saved. Court rulings and litigation involving cybercrime have occurred on a global scale. Cyber lawsuits will become more common as the number of cybercrimes recorded and committed in India keeps climbing sharply.

Xiaobing Li, (2018) The primary emphasis of this study is on cybercrime jurisdiction. The article lays out a fresh approach to cybercrime jurisdiction and suggests a method for establishing it. It does this by utilizing concepts like "priority of power," "territorial superior

rights," a negotiated system to settle disagreements about criminal jurisdiction, and a civil jurisdiction of computer cybercrime.

Hifajatali Sayyed (2019) The incidence of cybercrime is on the rise. Anyone, wherever in the globe, might potentially affect any computer system with just a few keystrokes. When an act occurs outside of a state's borders but impacts that state, the main issue is whether or not that state has authority over the act itself. Considering jurisdiction is crucial because it pertains to a state's sovereign rights over its territory. The purpose of this article is to go into various influential theories of jurisdiction as they relate to the groundbreaking 2001 Budapest Agreement on Cyber Crime, the initial global agreement to tackle the issue of cybercrime. The text tries to highlight the need of international collaboration as a practical strategy for fighting cybercrimes.

Challenges before the Judiciary:

With the rise of personal computer networks and the Internet, virtually every aspect of modern life is now online. This includes commerce, banking, currency exchange, data correspondence, exchanges with legislative and non-administrative authorities, academic pursuits, and many more. Consequently, online culture has become an essential component of modern life. These days, it's possible for everyone to access media or information online. However, this technology has several downsides that provide law-requirement authorities and legal functionaries with good reasons to be worried, even though there are many positives. The subsequent exploitation of PC networks for illicit purposes sparked numerous online discussions, comparisons, and questions. Although questions have existed since the beginning of human civilization, the disputes surrounding digital interactions are unique in their origin, scope, and handling, which poses a real challenge to the formal legal systems.

The variables that hamper legal condemning in cybercrime cases are as follows:

- They transcend national or even regional borders due to their transnational nature.
- Disputes involving digital technology are handled differently in different countries.
- The definition of cybercrime and the types of activities that fall under it are unclear.

Physical aggression or the existence of a suspect is superfluous in cybercrime because of its immaterial character. These considerations highlight how the conventional adversarial framework of litigation falls woefully short in achieving equity in contexts like cybercrime.

"The Internet and other data developments have brought problems that the legislation did not anticipate. It also failed to 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 several challenges."

Judicial Sentencing:

Even a quick look at India's legal system reveals that the accused's age, sex, educational background, mental edge, and growth all play a role in the overall legal condemnation. Factors considered while making a denunciation include the person making the accusation, the specifics of the infraction, and the potential impact on the accused or the general public. If the offender is young, has no prior criminal record, or both, then the sentence should be light; if the crime is substantial or the offender has a history of multiple offenses, then sentencing should be harsh. However, the government should be watchful in punishing the offenders regardless of these theories. There is limited wiggle space for juries considering punishment to disregard crime's more significant societal effects. In light of this, the future direction of events is highly dependent on the rulings rendered by the courts under these conditions.

Even if there is undeniably less case law about cybercrime than more conventional offenses, it is nevertheless on the rise. The reason is that PCs are getting easier to use all the time. Courts have a history of seeing cybercriminals through the lens of a planned offender and a potential threat to society; as a result, they are reluctant to reduce the sentences handed down to them.
Leon Radzinovicz contended that a punishment disproportionate to the crime is disgusting, even though it may be appropriate to impose an extended period because of the gravity of the offense or a shorter one because of the offender's regret or reparation.
The overall trend is to enforce harsh sentences for cybercrimes because they might cause significant damage. The critical issue is whether the punishment process for cybercrime should prioritize public safety or the prevention of criminal activity. There has been no concrete action in this area, although the current tendency seems to be toward controlling cybercrime by severely punishing those responsible. The case law cited below reflects the response and approach of the legal executive in settling digital concerns by offering medical treatment to survivors of such assaults.

Judicial Trend in India:

Before the Information Technology Act, 2000 was drafted and passed on October 17, 2000, there was minimal precedent in Indian case law on the courts' digital jurisdiction. An increase in cybercrime that seeks resolution outside the legal system is an unforeseen effect of data innovation's ascent as a more efficient mode of communication in the new millennium.
The judgment in P.R. Transport Agency v. Union of India and Others is an example. This includes judicial wards where wealthier neighborhoods have negotiated by email. During an online coal closeout performed by Bharat Cooking Coal Ltd. (BCCL) at numerous sites, the guilty party accepted its offer for 40,000 metric large loads of coal from the Dobara colliery. In an email sent on July 19, 2005, BCCL told potential purchasers that they had accepted their offer. Although BCCL had accepted and paid the 81.12 Lakhs cheque made payable to them, the wronged party never received the coal. The unhappy party was notified by email that the e-closeout stands were discontinued "due to certain specialized and unavoidable circumstances" at BCCL. The wronged party learned that BCCL had withdrawn their e-closeout coal offer after another bidder had submitted a higher bid for the same quantity, which had gone unnoticed previously owing to a technical glitch with the PC's program or data upkeep. The aggrieved party, P.R. Transport, took the respondent to Allahabad's High Court to find out if it could cancel the agreement.
The BCCL objected to the regional ward of the Court, arguing that the High Court of Allahabad should not have jurisdiction over the case because the alleged sin did not happen in Uttar Pradesh. The wronged parties contended that the court had the authority to hear their case because they were notified electronically in Chandauli, Uttar Pradesh, that the confidential document had been received. After considering the arguments on both sides, the Supreme Court concluded that every acknowledgment of an email is stored in the "worker's memory," which could be located anywhere in the world, and that the recipient's account holder can access this information from any location. Consequently, there is no hard and fast rule about the time it takes to send or receive an email.
According to Section 13 (3) of the Information Technology Act, 2000, an electronic report is considered to have originated from one's place of business. It is presumed that the location where the party responsible (here, P.R. Transport) conducts business is where the sensitive data is obtained. That court was given jurisdiction since Allahabad is in the state of Uttar Pradesh, which includes both Varanasi and Chandauli. If this option is chosen, the legal pattern of courts exercising venue in cybercrimes may be based on reasonable play and equity, which are always influenced by the following factors.

- How much of an effect criminal behavior or intentional disruption has on state-sponsored initiatives;
- How dissatisfied people are with the power of the state;
- getting the state to have an edge in the dispute resolution process;
- The state's duty to safeguard humanitarian groups' interests; and
- An assembly presided over by democratic members.
- The law requires the state to let the ward use the site and engage with them in some way so they can get help online.

Jurisdiction Conflicts:

Negative Conflicts

However, a negative jurisdiction conflict might arise when no country asserts authority over cybercrime, even though many countries' rules regarding cybercrime jurisdiction are quite broad. Most countries' laws may outright ban cybercrimes like hacking and denial-of-service attacks because of the seriousness of these crimes. For reasons such as the computer's location, the crime's gravity, and the victim's nationality, many countries may claim the authority to bring criminal charges. However, their determination of whether to establish jurisdiction to adjudicate is contingent upon many circumstances, including the gravity of the offense, the extent of the harm, and the offender's ties to the nation. When viruses and specific violations of content laws are implicated, the situation becomes much more complicated. Crimes like these frequently occur concurrently in a broad range of places (or "in Cyberspace") and seldom target specific computers, individuals, or countries. A negative jurisdiction conflict may arise, for example, if the offense is committed when the offender is a resident of a country known for its lack of regulation on cybercrime. There is usually something to establish jurisdiction over, such as the impact inside an area or the passage via data, for the most expansive jurisdiction claims, like the ones from West Virginia or Singapore. For example, when it comes to viruses or websites that host hate speech, some countries might not feel hurt enough to assert jurisdiction, maybe because they think another country will do so. The real question is whether states will ever have a strong enough reason to do so. Additional research is required to understand these types of issues and the possible solutions that could allow nations to communicate with one another in the case of a potentially harmful jurisdictional clash.

Positive Conflicts

More severe than harmful conflicts are positive jurisdiction disputes, which arise when many nations claim responsibility for the same cybercrime. Since cybercrimes frequently cross national borders and numerous countries have broad jurisdiction laws, multiple countries will probably have the power to pursue any crime. The preceding case is one in which at least three countries—the Netherlands, Belgium, and Utah—may assert jurisdiction. That country might assert jurisdiction if the data transfer happened within another country's borders, like Singapore or West Virginia. Many nations may be interested in claiming responsibility for a virus like the "love bug" or the "Blast worm" if it were terrorizing their territory. A website housed in Wyoming that links to child pornography on a website in Texas could be subject to jurisdictional claims from the federal government, the states of Wyoming and Texas, Belgium, Germany, and possibly other nations. Establishing a reasonableness level aims to reduce the global impact of such instances. If, for example, a country has endured substantially less damage than another or the data merely traversed the area without producing any harm, it is insufficient to establish jurisdiction simply because the data went through that country's borders. The reasonableness requirement is interpretable at the national level, which means that jurisdiction claims with weak links to the country could be allowed depending on which court is in charge. However, the reasonableness standard will not always lead to a decision in positive

conflicts; it is not always obvious which country has a stronger connection to the crime or has suffered more damage.

Theories of Jurisdiction:

States must prove that they have jurisdiction over a case by establishing some connection between themselves, the accused, or the crime. Different states have devised different ways of establishing authority.

- **Nationality Theory:** This argument relies heavily on the perpetrator's nationality. All country's residents are subject to stringent rules and restrictions. If a citizen commits a crime abroad, the state can penalize them. The law applies to Indian people wherever in the world, according to Section 4 of the Indian Criminal Code, 1860, which addresses this matter. An Indian national who commits a crime outside of Indian territory is nonetheless subject to Indian law, as stated in Section 4 of the Indian Penal Code, which employs the phrases "outside and beyond India" to emphasize this point.
- **Passive Nationality Theory:** According to the Passive Nationality Theory, victim nationalism is the main point. While this philosophy still believes that the state should have total authority over a country's affairs, it does it with less simplicity and more subtlety. If this is the case, then the victim's home state should be the one to handle the case. It makes sense, as the state has the most incredible control over its residents if they commit a crime outside the country. The state also has to protect its citizens from danger when they are overseas. Because it would meddle in the domestic affairs of other nations, several contend that this strategy would violate international law if put into practice.
- **Protective Theory:** According to this school of thought, a state can punish aggressive behavior that endangers its domestic or foreign interests. Foreign people can be tried in their home state for crimes that threaten national security, regardless of where they are. All nations must recognize these acts as crimes. The potential for transnational criminal activity has increased. Criminals carry out their damning initiatives in different locations to evade legal consequences that would arise from a strict application of the territoriality and nationality concept. The danger has been identified, and the governments have acknowledged the necessity of heightened security measures. The State must maintain constant communication with the international community if it wishes to implement the protective principle in a safe and nonviolent manner.
- **Universality Theory:** If this theory is correct, any nation-state can establish its authority over a crime, regardless of how it impacts that nation-state. If the offender is already in the custody of a state and the crime is internationally recognized as highly heinous, the state may exercise its jurisdiction. A wide range of human rights atrocities, including war crimes, crimes against humanity, hijackings and sabotage of airplanes, apartheid, torture, and other forms of human rights abuse, were brought under universal jurisdiction.

Issues of Jurisdiction:

Jurisdiction has been broken down into two distinct parts:

1. Prescriptive Jurisdiction:

This concept describes the ability of a state to establish its laws in whatever area it wants. State governments have the power to legislate on any matter, regardless of the location or nationality of the persons concerned, because of the fundamental principle that states have unlimited prescriptive jurisdiction.

2. Enforcement Jurisdiction:

Prescriptive jurisdiction must exist for a state to have the authority to enforce such laws. Even while one state has prescriptive authority over some regions, that state cannot, in fact, exercise

that authority over persons or events that are physically located inside another state's territory according to the Sovereign equality of states principle.

Jurisdiction According to Budapest Convention on Cyber Crime:

According to the Budapest Convention on Cybercrime, a state's enforcement power is generally total over all items and individuals located inside its own territory. As the first global treaty to tackle cybercrime, the Budapest Convention on Cybercrime aims to encourage cooperation among member states and standardize cybercrime laws.

One of its primary purposes is to make cybercrime laws more uniform and more accessible to enforce. They are creating a structure for international cooperation and enacting suitable rules. Cybercrimes are addressed in Article 22 of the Convention, which states that each Party must pass legislation establishing jurisdiction over the offense when it occurs within their territory, on a ship flying their flag, on an aircraft registered under their laws, or by one of their nationals, if the crime is punishable by criminal law where it was committed, or if it occurs outside of their territory.

The Convention allows the parties to determine jurisdiction by looking at factors including territoriality and nationality. Another critical point is the recognition of the aut dedere aut judicare principle. This principle argues that governments should prosecute individuals responsible for grave international crimes, regardless of whether any other country has asked for their extradition. Strict punishment for transgression is the foundational premise. The state is nonetheless obligated to investigate and prosecute the crime, regardless of whether it occurred within its boundaries or if the perpetrator and victim are not nationals of that nation.

The accused must be physically present in the jurisdiction of one of the Party States. The state that has been wronged must initiate the extradition process. If the Party whose territory the accused is in is legally obligated not to extradite, the requested Party must have the authority to investigate and prosecute within its own borders.

Conclusion:

In this context, "cybercrime" means any unlawful activity that occurs on the internet. The purpose of cyber laws is to prevent and punish cybercrime. The lack of protections for sensitive data and the accessibility of the internet both contribute to the growth of cybercrime—offenses committed by cybercriminals. Nevertheless, due to a lack of knowledge about the specifics of these offenses and sufficient evidence against the accused, the great majority of crimes remain unreported, and only a small fraction of those that are recorded lead to resignations. Chief Justice Yad Ram Meena of the Gujarat High Court acknowledged the difficulties forensics and law enforcement professionals encountered in investigating cybercrime. To address these issues, Justice Meena suggested the creation of a scientific research university in the state. This would provide the necessary training and resources for investigating authorities and judges to successfully handle cases involving cybercrime and other financial and technological offenses. Extending the extraterritorial scope of domestic criminal legislation connected to cybercrimes would be the most expedited and efficient legal technique for pursuing such acts.

References:

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