WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Comprehensive Analysis on Jurisdiction Issues in Cyber Crimes

Harsh Kumar[1], Pooja[2]

[1]Assistant Professor, School of Law, Galgotias University, Greater Noida, Uttar Pradesh.
[2]Scholar, School of Law, IMS Unison University Dehradun.

ABSTRACT

The Digital world is continually changing people's lifestyles, with such advancement of technology, their operational area has also expanded and has become a way of life for most people, including criminals. The contentious jurisdiction issues of cybercrimes globally in the age of technological advancements is scrutinized broadly in this research paper. The types of cybercrimes i.e., from hacking, cyber pornography to logic bombs has been elaborated in the existing paper. Though expanding technology has numerous benefits, it also has a dark side, which is explained in the form of current challenges in investigations of cybercrimes which elucidates who is conducting cybercrime investigation and additionally all obstacles related to cybercrime investigation are also being examined. Jurisdictional concerns are enormously significant in cyberspace, the present paper aimed at explaining jurisdiction of cyberspace accompanied by the extra-territorial jurisdiction and India's position in extra-territorial application of the law. The existent paper observes the Budapest Convention on the cybercrime whose goal is to enhance cybercrime and investigation collaboration among signatory countries. Further, in the paper the cybercrime during the COVID-19 pandemic in India is also inspected. In addition, the judicial pronouncements related to jurisdictional issues in cybercrimes has been enlightened in this research paper. The provisions of Information Technology Act, 2000 with respect to cybercrimes coupled with punishments and particular forums with sole jurisdiction to deal with the cyber offences listed in the Act has been described in this prevailing paper. The current paper discusses the resolution of cybercrime jurisdiction dealing with the tests currently in force. It is possible to conclude that there is an immediate need for a broad-based convention that would be addressing criminal substantive law queries, criminal procedural interrogations along with international criminal law procedures and contracts.

Keywords: *Challenges, Contentious, Cybercrime, Investigation, Jurisdiction.*

INTRODUCTION

Cybercrime does not have a precise definition defined anywhere in the statute. Cybercrime, conferring to the Black Law Dictionary, *"any wrongdoing committed using electronic device, computer science, or perhaps the Internet."*[1] Cyber world has somehow made life of the individuals easier, but have also simultaneously greatly aided the socio-economic, and cultural integration of various fragments of the sphere. The fourth generation of human rights, which in the present day undergoing jurisprudential dispute, encompasses the identification of particular tasks, and this fourth generation of human rights is concerned with digital rights or online rights.

Through the advancement of technological devices, there has been a rise in the misappropriation of digitalization, such as online stalking and harassment, as well as fraud, hacking, and defamation, which are all examples of cybercrime. The development of digital technologies has enabled us again with numerous benefits, including the ability to deal with possible threats and consequently has also presented cybercriminals with the opportunity to conduct offences with the aim of minimizing of exposure. The internet has proven to be a tremendous boost to current societal aberrant behavior.[2] The advancement of virtual defense, cyberattacks, and digital is accelerating as world continues to evolve.

In the year 1820, the first reported cybercrime took place. Although cyberspace is such a large area, cybercrime raises a jurisdictional question. Conferring to estimates from United Nations cyber security experts, high-tech gangs of criminals involved in formalized structured operations has committed approximately 80% of wholly internet-based wrongdoing.[3] Cybercrime is said to be simple to perform, difficult to spot, as well as it is difficult to track down.

The capacity and competence of the court to resolve issues in cyber world is known as cyber jurisdiction, and a judgement issued by the court without jurisdiction is considered to be meaningless. Cyber criminals use a variety of electronic equipment to carry out their operations, which may be in the

[1] *Cybercrime*, TheLaw.com Dictionary, Law Dictionary & Black's Law Dictionary, 2nd Ed https://dictionary.thelaw.com/ (Last visited Feb 04, 2024)
[2] *Nature and Scope of Cyber Crime*, LawPage, https://lawpage.in/cyber_laws/crime/nature-and-scope) (Last visited Feb 04, 2024)
[3] Vuk Mujović, *Where Does Cybercrime Come From? The Origin & Evolution of Cybercrime*, Le VPN, October 18, 2018, https://www.le-vpn.com/history-cyber-crime-origin-evolution/ (Last visited Feb 04, 2024)

same or separate countries. When crimes are committed outside the territory of India and have an impact on Indian nationals, the issue of jurisdiction arises. The difficulty in tracing cyberattacks is due to evolving technologies.

According to new research by the **US Federal Bureau of Investigation (FBI),** ranked amongst the top world's top five states in terms of cybercrime victims, with phishing and voice phishing etc., among the top cyber frauds committed in 2021.[4] During the COVID-19 epidemic, there was also a significant increase in cybercrime cases, opening the potential for malware creators to commit cybercrime which has caused many issues related to jurisdiction in order to capture the cyber offenders. In the digitization era, the cyber attackers are taking use of technological improvements as a means of conducting cybercrime which is a threat to the individuals.

CONTENTITOUS JURISDICTION ISSUES OF CYBERCRIMES GLOBALLY IN THE AGE OF TECHNOLOGICAL ADVANCEMENTS

In the age of technological advancements, the cyberspace has become the cornerstone of both the social and commercial worlds. Subsequently, the cybercrime is having global nature the jurisdiction is one of the most contentious concerns in the age of technological advancements. The territorial concept appears to be vanishing as the cyber milieu has been extended. Web users can access the internet almost anywhere in the globe at any time, yet many unlawful activities can be carried out through the internet. It is being alleged that there are no territorial limits in cyberspace; it allows for immediate long-distance contact with everyone who knows how to contact through the web or who has access to any website.

In most cases, an internet user has no way of knowing where the information on a website is coming from i.e., not aware about the origin of the source of data provided in the website. Jurisdictional constraints are highly essential in this context, i.e., in cyberspace. Cyberspace users stay in physical jurisdictions and are subject to laws regardless of their presence on the cyberspace, as the Internet does not tend to make geographical and jurisdictional borders evident.[5]

Cyberspace, which specifically refers to information and communications technology (ICT) equipment, is governed by territorial sovereignty. Third parties getting unauthorised access to information and communications technology (ICT) in foreign countries without the knowledge or permission of the host government or law enforcement personnel can undermine state sovereignty. Additional variables that are influencing cybercrime jurisdiction encompasses the criminal's nationality i.e., said to be as "*principle of nationality or the active personality principle",* the victim's nationality i.e., said to be as "*principle of nationality or the passive personality principle",* and the impact of cybercrime on the state's interests and security i.e., said to be as protective principle. The jurisdiction of these and other national cybercrime laws is essentially defined by the location of the perpetrators, victims, and cybercrime's effects.[6]

In India in order to deal with cybercrimes the Information Technology Act of 2000 was passed, and the IT Act contains particular boards with sole jurisdiction so as to deal with cases of the cyber offences computed in the Act but as a result that traditional means of dispute resolution should take precedence over new methods, these issues are not well addressed in the IT Act, 2000.

There are being several transnational groups of actors, especially states, have endorsed the concept of digital sovereignty in recent years to advocate their desire to reclaim control over statistics, communication, and internet set-up, etc. As a result, it is viewed that forthcoming worldwide cybersecurity regulation will face more challenging complications. In affluent countries, legal structures addressing cyberspace are rather well-established. Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Billey Act of 1999, and Homeland Security Act of 2002 are three major rules adopted at the federal level. Since 1988, the French government has established and implemented legal frameworks for cyberspace. Since 2006, Russia's federal authority has enacted Russian Federal Law on Personal Data No. 152 FZ. Nonetheless, those nations have differing perspectives on cyber world, with Russia contentiously prioritizing security concerns over private rights, and the United States having an identical difficulty after ***Edward Snowden's issue*** became public. Also, there are debates on endorsing global customary law the underpinning of global law on internet.[7] Hence, it is seen that addressing which subjects of law are legitimate to make and be influenced by international law on cyberspace, as well as what issues should be regulated, remains a huge challenge or a debatable issue.

Since the centuries been passed it is evident that in the present world advent of the internet, on the other hand, opened a Pandora's Box, as the internet was far larger than that of any device ever created. It is correspondingly obvious that everything from banking to communications, from facilitating ticket bookings to reinventing retail, everything was enhanced by the advanced cyber technologies. Presently, the thing is true that the Internet is intertwined with practically every other technology. Everything, including cell phones, computers, automobiles, and televisions, etc., is connected to the net. Today's net has such a widespread scope that most current technology would be dubious without it.[8] Psychologically it would be appropriate to say that not one

[4] Team TC, *FBI report ranks India in top 5 countries with victims of cybercrimes*, TECHCIRCLE, https://www.techcircle.in/2022/05/30/fbi-report-ranks-india-in-top-5-countries-with-victims-of-cybercrimes (Last visited Feb 04, 2024)

[5] Suneet Dwivedi, *Jurisdiction Issues in Cyber Crimes*, ACADEMIA, https://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime (Last visited Feb 04, 2024)

[6] *Cybercrime Module 7 Key Issues: Sovereignty and jurisdiction*, UNODC, United Nations Office on Drugs and Crime, June 2019, https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html (Last visited Feb 04, 2024)

[7] Abid A. Adonis, *International Law on Cyber Security in the Age of Digital Sovereignty*, E-International Relations, March 14 2020, https://www.e-ir.info/2020/03/14/international-law-on-cyber-security-in-the-age-of-digital-sovereignty/ (Last visited Feb 05, 2024)

[8] Manulawskills, *Critical Analysis of the Laws Against Cyber Crimes in India*, Law & Technology, manupatra LawSkills, February 15, 2019, https://blog.lawskills.in/2019/02/15/critical-analysis-of-the-laws-against-cyber-crimes-in-india/ (Last visited Feb 05, 2024)

in the present scenario would want to use their phone or computer that couldn't connect to the internet and with increasing technology of the cyberworld the internet is being misused by the cyber attackers.

The principle of territorial sovereignty has led to States predominantly claiming jurisdiction over crimes committed in the interior borders, resulting in jurisdictional issues and it has made the jurisdiction concern a controversial debate. Indian law court's jurisdiction in fighting cyber-crime executed by interlopers disturbing Indian cyberspace is still an opinion of debate or discussion. Indian Police currently for the cyber-attackers residing outside India for them are foremost concerned about of how to capture the cyber offender's exterior to their jurisdiction as the *"principle of territorial sovereignty"* of the states is playing a noteworthy role in the argumentative or contentious jurisdiction issues of cybercrime. Since municipal laws prevailing in most states are differing from one state to other states and this disparities in laws is acting as one of the major issues of cybercrime jurisdiction globally.

TYPES OF CYBER CRIMES

The following are some of the most common types of cybercrime in the 21st century:

i. **Hacking:** A simple definition of hacking is a potentially illegal intervention into a data system or web. Hacking is said to be performed by the hackers and they are principally *"computer programmers"* and it is considered hackers are having a deep knowledge of computers and this programming assistances is being commonly utilized by hackers for malicious acts. Through various ways hacking can be done. Phishing scam is the most prevalent type of hacking, in which hackers deceive victims into opening an email attachment or transmitting confidential information with the aim of getting login names and passwords or introduce malware into networked computing settings.[9]

Hackers utilize a variety of methods to reach you over the internet, including:

A. The first is **SQL injections**: SQL injection stands for ***Structured Query Language*** and is a method that enables hackers to exploit security flaws in the software that runs a website. For extracting statistics SQL injections can also be used from unsafe websites for seeking credit card numbers, etc.

B. Second is the **Theft of FTP** (File Transfer Protocol) Passwords: FTP (File Transfer Protocol) password hacking exploits the fact that many website owners keep their website username and password on their unprotected computers. The thief investigates the victim's computer for FTP login information, which he then sends to a remote computer.

C. Third is the **Cross-site scripting** which is often known as XSS (cross-site scripting), is a simple approach to get around a security mechanism. A hacker attacks a website with a fraudulent patron script or programme in a conventional XSS attack.[10]

ii. **Phishing:** This is a method of obtaining sensitive information such as credit card details and username/password combinations by impersonating a reputable company. Usually, cybercriminals create a bogus website and then send a bunch of phishing emails with a links to fake website. Usually by believing that links in the email is authentic the personal data is submitted by the users or victims of the cyberattacks and ultimately the phishers are selling or gathering information for malicious purposes.

iii. **E-mail Bombing:** Another sort of cybercrime is email bombing, which involves an attacker sending massive amounts of email to a target address, which is causing the victim's email account or mail servers to breakdown partially or completely. The matter possible that targeting numerous accounts on a mail server will outcome in a rejection of service attack.

iv. **Spamming:** Another type of cybercrime is spamming, which is a variation of email bombing. Unsolicited bulk messages are sent to a large number of users without regard for their preferences. Opening links in spam emails might lead to phishing websites that contain viruses. Infected files may also be attached to spam messages.

v. **Logic bombs:** Logic bombs ordinarily act alike a "virus", yet they aren't viruses. A logic bomb or slag code, is a fraudulent piece of code that is injected into software with the goal of doing a destructive activity when activated by a specified event. For keeping system safe from logic bombs, one need to be aware of data and install effective anti-virus software on each machine on the network.

vi. **DoS Attack:** DoS stands for denial-of-service attack. This attack is such a sort of cybercrime where attackers make a deliberate attempt to prevent intended users from using a service. This attack is causing the network server to crash or severely slow down, avoiding users from accessing it.

vii. **Identity theft:** It is a kind of cybercrime in which someone steals your identity and uses it to access resources in your name, such as credit cards, bank accounts, etc., The identity of users here could also be used by the pretender to accomplish additional crimes.

---

[9] Mike Berg, *Hacking*, Techopedia, March 27, 2020, https://www.techopedia.com/definition/26361/hacking#:~:text=Hacking%20generally%20refers%20to%20unauthorized%20intrusion%20into%20a,differs%20from%20the%20original%20purpose%20of%20the%20system. (Last visited Feb 05, 2024)

[10] *The 12 Types of Cyber Crime*, http://dcac.du.ac.in/documents/E-Resource/2020/Metrial/408sunitayadav4.pdf

viii. **Credit card fraud**: This credit card fraud in its utmost basic form is identity theft. This sort of cybercrime includes offences including identity theft and the use of your credit card to fund the criminal's transactions. The most prevalent technique for hackers to steal your money is through credit card theft.[11]

ix. **Database Piracy**: Practically all the data is available on the internet currently in the form of songs, movies, etc., Internet piracy is a part of our life that we all participate to directly or indirectly whether we grasp it or not. Piracy is not just about stealing someone else's intellectual property, it's also about passing it on to your pals, lessening the amount of money they deserve. Since pirates commonly infect software program with risky code, pirated software may contain Trojans, viruses, worms, and other malware.

x. **Cyber Pornography:** Any content that displays sexually explicit behaviors with a child is referred to as "cyber pornography." Photographs, movies, and digital or computer-generated images that are indistinguishable from a real minor are examples of visual portrayals.[12] The number of cases of cybercrime involving children has risen. According to data from the ***National Crime Records Bureau (NCRB),*** the number of cybercrime cases involving youngsters has increased 400 percent in the last year. However, the Central Bureau of Investigation (CBI) is currently quite active in the fight against child pornography and is conducting raids on a regular basis. The child pornography, rendering to the police reports, is linked around to 100 countries, by means of the CBI assisting in the examination.[13]

xi. **Cyber Stalking:** Cyber stalking is described as a cybercriminal's repeated acts of harassing or online harassment directed at a victim via the internet. Additionally, the cyber stalker does not directly follow his target; instead, he does it electronically by monitoring his user activity in order to gather information about her and harass and threaten the victim. In the cyberstalking one of the issues is an infringement of one's right to privacy on the internet. Cyber stalking differs from offline stalking in that it takes place over the internet or through other electronic methods, yet it is frequently accompanied by it.[14] In the cyberworld women are the most common sufferers of being stalked by men.

Stalking is defined in **Section 354D of the Indian Penal Code, 1860,** as anyone who attempts to monitor a woman's online activity. As a result, if the stalker engages in any of the activities listed in Section 354D of the Indian Penal Code, he will be charged with an offence of stalking. There are several flaws in this section one of them is that it only identifies "women" as victims of cyberstalking and ignores the fact that men can also be victims of the stalking.[15] The Indian Penal Code's Section 292 is mirrored in **Section 67 of the Information Technology Act, 2000.** This section deals with the "electronic form" of obscene material further as a result, this section deals with online stalking. If the stalker tries to disseminate obscene material about the victim on social media, i.e., in electronic form, in order to bully the victim, he will be charged under Section 67 of the IT Act.

Cyber stalking includes webcam hijacking as well as monitoring location check-ins on social media, etc. A few efforts have been taken by the Internet Service Provider to limit the stalker's harassing actions. To stop strangers from transferring messages with obscene content cyberspace services should allow users to report mishandlings. Users must take several preventive precautions linked to privacy settings while using electronic devices.

Various additional sorts of cybercrimes, such as cyber terrorism, viruses, trojans, and worms, cybercrimes involving finance and data theft, and so on, are other types of cybercrimes, and users must take precautions when using the internet.

CURRENT CHALLENGES IN INVESTIGATIONS OF CYBER CRIMES

Since the internet is not tied to a specific area, state or country, there are numerous obstacles in cyber-crime investigation. Cybercrime can be directed from anywhere in the globe and directed at a specific spot. Cybercrime laws are not uniformly enforced in all countries. The following are some of the current difficulties that investigators have when it comes to cybercrime:

- Cyber-attackers avoid penalty by manipulating cyber data via advanced technologies and adjust data using advanced technologies that make it rigid to track them down.[16]
- The investigation becomes difficult by the fact that national and international regulations are moreover weak or unwell applied.
- International cybercrime legislation is insufficient to penalize a cybercriminal and do not allow for the promotion of an investigation.
- It is nearly challenging to prosecute a cyber-criminal who is a citizen of another country. Security authorities may be aware of a cyber-attacker, but the government of the country in question will not sanction prosecution.
- By the geographical boundaries of a single country or state the cyberspace is not constrained. Several European countries have severe ***"Data Privacy rules"*** in place, which avoid the investigation from proceeding. Cyber-attackers are knowing diversity of techniques to conceal their

[11] *The 12 Types of Cyber Crime*, http://dcac.du.ac.in/documents/E-Resource/2020/Metrial/408sunitayadav4.pdf
[12] *Child pornography is sexual abuse material*, The Thorn, https://www.thorn.org/child-pornography-and-abuse-statistics/ (Last visited Feb 07, 2024)
[13] EDITORIAL, *Child pornography: Cybercrime cases against children increased by 400% in 2020, net spread to 100 countries, CBI engaged in investigation*, NEWSNCR, November 17, 2021, https://www.newsncr.com/national/child-pornography-cybercrime-cases-against-children-increased-by-400-in-2020-net-spread-to-100-countries-cbi-engaged-in-investigation/ (Last visited Feb 07, 2024)
[14] *The 12 Types of Cyber Crime*, (June 06, 2022, 03:55 PM), http://dcac.du.ac.in/documents/E-Resource/2020/Metrial/408sunitayadav4.pdf
[15] Ms. Heena Keswani, *Cyber Stalking: A Critical Study*, Bharati Law Review, April – June, 2017, http://docs.manupatra.in/newsline/articles/Upload/455C1055-C2B6-4839-82AC-5AB08CBA7489.pdf
[16] Ratnesh, *Challenges in Cyber Crime Investigation*, Security Escape, July 20, 2021, https://securityescape.com/challenges-cyber-crime-investigation/#:~:text=%20Challenges%20in%20Cyber-crime%20Investigation%20%201%20A%29,is%20useful%20for%20both%20victims%20and...%20More%20 (Last visited Feb 07, 2024)

physical location, yielding them to remain unidentified by investigators. Using the most powerful tools, cybercriminals are conducting crimes more frequently and precisely. High-speed Internet, data encryption, artificial intelligence, and other technology are assisting criminals in not only committing crime but also concealing their identities.[17]

- The cybercrime investigation is becoming difficult when the country's cyber-crime laws are feeble and for the proper investigation of the cybercrime the proper cooperation amongst national and international law is essential.

Investigators in India's law enforcement agencies are not computer proficient. Understanding the fundamentals of IP addressing is required in order to track internet users to their physical locations. IP addresses are used to establish a link between two computers so that they may communicate.[18] It is required that investigators of the cybercrimes must be proficient with the various advanced technologies of the cyberworld and by framing proper legal framework nationally & internationally can help the investigators to investigate beyond jurisdiction.

JURISDICTION OF CYBERSPACE

A court's verdict is ineffective and powerless if it lacks jurisdiction. Cyberspace jurisdiction can be divided as:

Subject matter jurisdiction: The court's subject matter jurisdiction is defined as its ability to hear and decide a certain type of case. The nature of the jurisdiction with respect to the categories of issues involved is described in the subject matter jurisdiction. A corporation winding up mechanism, for example, could only be handled with in the High Court and not in a district court.[19]

Personal jurisdiction: It is the court's straightforward understanding to evaluate whether or not a person is subject to the court in which the matter is filed or has authority over a person, regardless of their location.[20] The Court in ***Attaway v. Omega***[21] invoked the "minimum contacts" test to strengthen existing jurisdiction over defendants who bought a used car from the plaintiffs on eBay.[22] When the defendant was asked for damages, defendant revoked the payment, claiming that car was not as represented after the transaction was done, and asserted the defense of lack of personal jurisdiction.

Three parties are required for transaction in cyberspace: (i) the user, (ii) the server host, and (iii) the person with whom the transaction is being performed, all of whom must be within the same jurisdiction.[23] To begin with, personal jurisdiction refers to a court's ability to apply its laws to a party who is physically present within its jurisdiction. Each state has personal jurisdiction over individuals who exist inside its borders.

EXTRA-TERRITORIAL JURISDICTION AND INDIA'S POSITION IN EXTRA-TERRITORIAL APPLICATION OF THE LAW

Extra-territorial Jurisdiction

Meanwhile the cyberspace is worldwide, any rules or court rulings affecting it could have an extraterritorial impact. One feature of international communications over the internet that is difficult to determine is jurisdiction. As courts were confronted with concerns of jurisdictional law, they were unable to determine the right forum to hear matters involving cybercrime because the virtual world is uncertain when compared to the physical world, making it extremely problematic to regulate cybercrime. National laws are unable to address the problem of cybercrime using local machinery since our machinery is unharmonious with dealing global crimes.[24]

Penalizing and attempting to convict someone from another state pose a challenging difficulty in the area of jurisdiction and some of the characteristics that can lead to extraterritorial jurisdiction issues like unpredictability, contradiction, and uncoordinated activity as different establishments strive to implement decisions and laws. There is no international instrument dealing to cyber-jurisdiction, which is significant. Despite universal agreement on the importance of international cooperation in a society connected by computer networks, ***Russia's proposal***[25] to enact an international convention on

---

[17] Ratnesh, *Challenges in Cyber Crime Investigation*, Security Escape, July 20, 2021, https://securityescape.com/challenges-cyber-crime-investigation/#:~:text=%20Challenges%20in%20Cyber-crime%20Investigation%20%201%20A%29,is%20useful%20for%20both%20victims%20and...%20More%20 (Last visited Feb 07, 2024)

[18] Mamta Sanjay Karkar, *Issues and challenges in the investigation of the Cyber offences of Electronic Fund Transfer in India: An analytical study*, International Journal of Research in all Subjects in Multi Languages (IJRSML) ISSN: 2321 - 2853, Vol. 8, Issue: 10, Oct.: 2020, http://www.raijmr.com/ijrsml/wp-content/uploads/2020/12/IJRSML_2020_vol08_issue_10_Eng_04.pdf

[19] Abhay Singh, *CHAPTER II: JURISDICTION IN CYBER SPACE*, ACADEMIA, https://www.academia.edu/8990032/CHAPTER_II_JURISDICTION_IN_CYBER_SPACE (Last visited Feb 09, 2024),

[20] Suneet Dwivedi, *Jurisdiction Issues in Cyber Crimes*, ACADEMIA, https://www.academia.edu/3700793/Jurisdictional_Issues_in_Cyber_Crime (Last visited Feb 09, 2024),

[21] No. 11A01-0712-CV-608.

[22] *Jurisdiction in the Cyberspace*, LawTeacher, 2nd Aug 2019, https://www.lawteacher.net/free-law-essays/commercial-law/jurisdiction-in-the-cyberspace-commercial-law-essay.php#ftn14 (Last visited Feb 09, 2024),

[23] Deeksha Umakanth, *Jurisdiction in Cyberspace*, Indian Law Portal, December 25, 2020, https://indianlawportal.co.in/jurisdiction-in-cyberspace/ (Last visited Feb 09, 2024),

[24] Meetali Rawat, *Transnational Cybercrime: Issue of Jurisdiction*, International Journal of Law Management and Humanities, Volume 4, Issue 2, Page 253 - 266, https://www.ijlmh.com/paper/transnational-cybercrime-issue-of-jurisdiction/ (Last visited Feb 11, 2024)

[25] *Ibid*

cybercrime was rejected by the United Nations in the year 2010. These issues arise when determining the location of the offence and when various jurisdictions are equally competent.

India's position in Extra-territorial application of the law

The fundamental issue arises when cybercrime falls within an extraterritorial jurisdiction and in order to deal with cases of cybercrime, numerous forums have been established, each of which has exclusive jurisdiction to decide cases of cybercrime, as demarcated by the Information Technology Act of 2000. Cyber matters are addressed in the forums by an Adjudicating officer designated by the controller, as well as the "Cyber Regulations Appellate Tribunal" and the High Court.

According to section 75 of the Information Technology Act of 2000, India is claiming "long arm" jurisdiction over overseas parties who commit illegal activities beyond India that affect a computer data system in India. According to the section, the Act's provisions is applied to first, regardless of nationality to any person, and second, a crime or infringement committed exterior India. Consequently, to include mutually cyber violations and cybercrimes the IT Act has embraced the principle of universal jurisdiction.

Long arm statute jurisdiction is demonstrated in Section 75 of IT Act. Long arm statutes allow domestic courts to exercise personal jurisdiction over suspects who are located outside of the forum state's jurisdiction. The issue is that if the forum court's orders against defendants outside its jurisdiction cannot be enforced, the forum court's involvement would be then pointless.[26] Although India has signed **Mutual Legal Assistance Treaties (MLATs)** with a few nations to provide lawful aid in criminal issues, cybercrime may not be included by those agreements because dual criminality must be met. In addition, India is a signatory to the ***"United Nations Convention Against Transnational Organized Crime"***, which relates to criminal offences in overall and may not be useful in cybercrime investigations.[27]

As a result, there is a growing necessity for international collaboration and aid conventions and treaties, as combating international cybercrime will remain difficult without them. Thus, the Cyber Crime Convention endorses the idea that whenever concerns involving extraterritorial jurisdictions emerge, they can be handled by mutual cooperation.

BUDAPEST CONVENTION ON CYBERCRIME

The Convention is the primary global treaty on crimes happen with the use of the Internet and different computer networks, dealing specially with copyright infringements, computer-aided fraud, child pornography, and violations of community security. It additionally incorporates a sequence of powers and methods inclusive of the quest of computer networks and interception. Its principal objective, set out with inside the preamble, is to pursue a common criminal policy coverage geared toward the safety of society towards cybercrime, especially with the aid of using adopting suitable law and fostering global co-operation.

The Budapest Convention, officially known as the Council of Europe Convention on Cybercrime, opened for signature in 2001 and made enforceable in 2004, was the first international agreement with a particular focus on cybercrime.[28] As I wrote this article at the time, 66 countries, including the USA, have ratified the Budapest Treaty. Several other countries are also into the process to be a part to this agreement, these observer countries are signatories to the convention and invited to accede.[29] The Convention has three purposes.

a) Harmonization of domestic laws related to cybercrime;

b) Supporting the investigation of these crimes;

c) Strengthening global cooperation in countering cybercrime.[30]

In particular, the agreement requires member countries to pass laws prohibiting certain cybercrime. Participating states are also required to implement certain rules for collecting evidence, such as: B. Mechanisms that support rapid retention of stored data, etc. And if the country involved in the request does not have an existing MLAT, it will serve as a limited legal aid treaty (MLAT).[31]

---

[26] Aqa Raza and Mukesh Dwivedi, *Laws Relating to Cyber Crimes: Theories and Legal Aspects*, ACADEMIA, https://www.academia.edu/44228605/Laws_Relating_to_Cyber_Crimes_Theories_and_Legal_Aspects (Last visited Feb 11, 2024)

[27] Meetali Rawat, *supra* note at 26.

[28] Budapest Convention and Related Standards, Council of Europe, https://www.coe.int/en/web/cybercrime/the-budapest-convention; *see* Convention on Cybercrime, Details of Treaty No. 185, Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. (Last visited Feb 11, 2024)

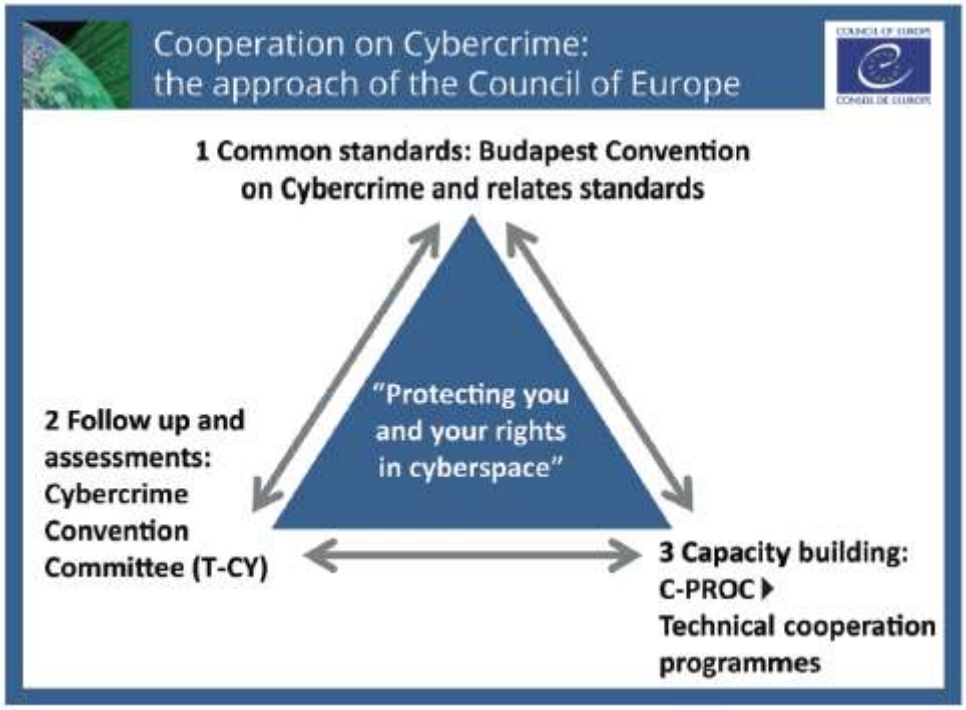
[29] Available at https://www.coe.int/en/web/cybercrime/parties-observers

[30] Preamble, Convention on Cybercrime, Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (Last visited Feb 11, 2024)
see Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention, European Commission, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_865. (Last visited Feb 12, 2024)

[31] Article 27 – Procedures Pertaining to Mutual Assistance Requests in the Absence of Applicable International Agreements, Convention on Cybercrime, Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. "The Convention further provides signatories with guidance on mutual assistance and acts as a mutual legal assistance treaty … for countries that do not have one with the country requesting assistance." E4J University Module Series: Cybercrime, Module 3: Legal Frameworks and Human Rights, International and Regional Instruments, United Nations Office on Drugs and Crime (June, 2022), www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html.

Cybercrime Convention Committee

The member states that presently quantity to 66, collectively with ten global organizations (inclusive of the Commonwealth Secretariat, European Union, INTERPOL, the International Telecommunication Union, the Organization of American States, the UN Office on Drugs and Crime and others), take part as participants or observers withinside the cybercrime convention committee. This Committee reviews implementation of the guidelines of convention by the members and keeps the convention updated. Current focus and efforts of committee are aimed on the regulation of enforcement and to the digital proofs on cloud servers.



Source: GFCE[32]

The Second Additional Protocol

Law enforcement powers are constrained by territorial boundaries as cybercrime surges and the problem of attaining electronic evidence that may be existed in foreign, multiple, or untraceable jurisdictions increases. As a result, only a very small percentage of cybercrime reported to law enforcement agencies leads to prosecution or decisions in court. The protocol addresses this problem and suggests tools to enhance the cooperation and disclosure of electronic evidence such as human rights and the rule of law system, including protection of data measures.[33]

On June 8, 2017, at the 17th session, the Committee on Cybercrime approved the terms and conditions for drafting the second additional Protocol of the Convention on Cybercrime in Budapest and defined its scope. Civil society and stakeholders were also made a part of session for the purpose of drafting to include cross-sectoral warnings. Refinement began in 2017 and has been followed by more than 90 meetings. The new protocol supports better efficient mutual assistance in legal matters ; working directly with service providers in different jurisdictions for subscriber information requests, retention requests, and emergency requests ; Human Rights Guarantee ; Cross-border access to data. It targets to provide a framework for more effective acquisition of electronic evidence.

India and the Budapest Convention

During the period of 2007-2008, Council of Europe gave cooperation to India regarding the better protections against cyber-crimes because of which changes were made in the Information Technology Act in India. These reforms delivered the regulation of India widely in line with the Budapest Convention. While member states withinside the Budapest Convention has become more than double in numbers since then, still India is yet to be a part of it. Although the exact reasons aren't known of India's not a part of Budapest Convention, but the concerns raised through different stakeholders include:

- That India was not a part withinside the negotiations and sessions of the Convention and therefore should not be part of it by signing it. But the benefits to be a part of it even without being a part of negotiations outweigh, this argument is supported by the membership of different countries.

[32] Available at https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/9 h June
[33] Available at https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention

- That Article 32b of the Budapest Convention permits for transborder get admission to information and for that reason violates on country sovereignty. After comprehensive analysis, the Cybercrime Convention Committee showed the constrained scope of Article 32b in a Guidance Note in 2014. This then made a few quarters withinside the authorities of India to condemn that Article 32 become too constrained, and that extra alternative might be required.
- That it's a treaty for the criminal justice and thus its coverage isn't over all the states and state actors, mostly states from where India has potential threats of cybercrimes aren't part of this treaty. So, it does not serve the purpose of India, because of the lack of universal coverage.

CYBER CRIMES DURING COVID-19 PANDEMIC IN INDIA

The Covid-19 pandemic has drastically altered lifestyles in all areas. These situations have created new lifestyle patterns that people have had to deal with. Thus, a complete and direct reliance on the use of insecure internet networks in the implementation of all aspects of life. For example, many organizations have officially launched via the Internet, students have switched to education, and online shopping has increased.

According to Kaspersky's[34] telemetry "*When the world went into lockdown in March 2020, the total number of brute force attacks against remote desktop protocol (RDP) jumped from 93.1 million worldwide in February 2020 to 277.4 million 2020 in March—a 197 per cent increase. The numbers in India went from 1.3 million in February 2020 to 3.3 million in March 2020. From April 2020 onward, monthly attacks never dipped below 300 million, and they reached a new high of 409 million attacks worldwide in November 2020. In July 2020, India recorded its highest number of attacks at 4.5 million. In February 2021—nearly one year from the start of the pandemic—there were 377.5 million brute-force attacks—a far cry from the 93.1 million witnessed at the beginning of 2020. India alone witnessed 9.04 million attacks in February 2021. The total number of attacks recorded in India during Jan & Feb 2021 was around 15 million*."[35][36]

"Cyber-crimes have gone up by almost 500% in India during the global pandemic. We need to consider the emerging threats from new technologies such as drones, ransomware, Internet of Things (IoT) devices and also the role of nation states in such cyber-attacks. The lockdown, which witnessed a deeper adoption of interconnected devices and hybrid work environment, has increased our dependence on technology. This renders us digitally more vulnerable than ever before," said by then Chief of Defence Staff (CDS) General Bipin Rawat, while he was addressing the opening address of the 14th edition of c0c0n, the annual cyber security and hacking conference arranged by the Kerala Police.[37]

RESOLUTION OF CYBER CRIMES JURISDICTION

The United Nations General Assembly passed a resolution on cybercrime on May 26, 2021. Two resolutions were filed at the start of the May meeting, one by the US and the other by Russia, expressing conflicting perspectives of how the committee should operate. Russia proposed that the revised resolution be approved as is, while Western and Latin American countries were anxious that their recommendations would be ignored. This resolution was primarily organisational in nature, establishing the policies and procedures for debating and potentially drafting a treaty "on combating the use of information communication technology (ICT) for criminal purposes," but it was met with strong opposition from member states, casting severe doubts over whether improvement could be made.[38]

JUDICIAL PRONOUNCEMENTS RELATED TO JURISDICTIONAL ISSUES IN CYBER CRIMES

The boom of net communique and trade has caused the transition of the world into a Global Village. More the access has made easier worldwide, more the vulnerabilities have arisen. Although for the physical crimes it's easier to determine the jurisdiction by traditional methods but in the cyber world the questions regarding the jurisdiction have been vaguely determined.

Determination of Cybercrimes Jurisdiction are as follows:

Minimum Contacts Test: In ***International Shoe Co. v. Washington***[39] the minimum contacts idea was laid out. The court decided that a non-resident can be sued if they have certain minimum contacts with the state, as long as the litigation is maintained without jeopardising traditional notions of

[34] Kaspersky is a global cybersecurity company founded in 1997. Kaspersky`s deep risk intelligence and safety know-how is continuously remodeling into revolutionary safety answers and offerings to defend businesses, essential infrastructure, governments, and customers across the globe.
[35] Available at https://www.business-standard.com/article/technology/india-becomes-favourite-destination-for-cyber-criminals-amid-covid-19-121040501218_1.html
[36] Available at https://www.kaspersky.co.in/about/press-releases/2021_the-growing-cyber-threats-for-digital-india-kaspersky-report-reveals-that-35-of-indian-online-users-were-attacked-by-web-borne-threats-in-2020
[37] Available at https://www.thehindu.com/news/national/cybercrime-went-up-by-500-per-cent-during-pandemic-chief-of-defence-staff/article37457504.ece#:~:text=%E2%80%9CCyber%20crimes%20have%20gone%20up,states%20in%20such%20cyber%20attacks. (Last visited Feb 15, 2024)
[38] Summer Walker, *Contested domain: UN cybercrime resolution stumbles out of the gate*, GLOBAL INITIATIVE Against Transnational Organized Crime, 02 Jun 2021, https://globalinitiative.net/analysis/un-cybercrime-resolution/#:~:text=On%2026%20May%202021%2C%20a%20resolution%20on%20cybercrime,was%20voted%20through%20the%20United%20Nations%20General%20Assembly. (Last visited Feb 15, 2024)
[39] 326 U.S. 310, 66 S. Ct. 154, 90 L. Ed. 95 (1945)

guaranteeing substantive justice. To invoke the jurisdiction, the defendant's contact with the state must be established.[40] Therefore, the dispute must rise out of or be connected to the defendant's forum-related activity wherein exercise of jurisdiction must be justified.

Purposeful Availment Test: In the case of ***Cybersell Inc. v. Cybersell Inc.***[41] this test was explained. The issue of jurisdiction over the defendant was addressed by Cybersell in this three-part test: The non-resident defendant must first do something that invokes the forum's jurisdiction, as well as the benefits and protections that come with it.[42] Second, the claim must be based on the defendant's forum-related activity, and finally, jurisdiction must be exercised in a reasonable manner.

Sliding Scale Test: ***Zippo Manufacturing Co. v. Zippo Dot Com. Inc.***[43] is the case that gave birth to the sliding scale test. The following are the three groups: The first type is passive information, which provides viewers with information without allowing them to respond. Second, it is interactive, it enables the defendant to convey with the citizens of the receiving state, and the citizens of the receiving state can respond. Third, it is integral to the perpetrator's corporate; it is used by the defendant to make transactions with the citizens of the forum state and to transmit information from targeted consumers.

Effects Test: The Supreme Court founded jurisdiction in ***Calder v. Jones***[44]**,** on the idea that because the defendant knew his action would harm the plaintiff, he must be believed to have anticipated being dragged into court where the injury occurred. Because any conduct in cyberspace has consequences in multiple countries, effect cases are particularly important.[45]

Position in India

In India, the doctrine of *'lex foris'* (The Law of the Court or Forum) is made applicable. India doesn't recognize the applicability of any foreign law in the matters of procedural aspects.

Ramanathan Chettier v Soma Sunderam Chettier[46]

It was held in this case that India recognizes the established principle of private international law that the law of the forum, where the judicial proceedings are initiated, governs all procedural issues.

In India, the questions of jurisdiction are decided according to the Code of Civil Procedure, 1908. The Code does not contain individual rules regarding the jurisdiction of private international disputes. It contains specific provisions to meet the service requirements of cross-territorial procedures. When it comes to jurisdiction, the issue of substantive jurisdiction, not jurisdiction, is treated differently. In other words, jurisdiction issues arise in private international disputes, as do domestic disputes.

The norms in the code include general provisions regarding pecuniary boundaries, subjects, and territorial jurisdictions. Sections 16-20 of the Code resolve the issues of local jurisdiction regarding complaints.

Sadly, negligible cases involving personal jurisdiction related to cyberspace have been settled by the higher courts in India.[47] The preferred method is of "minimum contracts" US approach and in compliance with Code's proximity test. With current rules of international jurisdiction Indian courts are to adapt existing national rules to international conditions as needed you can analyze other regions of private international law. The court's reaction depends largely on the question of contract containing jurisdiction clauses or not.

CONCLUSION

As the virtual world is unreliable when compared to the physical world, courts are facing jurisdictional issues, as they are unable to determine the proper forum to hear cases involving cybercrime. Considering technology has advanced locally and internationally, there is a need for cybercrime laws to be regulated in order to prevent cyber-attackers from conducting any form of cybercrime, such as hacking, phishing, cyber stalking, and so on. To combat cybercrime in India, the Information Technology Act of 2000 was enacted to control criminal activity in the cyberspace. The right to privacy is guaranteed by Article 21 of the Indian Constitution, and different provisions of the Indian Penal Code impose penalties for cybercrime. One of the primary concerns in international standards with regard to cyberspace crime is jurisdiction issues in cybercrime. The criminal's nationality is producing a debatable jurisdiction issue based on the principle of territorial sovereignty. The lack of adequate national and international rules has made cybercrime investigation challenging. As cyberspace becomes more advanced, cybercriminals will develop new and additional progressive methods of committing cybercrime

[40] Anjaly Jolly, *Cyberspace Explained*, LAWLEX TEAM, APR 8, 2014, https://lawlex.org/lex-bulletin/cyberspace-explained/9567 (Last visited Feb 15, 2024)
[41] 130 F.3d 414 (9th Cir. 1997).
[42] Ashabari Basu Thakur, *DETERMINATION OF JURISDICTION IN CYBER-CRIMES: ISSUES AND CHALLENGES*, Legal Pedia, https://www.legalpedia.co.in/article/DETERMINATION%20OF%20JURISDICTION%20IN%20CYBER%20_%20Ashabari%20Basu%20Thakur.pdf (Last visited Feb 15, 2024)
[43] 952 F. Supp. 1119, 1124 (W.D. Pa. 1996).
[44] 465 U.S. 783, 104 S. Ct. 1482, 79 L. Ed. 2d 804, 1984 U.S. 41
[45] Anjaly Jolly, *supra* note at 42
[46] AIR 1964, Madras 527.
[47] Though there are a few cases on cyber crimes and domain name disputes. See for example, *BulBul Roy Mishra v City Public Prosecutor*, Criminal Original Petition No.2205 of 2006, decided April 4, 2006, (Last visited Feb 16, 2024)

thus a worldwide uniform cyber law is urgently needed to combat cybercrime by establishing a global institution and establishing authority to resolve the jurisdiction of cyberspace issues, including cybercrime sanctions.