GLOBUS

Cosmos An International Journal of Management
A Refereed Research Journal
Vol 9 / No 2 / Jan-Jun 2020 ISSN: 2278-1218

JURISDICTIONAL ISSUE IN CYBER LAWS

*Gauranshi

Paper Received: 11.06.2020 / **Paper Accepted**: 25.07.2020 / **Paper Published**: 27.07.2020

Corresponding Author: Gauranshi; Email: gauranshi@gmail.com; doi:10.46360/cosmos.xxxxxxxx

Abstract

With the advent of technology and the emerging trends of cyberspace, the issue of jurisdiction in the cyber world has been evolving immensely. Cyberspace has no physical boundaries or national boundaries and the growing exponential and dynamic space has led to a chaos and confusion with respect to the principles of jurisdiction.These problems in the internet world are essential causes of concern and international conventions are required for regulation of the cyber world. The aim of this paper is to evaluate the basic set of principles of jurisdiction and to determine the existing laws and conventions related to the issue of jurisdiction in cyber laws. The paper will further draw a comparison between U.S Approach, European Approach and Indian approach and how application of U.S. approach universally can aid in adoption of a universal convention.

Keywords: Cyber Laws, Jurisdictional Approach, Personal Jurisdiction, Universal Convention.

Introduction

With the growth in the exponential and the dynamic space, today, a 'click of a mouse' makes any website in the world accessible. These websites however are in the nature of agreements and they come with certain 'terms and conditions' including privacy policies, disclaimers, etc. These websites are set up based on the domestic laws of the home country and any transaction with such websites binds the user who might be accessing such a website from a different country. In case of any traditional dispute between individuals of two different countries, an individual seeks recourse under the 'private international law'. However, in case of a "cyber offence", the cause of action and the series of various acts relating to the offence might have taken place within the jurisdiction of different countries. This can create a difficulty in determining the jurisdiction of such a cybercrime.

Conventions on Cyber Laws

1. UNCITRAL Model Law
   The adoption of UNCITRAL Model Law on E-Commerce by the UN in 1996 introduced an equal legal treatment of users of electronic communication and paper based communication. However, this convention dealt merely with the issue of e-commerce. With the increasing number of users and transactions in the cyber world, there was a need for a universal convention on cybercrimes.

2. Budapest Convention
   Convention on Cyber Crimes, 2001 also known as Budapest Convention is the first international treaty related to the crimes committed by means of internet and other computer networks. It deals with crimes such as infringement of copyright, child pornography, computer-related fraud, network security violations, etc. It also deals with the jurisdictional issues regarding substantive crimes. The main objective of the convention as has been laid under the preamble is pursuance of a common criminal policy which aims at protecting the society against cybercrimes. The first step at attaining so is through adoption of appropriate legislation and fostering international cooperation.

However, Budapest Convention fails to address the issue of jurisdiction in cybercrimes. The provisions encourage all the countries (signatory) to cooperate 'to the wildest extent as possible' in relation to both cybercrimes and evidence collection in e-form. However, such mutual assistance is subject to certain conditions as per the law of the requested party or on the basis of the treaties of mutual assistance including the grounds on which cooperation may be refused by the requested party. Various treaties of mutual assistance have the requirement of the principle of dual criminality also.

Extra-territorial Jurisdiction in traditional laws

1. Principles of Jurisdiction
   Principles of jurisdiction domestically as well as internationally with regard to traditional issues took a long period to be developed and adopted and these principles have been further extended to the cyberspace and has resulted in the formation of a new term 'cyber jurisdiction'. These established laws and principles continue to hold validity with the aspects of online activities and has application in the cyber world.

   The meaning of jurisdiction has to be looked

*Law Student, Amity Law School, Delhi, India.

into from various perspectives: (a) Personal Jurisdiction, (b) Perspective Jurisdiction and (c) Enforcement Jurisdiction

a. Personal Jurisdiction
Personal jurisdiction approach has been adopted by the U.S. for many years. Since 1945, as laid down in International Shoe Co. v. Washington, the focus of the constitutional judicial inquiry has been on the 'minimum contacts' between the defendant, the forum and the litigation. It is necessary that the defendant must have such minimum contacts and purposeful availment with the forum state that assertion of jurisdiction by such a court does not offend the traditional notions of fair play and justice. This will be dependent on the "quality and the nature" of the acts of defendant with regard to fair administration of law insured by due process of law. For determination of minimum contacts, two inquiries shall be necessary: (a) the degree up to which the defendant had acted in the forum state (b) the relation between the acts and the claim brought against her.

Various landmark cases including the Shoe case and the Hanson case lay down the principle of exercise of personal jurisdiction in e-commerce disputes. Both Shoe and Hanson make assumptions about the physical contact of the defendant with the forum state. However, in the cyber world, there may not be presence of any physical contact of the defendant with the forum state. In such cases, the courts have taken into consideration various other jurisdictional paradigms such as level of interactiveness, nature of website, etc.

b. Perspective Jurisdiction
Perspective Jurisdiction refers to the application of own laws by a state for regulation of its conduct. When there exists such a jurisdiction, entities subject to the law of such a state are obligated to comply with it. The doctrine of choice of law is used to determine that while exercising control constitutionally whether the law of that state or that of another state is applicable.

In determining that whether a state may or may not exercise jurisdiction, two constitutional provisions under the U.S. regime are considered relevant: due process and the full faith and credit clause. The due process clause applies a restraint on the choice of a state to apply its own law. Full faith and credit clause require the court of one state to recognize and apply the substantial law of another state in a case when a forum state has no law of its own to apply.

c. Enforcement Jurisdiction
Enforcement jurisdiction is another jurisdictional paradigm necessary in handling the issue of cyberspace. A judgment can be enforced only in a forum wherein the assets of the defendant can be found pursuant to the order of a court for seizure by the executive and thereby turning over the proceeds to the plaintiff for satisfaction of the government. The grant of recognition to the judgments enforced by another court is necessary for enforcement of such a judgment in the forum state. Enforcement of a foreign judgment depends upon the presence of a personal jurisdiction in the rendering state.

2. Extradition laws for cyber criminals
Jurisdiction of a country is futile in case there are no proper extradition laws for execution of the decree of a court, its enforcement in another country and laws for extradition of the offender.

To determine the procedure for carrying out the extradition of cyber criminals, it is first necessary to understand the extra-territorial jurisdiction of states and the laws of extradition under the traditional international law.

a. Exercise of extra-territorial jurisdiction under International Law
A state can exert its extra-territorial jurisdiction under certain circumstances based on the principles of territory, nationality, protection of the nation, passive personality, effects doctrine, universality, etc. Jurisdictional principles of international law have cognizance of both State and international law. The traditional principles of international jurisdiction have now been extended to cyberspace for formulation of cyberspace jurisdiction.

b. Extradition under International Law
The procedures of extradition are designed for ensuring that criminals are sent back from one country to another and at the same time, the rights of the individuals who are accused of crimes by the requesting country must also be protected.

It is necessary that certain necessary evidence is shown prima facie in order to prove a case against the accused.

Extradition law is regarded as a dual law. Even though it forms part of the municipal law, it is also a part of international law in so far as it governs the relations of two sovereign states in deciding the question that whether an offender should be handed over by one sovereign state to another. Usually, the power to decide upon such matters vests on the national courts in accordance with the international law rules, commitments and treaties.

c. Extradition under Cyber Law
The Cyber Crimes Convention, 2001 also referred to as the Budapest Convention has facilitated in the extradition in cybercrimes. As per the laws of extradition, punishment is awarded for an extraditable offence if such an offence is punishable under the laws laid down by both the contracting parties involved in such an extradition. This rule is referred to as the Double Criminality Rule as per which that the alleged act committed by an offender should be an offence in both the requesting State and the requested State. It is pertinent to consider that the convention covers all kinds of cybercrimes and all these crimes have been made extraditable under the said Convention.

The Convention also states that when two parties involved in mutual assistance do not have an agreement for governing the request, Art.27 of the Convention states that the requests of the mutual assistance will have to be executed as per the procedures of the specific party except in situations when such procedures are incompatible with the laws of the requested party. Also, cooperation can be refused when it is considered that the offence is a political offence or when it is believed that providing of assistance can cause prejudice to the security, public order or sovereignty of the state.

Various extraditions for cyber frauds have been carried out between U.S. and other countries such as UK, Romania, Ukraine, etc. For instance, three nationalists of Romania including Cristea Mircea, Ion Pieptea and Nicolae Simion were extradited to U.S. from Romania for targeting U.S. based internet customers by websites such as eBay.com and thereby committing a multimillion dollar cyber fraud.

Jurisdictional Paradigms under Cyber Law

With the advent of technology, the assumptions of jurisdictions have changed for acknowledging the authority of a state and for asserting jurisdiction over individuals not within the physical boundaries. Here are certain relevant paradigms which have aided the states in determination of cyber jurisdiction.

1. Physical Location ‘lex situs’
Traditionally, in determination of circumstances of extraterritorial jurisdiction, courts and legislatures have placed their focus on the place where the cause of action arises or where does certain activities give rise to the claim of the plaintiff. However, in the technological world, there might not be any physical contact with the defendant.

If the remote party (i.e. the party which was never in contact with the forum state) has the knowledge that the proximate party is in the forum state when the interaction between both the parties take place, the remote party has thereby created a tie between itself and the forum state. Additional factors such as ‘targeting’ will determine that whether such a tie is sufficient for enabling a forum to assert personal and prescriptive jurisdiction.

For instance, a doctor in U.S. by means of detailed visual and virtual information which was supplied to her electronically by her patient in China, diagnoses the patient thereby prescribing a course of treatment. In such a case, it can be said that the doctor has created a tie between herself and the forum state of China.

a. Targeting
As it has already been said, the presence of physical contact in the electronic commerce is absent in almost all the cases. In these situations, it becomes necessary to determine what forum or fora are targeted by the activities of an individual or a business on the internet. Those who are desirous of attaining certain “benefit” (purposeful availment) from the forum state via Internet are said to ‘target’ the forum state and thereby such a foreign actor subjects himself or herself to such personal and perspective jurisdiction.

However, it has to be noted that maintaining of a website itself cannot be referred to as targeting the world. On the other hand, website which is designed only for targeting the population of a single forum, clearly targets that forum state. For instance, Amazon.in has been set up as a subsidiary of Amazon.com for targeting the population of India. The 'intent' of the author of the website is necessary to be taken into consideration. Ignorance of the location of the other party cannot be used as an excuse.

In the case of U.S. v. Thomas, the defendant raised a contention that he did not "push" the pornographic pictures into Tennesse and rather it was "pulled" in the jurisdiction of the defendant by someone whose computer had the ability to gather 0's and 1's from the server and thereby created a pornographic picture.

b. Power Parameters (Balance between buyer and the seller)
When jurisdictional rules are taken into consideration, it can be ascertained that these rules presume imbalance of power between the buyer and the seller. Traditionally, it is the sellers who set out the terms of the purchase contract. In contrast, e-commerce has led to expansion in consumer choice which has undermined the assumption that sellers are much larger than the buyers. As a result, technology has aided a balance between the buyers and the sellers.

c. Role of Artificial Intelligence
Cyber robots or 'bots' are used wherein the buyer becomes in-charge of the decision to buy. Agents are computerized by use of artificial intelligence wherein enormous amount of information with regards to goods, services, preferences, capabilities, etc. are used. These bots can roam in the virtual space without any human intervention and are endowed with such information wherein they can apply their artificial intelligence for conducting intellectual, social and commercial transactions with the other bots. They further have the ability to appoint sub-agents which have the ability to speak in multiple languages or communicate through the means of a "computer speak".

In Burger King Corp. v. Rudzewicz, it was held by the court that a mere contractual tie with a forum party cannot permit an assertion of personal jurisdiction over the non-forum state. The view of the court clearly establishes that it is the level of the relationship between the parties and to what extent was such a relationship actively sought which determines the extent of jurisdiction.

d. Contractual Choice of Law
Choice of Law doctrine allows the parties to the contract make an agreement among themselves beforehand that for resolving a dispute between them, these parties would seek remedy under any court of natural jurisdiction or by a neutral foreign court of their choice as per the laws applicable to the said court. Based upon its convenience, it is open for a party to fix the jurisdiction of a competent court for adjudication by their court.

Sellers are presumed to target the market and define the terms and conditions on the basis of which commerce is undertaken with the consumers. As a result, the enforcement of contractual choice of law and forum clauses becomes controversial. In U.S., such contracts are enforceable unless they are unreasonable. Europe on the other hand has expressed unwillingness to enforce the same unless it is favourable to the consumer. However, the basis of such unwillingness are disappearing.

e. Nature of a website
website is regarded as the virtual representation of a business model. For determination of the jurisdiction, it becomes relevant to look into the nature or type of the website model. A website can be mainly divided on the basis of its orientation i.e. (a) business oriented or (b) information oriented. Such websites can be further categorised into passive, active or interactive websites based on the level of their interactiveness.

In Bensusan Restaurant Corp. v. King, Court held that even though the website was accessible to any internet user in New York, certain steps are still required by an individual to access this particular website for obtaining a ticket. These steps include making a phone call to Missouri and to travel all the way to Missouri to pick up the tickets. This would mean that the infringement will occur in Missouri and not New York. Therefore, there is no purposeful availment by the defendant to access the benefits of New York.

f. Effects Doctrine

The doctrine of the effect test is an extended version of the 'targeting of the forum state' since the effect of 'out of state' conduct is also considered. Therefore, for establishing personal jurisdiction, three elements are essential including: (i) acts which determine intention, (ii) such acts are aimed expressly at the forum state and (iii) causing of harm wherein the defendant has the knowledge that the harm of such an act is either suffered or is likely to be suffered in the forum state. The level of interactivity is used under the 'effects doctrine' to determine jurisdiction

In Calder v. Jones, the Supreme Court of the U.S. that on application of the "effects doctrine", it is necessary that the due process requirement of the minimum contacts should be satisfied for establishing that out of state conduct was present in the forum state.

g. Case laws based on different aspects of cyber disputes

- Regulation of Free Speech
  In 'French' Yahoo Case, U.S. court upheld the First Amendment of the Constitution of U.S. which granted its citizens the right to freedom of speech against the order of French Court which had placed a requirement on Yahoo! for blocking the citizens of France and barring them from accessing the memorable of Nazis on the auction website of Yahoo!

- Online Publications of Defamatory Content
  Joe Gutnick had brought proceedings in the court of Australia against the publication of an article in Barron's Online, a magazine which was published by Dow Jones and Co. Inc. alleging that such an article was defamatory and caused a harm to his reputation in Victoria, Australia. In 2001, the Supreme Court of Victoria held in favor of Joe Gutnick stating that the publication of the said article occurred in Victoria, Australia wherein the article was downloaded by the subscribers in Australia and not when such an article was uploaded to the server of the publisher.

  In October 2002, International Bar Association in Durban, South Africa was organized wherein media lawyers from around 21 countries discussed the issues with regard to the jurisdiction on the Internet. This led to the introduction of Durban Principles as per which a site having no sale of goods or services and merely maintains content, ordinarily, the jurisdiction will lie with the country wherein the editorial work on such a content was completed i.e. the place where the decision for publication was made.

- Trademark infringement
  In the case of Cybersell Inc. v. Cybersell Inc., the US Court of Appeals for the Ninth Circuit was of the opinion that just by posting an essentially passive homepage on the web, defendant did don't substantially avail himself of the privilege of doing business. The mere fact that the website was accessible to the residents in Arizona was insufficient for supporting the inference that the merchandising efforts of the defendant were deliberated directly towards the residents of Arizona.

- Location of a web server
  In the case of Jewish Defence Organization, Inc. V. Superior Court (Ramban), an action for defamation was brought about by the plaintiff in the court of California. The relevant contact of the defendant with California was that the defendant had contracted with the Internet Service providers which were "located in California" for hosting a website maintained by them from their New York residence. The court was of the opinion that the conduct of the defendant in contracting with Internet Service providers via computer which have databases in California is insufficient to prove purposeful availment.

- Jurisdiction in E-contracts
  In the case of Bremen v. Zapata Off-shore Co., the court arrived at a judicial view that the clauses of forum selection in the agreements are valid prima facie and are enforceable unless the resisting party points out that the enforcement is unreasonable.

- Social media websites
  The decisions laid down by the U.S. Supreme Court in landmark cases such as Zippo case has been applied in various social media disputes for analysing the relevant social media activity. These landmark cases look into the principles of interactiveness and minimum contacts for exercise of personal jurisdiction. However, in reality, the current framework is not accurate and cannot be applied in a straight jacket form to social media disputes.

In the present scenario, there is lack of consistency among the courts in viewing the activities of the social media as useful or persuasive element for the determination of jurisdiction. With the application of the present principles, some courts have exceeded in exercising their jurisdiction on the activities of the parties. For instance, in Spectra Chrome, LLC v. Happy Jack's Reflections in Chrome, Inc., a court in Florida rejected the contention of the defendant that merely having a Facebook page does not subject a party to sufficient 'minimum contacts' with Florida. The court held that it had rightful jurisdiction since there was presence of minimum contacts.

Approaches to Cyber Jurisdiction Adopted By Different Countries

1. U.S. Approach
   In order to understand the jurisdictional approach applied by U.S. to the cyber world, it is necessary to understand the traditional principles of jurisdiction including the principles of personal jurisdiction, long arms statute, due process clause, etc.

   a. Personal Jurisdiction
   The competence of a court to decide a particular case and the determination of whether a person is subject to the court wherein the case is being brought up is regarded as the personal jurisdiction of the court. Personal Jurisdiction is further classified into general and specific jurisdiction. A court can ascertain its general jurisdiction with regard to any cause of action which might arise in such a court.

   The power of a Court with reference to a particular cause of action established on the basis of certain 'minimum contacts' with a forum state relating to the cause of action determines the specific jurisdiction of a state.

   For differentiating between specific and general jurisdiction, the court determines the presence of "minimum contact". If the court comes to a conclusion that there exists "systematic and continuous contact" with the forum state, the court shall have a general jurisdiction over the defendant.

   On the other hand, in the case of specific jurisdiction, it is not necessary that the defendant's contact with the forum state should be strong and 'minimum contacts' need not be established. The only thing that shall be taken into consideration is the place wherein the cause of action arose.

   b. Long Arm Statute
   S. authorizes its court to apply the principle of 'long arm statute' to claim personal jurisdiction over a defendant who is a non-resident and whose principal business is also outside such a state, however the action of such a non-resident should fall within such an activity which should be required for qualification of jurisdiction.

   c. Due Process of Law
   As laid down by the Fourteenth Amendment of the U.S. Constitution, a state should not deprive any person of life, liberty, or property without a due process of law. For instance in case of a dispute between an end user of U.S. and an E-Business of a different domicile, the end user shall be required to prove before a court that there exists application of "long arm statute" and there has been no violation of the due process rights of the defendant (E-Business). Such an E-Business can file a motion for dismissal and can argue that there does not exists any personal jurisdiction with the State.

   d. Application of Personal Jurisdiction in Cyberspace
   The issue of personal jurisdiction with reference to a non-resident has been dealt by the U.S. Courts in various cyber disputes. In International Shoe Co. V. State of Washington, Office of Unemployment Compensation and Placement et al, U.S. court was of the view that the personal jurisdiction over the non-resident defendant was proper because of the existence of certain 'minimum contacts' of the defendant with

the forum state in such a manner that the maintenance of the suit is at power with the traditional notions of substantial justice and fair play.

Certain criteria has been laid down for establishment of certain minimum contacts. Firstly, 'purposeful availment' must be present i.e. the defendant had a privilege of doing the business with such a forum state. Secondly, a cause of action arose as a result of the activities of the defendant in the forum state. Thirdly, the exercise of jurisdiction should be fair and reasonable.

In Cody v. Ward, Court held that it could exercise personal jurisdiction over the defendant based on the bulletin board messages, e-mail messages and telephonic conversations from the defendant in California to the plaintiff in Connecticut. The e-contracts of the defendant satisfied the requirement of "purposeful availment".

The study of the approaches to jurisdiction in the cyber space adopted by different countries and legal systems including U.S., Europe and India has been discussed in detail for providing a set of legal principles which can help in ascertaining the dynamics behind the personal jurisdiction exercised by different jurisdictions. Personal Jurisdiction has been successfully interpreted by the American courts. The number of case laws dealing with cyber offences has grown considerably in U.S. which have been dealt with effectively.

The courts have been competent in introducing new measures, theories, factors, etc. for resolving such disputes such as the nature of website, the theory of push and pull, geographical location of the user, owner of the website, web server, method of sliding scale, etc. The Courts have further adopted the traditional methods and laws in a precise manner such as the agreements of service, disclaimers, choice of law, forum clauses, etc. In contrast, the U.S. emphasizes on the approach of "minimum contacts" and "purposeful availment".

With regards to choice of law in contracts, both American and the European Approach aim at embracing party autonomy which is regarded as the basic rule which allows the contracting parties to make the choice of law which should be applied to the contract dispute. However, both the approaches allow significant exceptions. In the case of American Restatement, the exception is public policy or the absence of the chosen law and in case of Rome Convention, the exception is the mandatory rules of the state of the consumer or the state with the most significant contract.

2. European Approach

Europe applies a distinct personal approach in comparison to the American approach in the case of cross border disputes. European Court of Justice holds the decision making authority to determine what will constitute as "direct activities". A website can be said to be "directed to other states when such a website offers a choice of currencies of other states, languages, specification of product, delivery times, prices for items, etc. When a website promotes or targets products or services to consumers in specific European Union States, such an act amounts to marketing exercise.

As per Art.2 of the Brussels Regulation, persons who are domiciled in a contracting state shall irrespective of their nationality can be sued in the courts of such a contracting state. Further, Art.5.1 of the Convention suggests that a person who is domiciled in a contracting state can be sued in another contracting state in matters which are related to contracts in the courts for the place of performance of the contract.

Art. 15 further suggests that a consumer can alternatively bring a case at his home country, if the trader has pursued any commercial activities or has directed such activities in the Member State of the domicile of the consumer. Since websites can be accessed from anywhere, a trader having a website can direct the activities of such a website to all the EU countries.

Rome Convention determines the laws of which country shall be applicable to contractual disputes. The contracting parties are granted the freedom of choice of the place under the convention. Art. 4.1 suggests that when there is absence of choice of law, the law of the country with which it is most closely connected governs the contract.

It has been highlighted in both the Rome Convention and the Brussels Regulations that proceedings can be brought against a trader by a consumer in the place of his domicile or place of residence if there was existence of an advertisement or a specific invitation addressed to him prior to the conclusion of the contract. There exists an ambiguity in determining whether these articles are applicable to the cyber world and the online websites and whether such promotions by a trader on websites be regarded as specific invitation.

3. Indian Approach
Indian Courts have the power to exercise their extra-territorial jurisdictional power under the Sec. 3 and Sec. 4 of the Code. The said section was amended to bring it in consonance with the provisions of the IT Act, 2000. Clause (3) of Sec.4 states that the code shall stand applicable to any individual in any place beyond India who commits the offence of 'targeting' a computer resource located in India.

For the purpose of this section, it is necessary that the computer resource that is being targeted should be located in India. The said section also showcases the presence of 'effects doctrine' since the individual shall be charged with an offence under the Act when he has targeted any computer device in India effecting the situation of the individuals in India.

CrPC includes provisions for punishing the citizens of India for commission of offence outside India. It can be said that the jurisdiction in cyberspace is similar to jurisdiction in traditional crimes in India and subjective territoriality concept prevails. Besides, Sec. 178 of the act deals with the crimes or part of such crimes committed in India and Sec. 179 relates to the consequences of such a crime in India. However, amendments have not been made under the CrPC to punish cybercrimes.

Section 75 of the IT Act, 2000 grants the extra-territorial jurisdiction to India for punishing an individual irrespective of his nationality for committing an act of crime outside India when the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

India has exercised very wide universal jurisdiction in cyber offences which may not be possible in practicality and there may arise difficulty in execution of such a decree. Moreover, IT Act, 2000 is insufficient to address various issues. For instance, it does not include any provision for catching the internet pornography of foreign websites accessed by Indian citizens and is applicable merely to Indian websites. IT Act merely punishes cybercrimes and facilitates e-commerce and has no mention to deal with issues such as digital forensics, cyber security, data protection, etc. which makes it further difficult to determine jurisdiction in case of dispute.

Conclusion

On taking a look at the present scenario, it can be determined that the cybercrimes are increasing at an alarming rate and it is the need of the hour to have a convention which is broad based and which deals with matters of criminal substantive law, questions of criminal procedure, along with agreements and international criminal law procedures.

The Budapest Convention on Cybercrimes, 2001 appears to be insufficient in addressing the present jurisdictional issues in the cyberspace. A comprehensive international treaty might be necessary which encompasses not merely cybercrimes but the state behaviour also in cyberspace.

India was not a party to the said convention and has still not ratified the same. India has raised certain concerns for not signing the same such as exclusion of input from developing countries. India has although amended its IT Act, 2000 by the Amendment, 2008 to bring it at power with the Budapest Convention, 2001, it has issues with regard to what is included and what is excluded and its priorities are not in line with the Budapest Convention as it stands right now.

The laws of various countries have amended their extradition laws for facilitating the extradition of cyber criminals. For instance, the Extradition Act 1988 (Cth) (EA) of Australia sets out the provision for extradition of hackers located overseas in foreign jurisdictions.

On the other hand, various countries have still not made any such amendments in their extradition laws to deal with cyber disputes. With respect to India, the bilateral extradition treaties executed by India with more than 50 countries does not mention cybercrimes under extraditable offences.

In addition to it, the Letter Regoratory Procedures laid down under the CrPC enabling the investigation of a crime in a foreign country are fruitless and difficult to be carried out. Moreover, these laws have further no scope with regard to the computer crimes wherein the evidences related to the crimes can be destroyed swiftly.

In SIL Import v. Exim Aides Silk Importers, the Supreme Court was of the view that it is necessary for the judiciary to make interpretation of a statute by making allowances for the relevant technological changes occurring in today's world. Unless, there exists a specific legislation for determination of jurisdiction of the courts of India for handling of Internet disputes or unless Indian becomes signatory to any International Treaty wherein there is clarity with regard to the jurisdiction of the national courts and the situations and circumstances wherein such jurisdiction can be exercised, Indian courts can do nothing but give a very wide interpretation to the existing laws and statutes for exercising such jurisdiction in cases of Internet disputes.

It is further necessary to make amendments to the present extradition laws and make arrangements with other sovereign states for prosecuting the cyber-criminals thereby preventing them to escape from liability.

It is essential to note that there is absence of specific extradition laws in India for dealing with the crimes committed on Internet. For addressing these issues, it is necessary that India should become a signatory of the Convention of Cyber Crimes treaty and should ratify the same. Such a move can make a great deal in granting a resolution to the jurisdictional controversies which may arise in the cybercrime cases. Besides, amendments with regard to extradition of cyber criminals should be made in the present Extradition Act, 1962.

India should negotiate extradition treaties with the foreign states and such treaties should include the provisions related to cybercrimes. As said by Mr. Talwant Singh, CBI Special Judge, New Delhi, in his seminar in 2012 that India does not have a single extradition treaty wherein a cyber-criminal can be extradited to India.

It can be said that the cyber boundary of India has not been determined yet and it is essential to protect our cyber boundaries along with the physical boundaries. It is 2020 now, and India is yet to sign the extradition treaties with other countries with regard to cyber boundaries.

References

1. Details of Treaty No. 185, Convention on Cyber Crime, Treaty Office, Council of Europe, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
2. Art. 23 and 25, Convention on Cyber Crime, 2001.
3. Art. 14, Convention on Cyber Crime, 2001.
4. Art.29 to 34, Convention on Cyber Crime, 2001.
5. Art. 25(4), Convention on Cyber Crime, 2001
6. 326 U.S. 310 (1945); Office of Unemployment Compensation and Placement, 326 U.S. 310, 316, 66 S. Ct. 154, 90 L. Ed. 95, 161 A.L.R. 1057 (1945)
7. Prior to the Shoe decision, the focus of the courts was on statute's power to render and enforce a judgment (Pennoyer v. Neff 95 U.S. 714 (1877))
8. International Shoe Co. v. Washington 326 U.S. 310 (1945).
9. Hanson V. Denckla 357 U.S. 235, 253 (1958).
10. 14th Amendment, Section 1: … No state shall … deprive any person of life, liberty, or property, without due process of law;
11. Article IV, Section 1: Full faith and Credit shall be given in each State to the public Acts, Records, and judicial proceedings of every other state. This clause is most familiar in the U.S. litigation because of the requirement of enforcement of a valid judgment of another state, but by its terms it also defines the recognition one state must give to another's laws.
12. Article 24, Convention on Cyber Crimes, 2001.
13. Ibid.
14. Foltyn, Tomas, (2018). Quarterly cyber crime digest: Extraditions and more. We Live Security by Eset. April 17. https://www.welivesecurity.com/2018/04/17/quarterly-cybercrime-digest-extraditions/; BBC (2018) Lauri Love Case: Hacking suspect wins extradition appeal. BBC News. February 5. https://www.bbc.com/news/uk-england-42946540; Helena Horton and Cara McGoogan (2018) British hacker Lauri Love wins fight against extradition to US. The Telegraph. February 5. https://www.telegraph.co.uk/news/2018/02/05/british-hacker-lauri-love-wins-fight-against-extradition-us/
15. Department of Justice (2013) Three Members of International Cyber Fraud Ring Extradited From Romania to the United States, U.S. Attorney's Office, May 2.
16. 117 S Ct. 74 (1996).
17. 471 U.S. 462 (1985)
18. Art. 7 of the Hague Convention.
19. 937 F. Supp. 295 (SDNY,1996)
20. 465 US 783, 789 (1984)
21. Yahoo! Inc. v. LICRA 169 F. Supp. 2d 1181 (N.D. Cal 2001)
22. 130 F.3d 414 (9th Cir. 1997).
23. 72 Cal.App.4th 1045, 85 Cal.Rptr.2d 611 (1999).
24. 407 U.S. 1, 9-10 (1972).

25. Tiffany Hendricks & Cecilia Gonzalez, "Social Media, The Internet & Jurisdiction" The Social Media Esquire, Wordpress, April 9, 2015. [online] Retrieved from: https://thesocialmediaesquire.wordpress.com/2015/04/09/social-media-the-internet-jurisdiction/
26. 2011, WL 1337508 (M.D. Fla. 2011).
27. Ferrera, G.R, Lichtenstein, D.S., (2000). Cyber Law- Text and Cases, p. 21, (West Thomson Learning, USA, 2000)
28. 326 U.S. 310, 316 (1945).
29. 95 F. Supp. 43 (D. Conn. 1997).
30. UK Department of Trade and Industry (DTI)
31. Indian Penal Code, 1860.
32. Kovacs, Anja, (2015). Addressing India's global cyber security concerns: Norm Development, Regulatory Challenges, Alternative Approaches. New Delhi: Internet Democracy Project: https://internetdemocracy.in/reports/india-and-the-budapest-convention-to-sign-or-not-considerations-for-indian-stakeholders/#fnref:20
33. Singh, Vikram Pratap, (2013). India Won't Sign Budapest Pact on Cyber Security. Governance Now, October 15, 2013. http://www.governancenow.com/news/regular-story/india-wont-sign-budapest-pact-cyber-security
34. Bhaumik, Anirban, (2012). India, Allies to Combat Cybercrime. Deccan Herald, May 16, https://www.deccanherald.com/content/249937/india-allies-combat-cybercrime.html
35. Sec. 166A and Sec. 166B, CrPC, 1973.
36. (1999) 4 SCC 567.
37. "Cyber Jurisdiction in India" Lexwisdom, November 4, 2012. [online] Retrieved from: https://lexwisdom.wordpress.com/2012/11/04/cyber-jurisdiction-in-india/
38. "Cyber Jurisdiction in India" Lexwisdom, November 4, 2012.
39. India TV News Desk, (2012). No extradition treaty signed in respect of cybercrimes, India TV, October 5, https://www.indiatvnews.com/crime/news/no-extradition-treaty-signed-in-respect-of-cyber-crimes-1753.html
40. Talati, Juhi, (2019). Cyber Crime: Default in success of conviction due to lack of jurisdiction, Legal Services India, http://www.legalservicesindia.com/article/1374/Cyber-Crime:-Default-in-success-of-conviction-due-to-lack-of-jurisdiction.html.
41. Agarwal, Ekansh, (2019). A Review of Test Prioritization Regression Testing Based On Time. Globus: An International Journal of Management and IT, 11(1); 35-38.
42. Gupta, Sakshi and Jayant, K.P., (2019). A Review Study on Phishing Attack Techniques for Protecting The Attacks. Globus: An International Journal of Management and IT, 10(2); 22-25.
43. Solanki, Anuj, (2018). Information Security Objectives. Globus: An International Journal of Management and IT, 9(2); 1-3.