

# **CYBER LAW -I**

**By: Veena Kumari**

Faculty of Law

University of Lucknow

Lucknow

Disclaimer: This content is solely for the purpose of e-learning by students and any commercial use is not permitted. The author does not claim originality of the content and it is based on the following reference.

**LLB.(Hons) (Fifth Year) IXth Semester**

**(Optional Paper) : Paper-VII-E**

**&**

**L.L.B.(Three years course)(Third Year) Vth Semester**

**(Optional Paper) : Paper VII. F**

**Cyber Law – I**

**Unit I : Cyber Space**

- Fundamentals of Cyber Space
- Understanding Cyber Space
- Interface of Technology and Laws Defining Cyber Law

**Unit II. Jurisdictional Issues in Cyber Space**

- Jurisdiction in Cyber Space
- Concept of Jurisdiction
- Internet Jurisdiction
- Indian Context of Jurisdiction
- International position of Internet Jurisdiction Cases in Cyber Jurisdiction

**Unit III. E-commerce- Legal issues**

- E-commerce- Legal issues
- Legal Issues in Cyber Contracts
- Cyber Contract and IT Act 2000
- The UNCITRAL Model law on Electronic Commerce

**Unit IV. I.P.R. & Cyber Space**

- Intellectual Property Issues and Cyberspace – The Indian Perspective
- Overview of Intellectual Property related Legislation in India
- Copyright law & Cyberspace
- Trademark law & Cyberspace
- Law relating to Semiconductor Layout & Design

# Jurisdictional Issues In Cyber Space

## I. Jurisdiction in Cyber Space

**Cyberspace** is a concept of recent origin and evolving everyday with the development of sophisticated technology in the form of software and hardware. The nature of cyberspace has challenged the traditional notion of jurisdiction of court world over.

**Jurisdiction** is the power of State to regulate the conduct of its subjects by legislations, adjudication and enforcement. The current module only deals with the adjudicative jurisdiction of court prescribe by State to resolve issues and fix the liability of parties.

**Cyber Jurisdiction** or **Jurisdiction in Cyber Space**- In simple terms, is the extension of principles of international jurisdiction into the cyberspace. Cyberspace has no physical (national) boundaries. It is an ever-growing exponential and dynamic space. With a 'click of a mouse' one may access any website from anywhere in the world. Since the websites come with 'terms of service' agreements, privacy policies and disclaimers – subject to their own domestic laws, transactions with any of the websites would bind the user to such agreements. And in case of a dispute, one may have recourse to the 'private international law.

In case the “**cyberspace offences**” are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of services of such networks to commit traditional offences, then one may find oneself in the legal quagmire. The question is not only about multiple jurisdictions but also of problems of procedural law connected with information technology. The requirement is to have broad based convention dealing with criminal substantive law matters, criminal procedural questions as well as with international criminal law procedures and agreements.

## I. Concept Of Jurisdiction

The word jurisdiction is derived from Latin “*juris-dictio*” meaning ‘the saying or speaking of the law’. It indicates the value, validity and articulation . The concept of jurisdiction of a court emanates from the Sovereignty theory and Territorial Theory of State.

The authority of a court to hear a case and resolve a dispute involving person, property and subject matter is referred as the jurisdiction of that court. It is the legislative function of the Government to enact laws and judicial and/or administrative function to enforce those laws. Thus, the principles of jurisdiction followed by a State must not exceed the limits which international law places upon its jurisdiction. Jurisdiction is the authority of a court to hear a case and resolve a dispute involving person, property and subject matter. These principles of jurisdiction are enshrined in the constitution of a State and part of its jurisdictional sovereignty. All sovereign independent States possess jurisdiction over all persons and things within its territorial limits and all causes, civil and criminal, arising within these limits.

**Types of Jurisdiction includes:**

**Generally there are three kind of jurisdiction i.e.**

**Legislative, Enforcement and Adjudicative Jurisdiction.**

Jurisdiction to legislate is the right of a State to prescribe the normative standards for the regulation of its subjects. However the State has to take into consideration the limitation of international law in the exercise of jurisdiction in cases that involve non territory entities. The prescriptive jurisdiction of state is not unlimited as the State would not like to prescribe a conduct for the enforcement of which there is no basis in the practical aspect. In fact unlimited power of prescription measures will seriously undermine the sovereign authority of the other State. As per the international customary norms the State is obliged not to interfere in any form or for any reason whatsoever in the internal and external affairs of other State. Therefore generally State adopts the principle of territoriality or effects doctrine and the legislative power of the State.

**Personal Jurisdiction:** The authority of a court to hear and decide a dispute involving the particular parties before it. Types of Personal Jurisdiction.

**Personal Jurisdiction may be further classified into following 2 types:**

**General Jurisdiction** - The "general" jurisdiction subjects a person to the power of the applicable court with respect to any cause of action that might be brought. It has historically relied on very close contacts of the person with the state, such as residency or domicile within the state, physical presence in the state at the time of service of process, or some other substantial "continuous and systematic" contact with the forum state.

**Specific Jurisdiction** - The "specific" jurisdiction, refers to the power of the applicable court with respect to a particular cause of action based upon some set of "minimum contacts" with the forum state that relate to that cause of action.

**Subject Matter Jurisdiction:** The authority of a court to hear and decide a particular dispute before it.

**Original Jurisdiction:** The authority of a court to hear and decide a case in the first instance over the authority of other courts. For example, trial courts are courts of original jurisdiction in many cases.

**Appellate Jurisdiction:** The authority of a court to review a prior decision in the same case by another “lower” court.

**The jurisdiction is to be based on different principles and theories and tests:**

Jurisdiction is the basic rule of fair play which is essentially two-dimensional in both civil and criminal matters. While in **civil matters** it comprises of ; **subject- matter jurisdiction** and **personal jurisdiction**, in criminal matters it is **personal** and **territorial**, related to the place of commission of crime. As regarding civil jurisdiction, variable rules are found when contractual, consumer, copyright, intellectual property and trademark disputes are concerned. Wherever overlapping jurisdictions were manifested in litigations, they were resolved by resorting to theories like choice of law rule and minimum contacts theory

**Subjective territoriality** Under the subjective aspect of territorial jurisdiction a sovereign is recognized as having the power to adopt criminal laws that apply to crimes that are physically committed within his territorial borders. As other states make inadequate adjudication hence the state extend the subjective territorial principle and expand their Net to bring the culprit within their domestic laws. The said principle extends jurisdiction to activities which commence within a State’s geographical territory but completed or consummated in other territories. So, for example, the United Kingdom can adopt a statute that makes it a crime for anyone to commit an act of murder within its borders.

**Objective territoriality** – Under the objective aspect of territorial jurisdiction a sovereign is recognized as having the power to adopt a criminal law that applies to crimes that take effect within its borders even if the perpetrator performs the act outside of its borders.

In other words, Under this principle jurisdiction of the State is extended to those acts that are commenced in another state’s territory but either

- (a) Consummated or completed in its own land or
- (b) Such activities produce harmful effects in the territory of the party extending jurisdiction .

The consummation of activity factor is complement to the subjective territorial principle.

**Principle of Nationality:** It applies where the alleged offender is a national of the State, the laws of which have been violated by his acts. In India, according to IPC, an Indian national is liable to prosecution in India for an offence committed in a foreign country which is punishable under Indian law. (Sec 3) Punishment of offences committed beyond, but which by law may be tried within, India.—Any person liable, by any [Indian law] to be tried for an offence committed beyond [India] shall be dealt with according to the provisions of this Code for any act committed beyond [India] in the same manner as if such act had been committed within [India]

**Principle of passive personality-** The passive personality principle gives jurisdiction to a State over the activities of foreigners which harms the nationals of that foreign state. This test is detested by customary international law too and in the Lotus case the Turkey Statute justified the jurisdiction.

**Principle of Universality.** Universal Jurisdiction: ☒ Another form of assuming jurisdiction is known as universal jurisdiction or the universal interest jurisdiction. ☒ As the name points out, this jurisdiction is assumed by any State to prosecute an offender for acts which are known universally by International law to be a heinous crime, i.e. hijacking, child pornography, cyber terrorism etc. ☒ A cyber criminal can be prosecuted by any country based on universal

**Protective Principle-** As the term suggests this principle comes to play where security of any state endangered by the act of any foreign national. According to the principle a state has jurisdiction in respect of “certain conduct outside its territory by persons that directed against the security of the state or against a limited class of other state interests.

### **Tests to determine jurisdictions:**

#### **1. Minimum Contacts theory**

The Minimum Contact theory comes into picture when either or both of the parties seem to be from outside the Court's territorial jurisdiction. It is used as a method to establish the Court's jurisdiction over the parties to a case by determining their quality and intensity of their contact i.e. services or transactions with the Forum State. ☒ Minimum contact rule establishes that so long as a corporation had a degree of contact within the state bringing suit, they are subject to the laws of the state and can be sued by and within the forum state in court. ☒ Examples of minimum contacts include conducting business within the state, incorporating in the state, and visiting the state.

The theory was laid down in a landmark case i.e. **International Shoe Co. v. Washington, 326 U.S. 310 (1945)**. There was a landmark decision of the Supreme Court of the United States in which the Court held that a party, particularly a corporation, may be subject to the jurisdiction of a state court if it has "minimum contacts" with that state. The ruling has important consequences for corporations involved in interstate commerce. It was held: Suit cannot be brought against an individual unless they have minimum contacts with the forum state.

Following International Shoe, courts have generally applied a three- part test in evaluating minimum contacts sufficient for jurisdiction:

- (1) The non-resident defendant must do some act or consummate some transaction with the forum or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections.
- (2) the claim must be one which arises out of or results from the defendant's forum-related activities; and (3) exercise of jurisdiction must be reasonable.

#### **2. Effects test or Calder Effect Test**

The theory was laid down in a landmark case i.e. **Calder v. Jones, 465 U.S. 783 (1984)**, It was a case in which the United States Supreme Court held that a court within a state could assert personal jurisdiction over the author and editor of a national magazine which published an allegedly libellous article about a resident of that state, and where the

magazine had wide circulation in that state. ¶ Held :A state's courts could assert personal jurisdiction over the author or editor of a libellous article, where the author or editor knew that the article would be widely circulated in the state where the subject of the article would be injured by the libellous assertion. Held that California courts had jurisdiction over the defendant.

**Fact of the case :** The plaintiff, actress Shirley Jones sued the defendants, the National Enquirer, its distributor, the writer of the article, and Calder, the editor-in-chief of the magazine, over an October 9, 1979 article in which the Enquirer alleged that Jones was an alcoholic. ¶ Jones lived in California, and although the Enquirer article had been written and edited in Florida, Jones filed her lawsuit in a California state court. ¶ Jones asserted that the court had jurisdiction based on the large circulation Enquirer enjoyed in California. ¶ . Held that California courts had jurisdiction over the defendant.

**Following conditions needs to be satisfied-**

- (a) an intentional action,
- (b) that was expressly aimed at the forum state,
- (c) with knowledge that the brunt of the injury would be felt in the forum state.

Note: If a court finds that a defendant's actions meets the standard of purposeful direction, then personal jurisdiction may be asserted based on Internet activities which do not meet the requisite level of interactivity or minimum contacts needed for other tests of personal jurisdiction in Internet cases.

**3. Personal Jurisdiction Theory**

All the person living within a defined area fall under the jurisdiction of court concerned. But the dispute takes place when the party or parties live out of its jurisdictional territory or even out of the said political entity or country. This jurisdiction receives a definite setback in the internet arena as in it, almost in every country there are a number of cases, civil or criminal in which one party or the accused is a resident of another country .

However, this traditional theory was slightly twisted by the court in **Zippo manufacturing Co. V. Zippo Dot Com Inc** . Which propounded the “**sliding scale**” theory which said that the nature of the defendant activity is the decisive factor in determining jurisdiction. Website which is passive , does not entail personal jurisdiction.

**4. Sliding scale theory**

The "sliding scale" or "Zippo" Test has been generally accepted as the standard in Federal Courts in deciding personal jurisdiction in Internet cases. Such cases are now primarily decided based on a determination of the website's "interactivity". Courts have held that the greater the commercial nature and level of interactivity associated with the website, the more likely it is that the website operator has "purposefully availed itself" of the forum state's jurisdiction.

**5. Choice of law theory**

There is a choice of laws option in case of conflict of law situation. There are in the physical world a number of approaches which govern the transnational disputes ; for example the “choice of law methodologies to mitigate the “ spill over effects” , the rule of international law, etc.

#### **6. Country-of -origin or Country of destination theory**

There are divergent opinions regarding the rules country- of- destination applicable to online commercial activity as the business house is required to answer in a law court a few 100 miles away for non compliance with the law of that country. Then it will become not only impractical for the entrepreneur to run business in this way but it will also have to be on an extra charge to face a litigation outside and away from their own jurisdiction.

#### **7. Forum Selection Theory**

In fact, the parties may themselves agree beforehand that for resolution of their disputes, they would either approach any of the available courts of natural jurisdiction or to have the disputes resolved by a foreign court of their choice as a neutral forum according to the law applicable to that court. Thus, it is open for a party for his convenience to fix the jurisdiction of any competent court to have their dispute adjudicated by that court alone. In other words, if one or more courts have the jurisdiction to try any suit, it is open for the parties to choose any one of the two competent courts to decide their disputes. In case parties under their own agreement expressly agree that their dispute shall be tried by only one of them then the parties can only file the suit in that court alone to which they have so agreed.

- **In Modi Entertainment Network v. W.S.G. Cricket Pvt. Ltd.,** it was held that it is a well-settled principle that by agreement the parties cannot confer jurisdiction where none exists, on a court to which CPC applies, but this principle does not apply when the parties agree to submit to the exclusive or non-exclusive jurisdiction of a foreign court

## **II. Internet Jurisdiction “Lex loci delicti “ rule**

### **“Cyber Crimes have extraterritorial aspect.”**

In the pre Internet period , personal jurisdiction was understood in terms of territoriality. The Physical Presence Theory (service within jurisdiction) is one of the core theories on which a court may claim to exercise jurisdiction over a defendant .

Cyber space is a broad term which includes computers, networks, software, data storage devices, the Internet, websites, emails and even electronic devices such as cell phones, ATM machines etc.

When one is online ,one is almost everywhere. Traditional interpretations spelled limitations be it subject matter related or territorial ,in the internet Age it means earth wide. As a single act on the net is the work play of several participants, as there are website owners, the online intermediaries ,the host ,the author or creator of a piece of writing or painter,etc, the corporate, the end user and so on. Hence a single infraction or wrong may

involve all or some of these and again as the nature of Net goes, it is quite possible that all of these come from various countries and hence, from various jurisdiction, In such a case , even if one applies traditional principles of jurisdiction some of these may fall in different jurisdiction by virtue of subject matter jurisdiction and some may fall under yet another jurisdiction due to personal jurisdiction and yet some of the participants may remain uncovered by these principles.

This leads to the birth of a law of cyberspace based on private contracting on a global basis and enforced by a combination of the SYSOP's (system operators) ultimate right to banish unruly users and the users ultimate right to migrate to other online service providers (such as ISPs).

Traditional theories of jurisdiction are inapplicable to the Internet due to the following reasons:

- 1.material posted on the internet has worldwide audience;
- 2.It is easy to move website from one territory to another;
- 3 .A website can be hosted on one area, but directed at users in another geographic location;
- 4.Parts of a website may be hosted in one area, while other parts of the websites are hosted in another location; and
- 5.It is not always possible to determine where a website or user is located.

#### **Areas of conflict : Traditionally notions of jurisdiction and the Internet**

The advent of internet culture gave the concept of a virtual world called as Cyber space which is basically a virtual environment created by interconnected computers and computer networks on internet without any boundary of distance and physical limitations and overturned the century-old established theories of jurisdiction which were deeply rooted in the territorial and physical concept. While the Internet absolutely negates tangibility and terrestrial forms; applicability of laws of the physical world are bound to face unprecedented legal hardships.

#### **The main areas of conflict are discussed in the subsequent sections-**

**Inter- sovereign conflict** - Extension of laws of one State to another has been an unimaginable concept unless it is backed by some treaty between the two states. For the Internet environment, this is the first requirement as the borderless cyberspace has no established norms.

**Hypothetical situation-** X, a physician registered in the UK, diagnoses and prescribes medicine through a website to patients in India. A dispute thus arising between X and any patient in India, an Indian court can claim subject matter jurisdiction over the matter and issue, either summon or warrant to X to achieve his presence in the court saying that X is treating patients in India without being formally registered here. This situation will obviously give rise to a conflict between UK and India and according to the traditional notion of

sovereignty, both the countries are rightfully exercising their jurisdiction and authority over the matter. This conflict has actually occurred in several cases like **Yahoo! Inc. V. Ligue Contre Racisme et L'Antisemitisme** , **United States v. Thomas**, etc.

**Over inclusiveness-** The traditional view rests on the concept that every sovereign state has unquestionable authority within its geographical limits but when a website is created, the server is physically located within the boundaries of the state concerned. While as State, as according to the traditional notions , has legitimate control over its subjects and over the physical infrastructure of the Internet (server, etc.), the particular web page being visible in any part of the globe , all the 300 states of the planet may have; applying the same traditional notions equal authority and interest.

**Under inclusiveness-** In this dimension of traditional theories States are forbidden to cross the limit in in case of dispute arises between the parties from two different jurisdiction. It shuns the Idea of crossing these boundaries and advocates the limits of a states authority within its territorial boundaries.

Thus the under-inclusiveness of traditional concepts is revealed because the States that want to regulate internet activities cannot effectively enforce their laws against “purveyors of harmful material through the Internet” who are located outside their territorial borders.

### **III. Indian Context of Jurisdiction**

The adjudication jurisdiction is the power and authority of a court to decide a dispute. The court adjudicate the matter depending on the subject matter, pecuniary value and local limits involved in the issue. The jurisdiction of court is generally based on the territorial nexus of the defendant and the cause of action. In Indian context the Code of Civil Procedure and Criminal Procedure Code incorporates the jurisdiction of the Court in the case national and international aspects of issues.

In case of India the **general jurisdiction** rules are contained in **Code of Civil Procedure, 1908(“Code”)** The Code has specific jurisdiction provisions relating to moveable, immovable property in **section 16 to 18**. In case of moveable property the jurisdictional rule is mostly defendant centric and in case of immovable property it is the lex situs rule prevails i.e., the law of the forum where the property situated. Section 20 of the Code covers the international jurisdiction and has interpreted in the internet related cases.

#### **Jurisdiction under the Information Technology Act, 2000**

The substantive source of cyber law in India is the **Information Technology Act, 2000 (IT Act)** which came into force on 17 October 2000. The objective of the Act is to provide legal recognition to e- commerce and to facilitate storage of electronic records with the Government.

- The State legislative enactments primarily reflect its prescriptive jurisdiction. For example, the IT Act, 2000 provides for prescriptive jurisdiction as it States: “The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.”.
- Further this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.
- It is the legislative function of the Government to enact laws and judicial and/or administrative function to enforce those laws. Thus, the principles of jurisdiction followed by a State must not exceed the limits which international law places upon its jurisdiction.

**The Indian Information Technology Act under the Section 1(2) and Section 75 of the Act incorporates the effect test of jurisdiction.**

The IT Act also penalizes various cybercrimes and provides strict punishments. In pursuant to this there are certain provision under this act which renders the idea of jurisdiction of court for the trial of cases pertaining cyber crimes in India as well as outside India.

**Provisions of IT Act are as follows:**

**Sec 1 specifies the extent of the application of this act. It states that:**

(2) It shall extend to the whole of India, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

**Sec 75 deals with the provisions of the act to apply for offences or contravention committed outside India.**

It states that: subject to the provision of sub section (2), the provision of this act shall also apply to any offence or contravention committed outside India by any person irrespective of his nationality.

For the purpose of sub section (1), this act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

**Sec 46 of the Act renders power to adjudicate in case of contravention** of any provision of this act and for the purpose adjudging it provides for the appointment of adjudicating officer who is vested with the powers of civil courts which are conferred on the Cyber Appellate Tribunal

**Sec (48) of the act provides for the Establishment of Cyber Appellate Tribunal**

- (1) The Central Government shall, by notification, establish one or more appellate tribunals to be known as the Cyber Regulations Appellate Tribunal.

**Sec.( 61) Civil Court not to have Jurisdiction**

**No Civil Court shall have jurisdiction to entertain any suit or proceeding in respect of any**

**matter which an adjudicating officer or the Cyber Appellate Tribunal is empowered to determine under this Act. No court shall grant injunction in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.**

**Sec. (62) Appeal to High Court:**

Any person aggrieved by any decision or order of Cyber Appellate Tribunal may file an appeal to the High Court within 60 days from the date of communication of such decision or order. An appeal may be on any question of fact or law arising out of such order.

The High Court may allow it to be filed within a further period of 60 days, if it is satisfied that sufficient cause prevented him from filing the appeal within the prescribed period

**The Information Technology Act 2000** seems exhaustive when it comes to adjudicate the matter where the parties are Indian citizen and the offence or any contravention has been committed in India as the Indian Courts follow the Principle of *lex foris* that means the law of the country but it still creates confusion in order to exercise its extra territorial jurisdiction where the offence has been committed outside India or by any non-citizen.

For instance, if an American citizen damaged the reputation of one of the Indian Politician by publishing lewd comments through the social media and the aggrieved person approached to Indian court for the justice. It is obvious that **IT act, 2000** provides for extra territorial jurisdiction but the issue arises here that how far would it be effective to bring the American citizen to India to be prosecuted for cyber defamation as the IT Act is not applicable to the American citizen.

Jurisdiction is a major issue which is not satisfactorily addressed in the ITA or ITAA. Jurisdiction has been mentioned in **Sections 46, 48, 57** and **61** in the context of adjudication process and the appellate procedure connected with and again in **Section 80** and as part of the police officers' powers to enter, search a public place for a cyber crime etc. In the context of electronic record, **Section 13 (3) and (4)** discuss the place of dispatch and receipt of electronic record which may be taken as jurisprudence issues.

In the case of **India TV Independent News Service Pvt. Limited v. India Broadcast Live Llc & Ors.**<sup>15</sup> the court applied the effect test of USA Court. The case is related to the launching of leading TV channels "INDIATV" in March 2004. As per the plaintiff the mark was adopted since 01.12.2002 and they applied for registration of the same mark on 22.01.2004. The mark was published in 2006 without any objection within the stipulated period. During the search on internet plaintiff discovered the website <indiatvlive.com>. Plaintiff filed a suit against defendant for permanently restraining the defendant from the use of the mark. The Defendant questioned the jurisdiction of the court as they claimed that they were American entities and don't reside or work for gain in India. Realising the incompetency of the traditional jurisdictional rules due to outside Indian territorial jurisdiction the court referred to jurisdiction rule of the USA court.

Further, in the case of **Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy** - the Plaintiff Company involved in hospitality industry had registered office at Singapore and

defendants were from Hyderabad. It adopted the mark “Banyan Tree” and Banyan tree as device and maintain website <www.banyantree.com>, <www.banyantreespa.com> since 1996. The Banyan tree was not a registered mark as per the law of the land as the application was pending for registration. Defendant initiated the project by the name “Banyan Tree Retreat” and advertised on website. Plaintiff filed case with Delhi High Court alleging dishonesty on part of the defendant. The court raised some important questions and replied it applying the jurisdiction rules of the USA court.

The case of **Super Cassettes Industries Ltd. v. Myspace Inc. & another**, is related to copyright issues, cyber law and international jurisdiction. The plaintiff filed the suit for restraining infringement of copyright, damages etc. through website of Myspace having base at US. Defendant Myspace raised the jurisdictional objection on the ground that:

- (1) The defendant is residing and carrying on business outside the jurisdiction of this court i.e., USA,
- (2) The cause of action has not occurred within the territorial jurisdiction of Indian court.

The Court in the case discussed jurisdiction rules of Copyright Act and the Code in detail. The Court emphasising on **Section 62 of the Copyright Act** held that the **specific jurisdictional** provision is plaintiff centric and due to non obstante clause it will operate in additions to what has been provided in the Code. This is to be treated as an additional ground above the normal grounds laid down in **Section 20 of the Code of Civil Procedure**. The operation of the rule under **Section 20 CPC** is not absolute and is subjected to the municipal law. If municipal law provides otherwise or overrides the Private International Law principles, then the municipal law will prevail. In the given case the Code of Civil Procedure rules are overridden by the **Copyright Act 1957** rules on jurisdiction. Deliberating on the jurisdiction ground of ‘torts’, the Court held that the commission of the tort is India.

The website of the defendants was engaged in providing the online business worldwide including India. The tort or civil wrong is caused in India as the act of downloading of copyrighted songs has occurred in India without the permission of the plaintiff. In case where the work is uploaded by the user on the foreign server, the initiation of the tort or part of the same has occurred in India as the infringing work without the authority of the plaintiff is communicated to the defendant with a limited licence to further modify and communicate further. The said commission of the acts or the part of the overt acts constitutes the part of cause of action within the meaning of **Section 20 (c)** of the Code of Civil Procedure and therefore the court have jurisdiction even on the basis of the cause of action clause of CPC.

**Apart of IT Act 2000, there are other relevant legislation under Indian laws that gives the authority to India Courts to adjudicate the matters related to cyber-crimes such as:**

### **Contract**

Traditionally in case of contract the parties enjoy the autonomy of having option to make choice of court agreement relating to the future contractual disputes. The same autonomy

is applicable in the case of online contracts also. It is established principle that where more than one court have jurisdiction in a certain matter, the agreement between the parties to confer jurisdiction only on one, to the exclusion of the other is valid and cannot be considered contrary to law. The same rule is applied to cases involving foreign elements.

The Court in the case of **Hakam Singh v. Gammo (India) Ltd.** laid down two important conditions for the application of autonomy to decide the jurisdiction of the court.

1. first, the Court selected by the common consent should have inherent jurisdiction,
2. second, more than one court should have the jurisdiction so that the choice of forum agreement can be exercised.

However in case where the parties have not selected or applied their autonomy regarding the jurisdiction of the court then jurisdiction can be fixed on the basis "cause of action". The "cause of action" arises in the following places:

1. The place of formation of contract i.e., where the contract has been entered;
2. The place of performance i.e., where the contract is performed or is required to be performed as per the terms of contract;
3. The place where, the consideration is made

### **Jurisdiction Based on Code of Civil Procedure, 1908**

The concept of jurisdiction can be understood in a better way with reference to **section 15 to 20 of code of civil procedure (1908)**, which talks about the place of suing or the subject matter jurisdiction and section 20 of this code specifically speaks about any other category of suit which is not covered in **section 15 to 19 of the code**. Section 20 serves important ingredients for the purpose of institution of other suit in a court within the local limits of whose jurisdiction' the defendant or each of the defendants resides, or carries on business, or personally works for gain at the time of the commencement of suit.

Any of the defendants, where there are more than one defendants resides, or carries on business, or personally works for gain at the time of the commencement of suit provided that in such cases either the leave of the court is given, or the defendants who do not reside, or carry on business, or personally works for gain, as aforesaid, acquiesce in such institution or, the cause of action wholly or partially arises.

**However, this section doesn't seem to be fit in virtual world.** The issue with the cyber space jurisdiction is the presence of multiple parties across various part of the globe who only have virtual connections among them therefore we cannot have a clear idea about the parties and the place of suing so that the jurisdiction of the court could be determined to try such cases.

In all civil matters, **the Code of Civil Procedure (CPC), 1908**, basically formulates the Indian approach to jurisdiction. Under CPC, one or more courts may have jurisdiction to deal with a subject matter having regard to the location of immovable property, place of residence or work of a defendant or place where cause of action has arisen. Where only one court has a jurisdiction, it is said to have exclusive jurisdiction; where more courts than one have jurisdiction over a subject matter, they are called courts of available or natural jurisdiction. The jurisdiction of the courts to try all suits of civil nature is very expansive as is evident from the provisions of CPC.

#### **Basis of Jurisdiction – i. Pecuniary ii. Subject-matter iii. Territory and iv. Cause of action**

In **Casio India Co. Ltd. v. Ashita Tele Systems Pvt. Ltd.**, the plaintiff was aggrieved by the registration of the domain name [www.casioindia.com](http://www.casioindia.com) by the defendant with its registered office in Mumbai. It filed a suit for trademark infringement in the Delhi High Court under the relevant provisions of **the trademarks Act, 1999** along with an interim injunction application under Order 39 Rule 1 & 2 CPC, 1908. On the issue of territorial jurisdiction, the defendant contended that it carried on business in Mumbai only and no cause of action arose in Delhi. The plaintiff, however, averred that the website could be accessed from Delhi also. After referring to Gutnick, Justice Sarin observed that “once access to the impugned domain name website could be had from anywhere else, the jurisdiction in such matters cannot be confined to the territorial limits of the residence of the defendants.” Hence, it was held that ‘the fact that the website of the defendant can be accessed from Delhi is sufficient to invoke the territorial jurisdiction of this court.’

In **Satya v. Teja Singh**, the Supreme Court held that “every case which comes before an Indian court must be decided in accordance with Indian law. It is another matter that the Indian conflict of laws may require that the law of a foreign country ought to be applied in a given situation for deciding a case, which contains a foreign element. Such recognition is accorded not as an act of courtesy, but on considerations of justice. It is implicit in that process that a foreign law must not offend our public policy.”

#### **Jurisdiction based on the Criminal Procedure Code, 1973**

The Criminal Procedure Code and Information Technology Act 2000 resolve the jurisdictional issue in case of Cyber Crimes in India. **Section 1(2)** of the IT Act refers to the concept of extraterritorial application of the Act by stating that it is extended to whole of India and applies to any offence or contravention committed outside India by any person. The interpretation of the above provision suggests that the nationality of the offender is not an issue for the application of IT Act.

**Section 75** further clarifies that the jurisdiction extends to any offence or contravention committed outside India by any person irrespective of his nationality provided the act or conduct constitute offence or contravention involving a computer, computer system or computer network located in India. Therefore, the effect principle of jurisdiction has been accepted for the jurisdiction of court.

Further, the Criminal Procedure Code under **Section 177 to 189** deals with the jurisdiction of Court. **Section 177** lays down that the offence will be tried down by the Court within whose local jurisdiction the offence was committed. If the offence is a continuing one or committed in parts in different territory, as per **Section 178** the Court having the jurisdiction over any of such local area can entertain the trial. **Section 179** lays down the principle that the jurisdiction of Court where offence is committed or consequence is ensued. Following it **Section 182** requires that any offence of cheating by means of telecommunication be tried into any court whose local jurisdiction such message were sent or received. In case of the offender commits the crime beyond local jurisdiction but resides within the local jurisdiction, then within the jurisdiction of local court where he resides may inquire into the offence as if it is committed in the local area. Section 188 incorporate the nationality principle of jurisdiction as it provides that if a citizen of India outside the country commits the offence, the same is subject to the jurisdiction of court in India. However the court can apply the jurisdiction in the above case only if the offender is brought within the territory of the State. Above

- The Cr.P.C. lays down that the ordinary place of trial and inquiry is the court in whose jurisdiction the crime has been committed. However, the subsequent provisions of the Cr.P.C. dilute the strict necessity of territorial jurisdiction.
- The place of commission of an offence is uncertain, the offence is continuing or it has been committed partly in one and partly in another or it is several acts in several places, a court having jurisdiction in any place may try the case.
- An offence can be tried where the consequence ensues. These provisions are very relevant with regard to computer offences, in which the place of commission is very difficult to locate.
- In case of offence by letters or telecom messages, jurisdiction lay with the court where the message was sent or received. Thus, this provision shall be resorted to in case of offences involving an e-mail.
- Further the Cr.P.C. provides that no sentence or order of a criminal court can be set aside for wrong

**Section 179** deals with the consequences of crime in Indian territory.

**Section 188 of CrPC 1973** provides that even if a citizen of India outside the country commits the offence, the same is subject to the jurisdiction of courts in India.

#### **Jurisdiction under IPC, 1860**

**Sec. 3. Punishment of offences committed beyond, but which by law may be tried within, India.**—Any person liable, by any [Indian law] to be tried for an offence committed beyond [India] shall be dealt with according to the provisions of this Code for any act committed beyond [India] in the same manner as if such act had been committed within [India].

**Sec. 4 Extension of Code to extra-territorial offences.** —The provisions of this Code apply also to any offence committed by:

- (1) any citizen of India in any place without and beyond India;
- (2) any person on any ship or aircraft registered in India wherever it may be;]
- 3) any person in any place without and beyond India committing offence targeting a computer resource located in India .

Discussion reflects that the jurisdiction issues are comprehensively dealt by the Information Technology Act and Criminal Procedure Code. The jurisdiction of the court in case of cyber crime committed by out state offender having impact within the territory of local court is not useful till the time offender is not within the jurisdiction of any local court. In such cases the extradition is the option to bring the offender within the territory of India. Though presently there is no Universal Convention on Extradition and therefore, in the absence of it, extradition is facilitated between States by bilateral agreement.

#### **Relevant cases laws:**

##### **SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra**

This is a case related to cyber defamation. This is first case of its kind from India. In this case, the defendant was an employee of the plaintiff's company who used to send derogatory, obscene, vulgar, and abusive emails to his employers and also to different subsidiaries of the said company all over the world. The motive behind sending those emails was to malign the reputation of the company and its Managing Director all over the world.

The High Court of Delhi assumed jurisdiction over a matter of defamation of reputation of corporate through e-mails. An ex-parte injunction was granted by the court.

##### **SIL Import v. Exim Aides Silk Importers**

In this case the court successfully highlighted the need of interpretation of the statute by judiciary in the light of technological advancement that has occurred so far . Until there is specific legislation in regard to the jurisdiction of the Indian Courts with respect to Internet disputes, or unless India is a signatory to an International Treaty under which the jurisdiction of the national courts and circumstances under which they can be exercised are spelt out, the Indian courts will have to give a wide interpretation to the existing statutes, for exercising Internet disputes.

##### **Impresario Entertainment & Hospitality Pvt. Ltd. vs S&D Hospitality**

Facts – in this case the plaintiff's company offers restaurant services which has its registered office in Mumbai and is carrying its business in New Delhi and a restaurant under the name and style of 'SOCIAL' which it has trademark and has various branches as well. The plaintiff came to know about the defendant's restaurant in Hyderabad under the name 'SOCIAL MONKEY.

Also, it has a popular beverage by the name A GAME OF SLING and the defendant has named a beverage as Hyderabad Sling which is identical or deceptively similar to the plaintiff's beverage. Both these outlets had entered into contract with websites like Zomato

and Dine Out and so the information of both, along with menu and contact info was made available on the websites of Zomato and Dine Out.

Therefore, issue before the Delhi High Court was whether it had the jurisdiction to adjudicate upon the matter?

The Hon'ble Court also observed that for the purposes of a passing off or an infringement action (where the plaintiff is not located within the jurisdiction of the court), the injury on the plaintiff's business, goodwill or reputation within the forum state as a result of the Defendant's website being accessed in the forum state would must be shown. Therefore, the court held that mere interactivity of the website in the forum State did not attract its jurisdiction.

Earlier similar view was given in the case of **Banyan Tree Holding (P) Limited v. A. Murali Reddy and Anr** wherein the court held that a passive website, with no intention to specifically target audiences outside the State where the host of the website is located, cannot vest the forum court with jurisdiction.

#### **IV. International Position Of Internet Jurisdiction Cases in Cyber Jurisdiction**

The internet today is making a complete mockery of the law....not just the traditional laws but even the so-called modern laws. The very basis of any justice delivery system, the jurisdiction, which gives powers to a particular court to accommodate a particular case, is itself being threatened over the internet; leave alone the other traditional laws.

##### **Stand of The United States of America**

It is important to understand the traditional principles of jurisdiction, like personal jurisdiction, local state's long-arm statute and the due process clause of the US Constitution to know how these principles have been used by various courts to resolve e-commerce related disputes. Computer crimes because of their transitional nature involve certain difficult jurisdictional questions. Suppose a hacker operating from a computer in country A, enters a database in country B, and after routing the information through several countries causes a consequence in C.

The USA recognises two different forms of personal jurisdiction known as "**General Jurisdiction**" and "**Specific Jurisdiction**". The Courts under the General jurisdiction adjudicate any claim against defendant related to claims linked with the forum State.

Traditionally speaking, the US Constitution requires minimum contacts between a potential defendant and the forum State. The two constitutional tests regarding asserting jurisdiction over a foreign defendant were laid down in **International Shoe Co. V. Washington**.

In tort matters, the *lex loci delicti*, the rule that the place in which injury occurred is place of suing; was followed, But now the ever-expanding boundaries of the Internet have, both in civil and criminal matters, exposed the defendant to universal jurisdiction.

In the minimum contacts rule if the action is against a person in personam, then the minimum contact must apply to the defendant and if the action is against a thing in rem, then the minimum contacts must apply to that thing. In rem, jurisdiction might apply to the assertion of claims for jurisdiction based on e-mail storage box or stored file that is located on a computer server in the forum jurisdiction. The minimum contacts jurisdiction has been based on domicile and consent. However, domicile is not affected by the internet and the transactions that pass through the internet. In internet transactions the minimum contact test is met by establishing the Internet related actions which are but certain electronic transmission to decide whether there are sufficient minimum contacts before a particular court to assert jurisdiction.

Thus in the US, the courts have taken electronic transmission into or other electronic connections with the forum jurisdiction as the basis of jurisdiction

But some courts have found that using an electronic network does not subject the user to jurisdiction everywhere. The crucial issue of applicability of personal jurisdiction to Internet activities is being debated in legal circles of the US where the judiciary opined that mere availability of a website is not enough to establish minimum contact so as to exercise jurisdiction over it. Other contacts in the forum State must also be established before justified jurisdiction is exercised, held in **Hoarst Corpn. V. Goldberger 1997 US Dist LEXIS 2065(SDNY)**

The sliding- scale approach is comprehensively and formucally stated in **Zippo Manufacturing Co.v. Zippo.Com Inc 952 F supp 1119(WD Pa 1997)**

Apart from **sliding scale theory**, determination of jurisdiction also takes place with the aid of **effects test** also known as **Calder Effect Test**, propounded by the US Supreme Court in *Calder v Jones*, in which it was held that jurisdiction can be premised on the intentional conduct of the defendant outside the forum state that is calculated to cause injury to the plaintiff within the forum State. This test was applied for online activity was enough to establish jurisdiction as the defendant knew that his act will cause injury to the plaintiff in the forum State where the plaintiff corporation had its principle place of business and thus, fulfilled the requirement of " purposeful availment".

The test was more elaborately applied in **Yahoo! Inc.v. La Ligue Contre Le Racisme**, in which the court held that jurisdiction could be exercised in California over French civil rights groups under french hate laws.

Out of two approaches, the sliding-scale theory is mainly helpful in resolving the disputes which are mainly in the area of commercial activities, copyright or trademark infringements, or in intellectual property cases. The effects test is mainly useful in criminal matters.

here at least three jurisdictions are involved and who shall try him? The dilemma was described very appropriately by **La Forest, J.**, in **Libman v. The Queen**, in following words: "one is to assume that the jurisdiction lies in the country where the crime is planned or initiated. Other possibilities include the impact of the offence is felt, where it is initiated, where it is completed or again where the gravamen or the essential element of the offence

took place. It is also possible to maintain that any country where any substantial or any part of the chain of events constituting an offence takes place may take jurisdiction.

In **Burger King Corp. v.**, it was held that the exercise of personal jurisdiction over an out-of-state defendant must comport with constitutional due process. In *Doe v. Unocal Corp.*, it was held that when an exercise of personal jurisdiction is challenged, the burden is on the plaintiff to demonstrate why the exercise of jurisdiction is proper.

In **Ballard v. Savage**, it was held that the plaintiff can satisfy this burden of proof by showing the following 3 things: (a) the defendant purposefully availed itself of the privilege of conducting activities in the forum state by invoking the benefits and protections of the forum state's laws;

### **Jurisdiction on the Basis of Online Contract**

Online contracts come with 'terms of service' agreements and disclaimers. These agreements impose restrictions on the users regarding the choice of law and forum selection.

In **Bremen v. Zapata Off-Shore Co.**, the judicial view arrived was that "such clauses (forum selection) are prima facie valid and should be enforced unless enforcement is shown by the resisting party to be 'unreasonable' under the circumstances." This rule applies, under the federal law, both if the clause was a result of negotiation between two business entities, and if it is contained in a form of contract that a business presents to an individual on a take-it-or-leave-it basis.

### **Forum Selection Clauses: Click-trap Contracts**

It makes a good legal sense for the online service providers to limit their exposure to one jurisdiction only. Defending lawsuits at multiple locations could be both expensive and frustrating. Thus, the online service provider has no other choice but to subject themselves to only one set of forum and applicable laws only. The user has no other choice, but to accept the service provider's 'terms of service' conditions by clicking an on-screen button that says "I Agree", "I Accept" or "Yes".

In **Steven J Caspi et al v. The Microsoft Network, L.L.C., et al.**, the user could not use Microsoft Network unless she clicked the "I agree" button next to a scrollable window containing the terms of use. Each plaintiff clicked the "I agree" button to use Microsoft Network, indicating their assent to be bound by the terms of the subscriber agreement and thus forming a valid licence agreement. The Superior Court of New Jersey held that the forum selection clause contained in Microsoft Network subscriber agreements was enforceable and valid.

### **Jurisdiction Based on Location of a Web Server**

Asserting personal jurisdiction based on the defendant's use of IT infrastructure of a service provider, located in the forum state, to host its website may also compel the forum state to exercise its jurisdiction over such defendant.

In **Jewish Defence Organization, Inc. v. Superior Court**, the plaintiff brought an action for defamation in a California court. Defendant's only relevant contacts with California consisted of contracting with Internet service providers, "located in California," to host a website which they maintained from their residence in New York. The court concluded that the defendant's conduct of contracting, via computer, with Internet service providers, which may be California corporations or which may maintain offices or databases in California, is insufficient to constitute 'purposeful availment. But in **3DO Co. v. Poptop Software Inc.**, the court found it relevant that "defendants use a San Francisco-based company as a server to operate a website that distributes allegedly infringing copies of software."

### **European Approach to Personal Jurisdiction**

The European approach to personal jurisdiction in cross-border dispute is rather different from the American approach. The rules determining which country's courts have jurisdiction over a defendant are set out in a regulation issued by the Council of the European Union, known as the 'Brussels Regulation'. This new regulation is an update of a 1968 treaty among European countries, known as the Brussels Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial matters.

**Brussels Regulation** - The Brussels Regulation, which became effective on March 1, 2002, (The Regulation on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial matters and online commercial disputes) replaces Brussels Convention of 1968. It is applicable to all European Council countries except Denmark, which will continue to follow the rules of the Brussels Convention and the EFTA countries (Iceland, Liechtenstein, Norway, Switzerland and Poland), where rules of the 1988 Lugano Convention will be applicable.

### **Applicability of Brussels Regulation in Online Environment**

On the issue of jurisdiction the Brussels Regulation sets the rule: "subject to the provisions of this Regulation, persons domiciled in a Contracting State shall, whatever their nationality, be sued in the courts of that State". Further, a person domiciled in a Contracting State may, in another Contracting State, be sued 'in matters relating to contract, in the courts for the place of performance of the obligation in question'. Further, the domicile of a company or other association (including a partnership) is where it has its statutory seat (i.e., its registered office), its central administration or its principal place of business.

From the point of promotions and sale, the Regulation says that the consumer may sue at home if the trader pursues commercial activities in the Member State of the consumer's domicile or, by any means, directs such activities to that Member State.

### **India and international convention over cyber jurisdiction:**

**Convention on Cyber crime, 2001** also known as the Budapest Convention, is the first international treaty which discusses about the Internet and cybercrime by considering national laws, increasing cooperation among nations and improving investigative techniques

The Convention on Cyber crime was opened at Budapest on 23rd November, 2001 for signatures. It was signed by the Council of Europe in Strasbourg, France, Canada, Japan, Philippines, South Africa and the United States. However, countries like India and Brazil have declined to adopt the Convention on the grounds that they didn't participate in its drafting but due to increasing incident of cyber crimes India has been reconsidering its stand on the convention since 2018.

It was the first ever-international treaty on criminal offences committed against or with the help of computer networks such as the Internet. The Convention deals in particular with offences related to infringement of copyright, computer-related fraud, child pornography and offences connected with security. It also covers a series of procedural powers such as searches of and interception of material on computer networks. Its main aim is to pursue "a common criminal policy aimed at the protection of society against cyber crime, inter alia by adopting appropriate legislation and fostering international co-operation."

**Article 22 The Convention on Cyber Crime, 2001** allows the country to have jurisdiction if the cyber crime is committed:

In its territory;

On board a ship flying the flag of the country;

On board an aircraft registered under the laws of the country

By one of the countries nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State

India is still not a signatory to the Cyber Crime Convention and the bilateral extradition treaties, which it has signed with around 50 countries so far, do not mention 'cyber crime' as extraditable offences. But it may not deter the Indian government from granting extradition, as it was held in **Rambabu Saxena v. State**, that "if the treaty does not enlist a particular offence for which extradition was sought, but authorizes the Indian government to grant extradition for some additional offences by inserting a general clause to this effect, extradition may still be granted."

#### **United Nations Convention against Transnational Organized Crime (UNTOC):**

This treaty was adopted by resolution of the UN General Assembly in November 2000. India being a signatory to this joined in 2002. UNTOC is also known as the Palermo Convention, under this the state parties are obliged to enact domestic criminal offences that target organised criminal groups and to adopt new frameworks for extradition, mutual legal assistance, and law enforcement cooperation. Although the treaty does not explicitly address cyber-crime, its provisions are highly relevant. In pursuant to this treaty Indian Parliament enacted the Information Technology Act 2000.

#### **Rome Convention**

To resolve cross-border consumer contractual disputes, the EU Member States became signatories to the Rome Convention, 1980. It decides which country law would apply in

contractual disputes. The Convention gave freedom of choice to the contracting parties, as it states that “a contract shall be governed by the law chosen by the parties. The choice must be express or demonstrated with reasonably certainty.” It further states that “the mandatory rules of the consumer’s country of habitual residence will always apply whatever choice of law is made.”

**Conclusion:**

The issue of jurisdiction of State as well as court becomes important as the first step in the process of regulation of cyberspace. Right from legislative jurisdiction of State to adjudicative jurisdiction of Court the traditional notion of jurisdiction has been challenged by cyberspace. It is very difficult to decide the location of offender or defendant whereas it is equally easy for to commit crime and contraventions. In particular the cross border nature of offence creates a big challenge for regulation. As cyber space is a world with limitless boundary, hence the need of the hour is to develop a unique law which can be applied to deal with the case of cyber crime without any difficulty or confusion.