# UNIT 10 ISSUES OF JURISDICTION AND APPLICABLE LAW IN CYBERSPACE

**Structure**



## 10.1 INTRODUCTION

In the previous block we have discussed the various types of cyber wrongs. In the first unit of this block we shall discuss the jurisdictional issues involved in adjudging these wrongs i.e. which court or courts can take cognizance of these offences.

This unit deals with jurisdiction and applicable law with respect to computer crimes and offenders. The issue of jurisdiction of courts in crimes is perplexing in the cyberspace world and computer crimes era. It is easier to sit in New Zealand and hack a computer in Chandigarh and steal digital information than it would be for a thief to physically steal something from the neighbourhood. The digital world makes national and international borders a relic. Courts exercising jurisdiction on the basis of such national and international borders are left aghast by the speed and ease with which a cyber-criminal moves from one jurisdiction to another with the use of a mouse. The issue arising out of such activities, at the foremost, contains that of the jurisdiction of a court. *Which* court shall have the jurisdiction to entertain the matter? And then, *which* law shall be applicable in such cases?

In an online environment, the offender and the victim might reside in different geographical locations governed by different procedural and substantive laws – probably, in different countries. For instance, a person might open an online gambling website while in Las Vegas. The website is open for all to see and use. It might be legal in Las Vegas. But, when people access and make use of this website in, say, Qatar, Australia and Indonesia, the question as to permissibility of offering to gamble might crop up.

## 10.2 OBJECTIVES

After studying this unit you should be able to:

- explain the term jurisdiction and discuss the importance of it in cyberspace;
- discuss various theories relating the criminal jurisdiction quoting relevant provisions of Indian laws and court decisions; and
- analyse the importance of the effect doctrine in the light of the extra territorial nature of the cyber crimes; and
- examine the issue of applicable law with special reference to India by citing relevant sections of the IT Act 2000.

## 10.3 JURISDICTION IN CYBERSPACE

'Jurisdiction', as applied to a particular claim or controversy, is the power to hear and determine that controversy. The term imports authority to expound or apply the laws, and excludes the idea of power to make the laws. It refers to the right to adjudicate on a given point; the local extent within which the court can and does exercise the right when ascertained. The law relating to crimes would generally require that the courts within a state would have jurisdiction to try and adjudicate upon all such offences committed by a person within the territorial boundaries of such a court. However, the exceptions have been created where even though, technically and strictly, the offender might not have committed the crime on the soil of the country, yet the courts would exercise jurisdiction over such an offender.

To fully appreciate and comprehend this issue, we first need to understand the jurisdiction issues arising in an offline environment in India in criminal cases and the body of law applicable to ascertain jurisdiction. Then we proceed to apply the same rules in a cyberspace environment and assess the difficulties.

### 10.3.1 Theories of Jurisdiction in Criminal Cases

We have to bear in mind that a State, while framing laws, exercises its legislative power to (a) regulate; (b) adjudicate upon; and, (c) enforce measures, against criminal actions. Law of regulation of criminal actions encompasses declaring certain acts or omissions to be a crime and provides for punishment thereof. Law of adjudication provides for establishment of courts and defining their jurisdiction. Enforcement measures ensure that the orders of the court are carried out and persons found guilty are appropriately punished.

There are six generally accepted bases of jurisdiction or theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity.[1]

**Subjective territoriality** is by far the most important of the six. The substantial part of criminal legislation across the globe is based on the theory that if an activity takes place within the territory of the particular country, then the said country has the jurisdiction to regulate and punish for such activity. For instance, section 2 of the Indian Penal Code provides for punishment of offences committed within India.

**Objective territoriality** is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. Commonly known as the '*effects*' doctrine is the situation , where the action takes place outside the territory of a country, but the primary effect of that activity is within the said country, it assumed jurisdiction. For instance, a person from Pakistan shoots across the border and an Indian is injured in the process. Though the action was initiated in Pakistan, the effect was in India. Section 179 of the Code of Criminal Procedure endorses the effects doctrine.

**Nationality** is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. For instance, section 4 of the Indian Penal Code stipulates that the provisions of the Code would also apply to any offence committed by any citizen of India in any place without and beyond India.

**Passive nationality** is a theory of jurisdiction based on the nationality of the *victim*. Passive and "active" nationality are often invoked together to establish jurisdiction because a state has more interest in prosecuting an offense when both the offender *and* the victim are nationals of that state.

The **Protective principle** expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the "victim" would be the government or sovereign itself. This principle is not preferred for the obvious reason that it can easily offend the sovereignty of another nation.

Lastly, nations also exercise a **Universal jurisdiction** with respect to certain offences. Sea piracy has been, for long, a part of this jurisdiction. Any nation could have captured and punished pirates. This form of jurisdiction has been expanded lately to include slavery, genocide, and hijacking (air piracy). For instance, Article 105 of the United Nations Convention on the Law of the Sea stipulates that on the high seas, or in any other place outside the jurisdiction of any State, every State may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board. It further provides that the courts of the state which carried out the seizure may decide upon the penalties to be imposed, and may also determine the action to be taken with regard to the ships, aircraft or property, subject to the rights of third parties acting in good faith.

With the advent of Internet and increase in cyber crime, especially, cross-border illegal activities, it is a matter of much concern to the courts whether they have the jurisdiction to put the offenders under trial and if found guilty, eventually punish them.

### 10.3.2 General Jurisdiction in Computer Crimes

The law of jurisdiction with respect to crimes relating to computers is the same as that relating to traditional crimes. The theory of subjective territoriality would apply. In India, Chapter XII of the Code of Criminal Procedure, 1973 relates to jurisdiction of courts with regard to criminal matters. The foremost and most commonly applied theory of territoriality is embodied in section 177 of the Code in the following words:

*177. Ordinary place of inquiry and trial.-* Every offence shall ordinarily be inquired into and tried by a Court within whose local jurisdiction it was committed.

Thus, any computer crime committed, say, in Indore, would be tried by the criminal courts in Indore itself. However, computer crime, by its very nature, is capable of being committed at more than one place at the same time. For instance, a person sitting in Mumbai can hack into a computer at the IISc at Bangalore through a proxy server located at Kanpur. In such situations, the offence can be inquired into and tried by a court having jurisdiction over any of such areas where the crime has been committed. Section 178 of the Code provides for this kind of a situation:

*178. Place of inquiry or trial.-* a) When it is uncertain in which of several local areas an offence was committed, or

b) Where an offence is committed partly in one local area and partly in another, or

c) Where an offence is a continuing one, and continues to be committed in more local areas than one, or

d) Where it consists of several acts done in different local areas, it may be inquired into or tried by a Court having jurisdiction over any of such local areas.

Thus, based upon the subjective territoriality theory and the above provisions of our criminal procedural law, the requirement that our courts should have jurisdiction to book persons found guilty of committing crimes relating to computers within the territory of India is well taken care of. However, issues arise when someone is sitting across the border and initiates a digital action which has a direct adverse consequence within the territory of a state. The 'effects' doctrine (objective territoriality theory) assumes significance when offenders involved in cross-border crimes are required to be put on trial.

### 10.3.3 Application of 'Effects' Doctrine in Computer Crimes

Also known as the 'consequence' or 'terminatory'[2] theory, the principle is that where an act is done abroad and the criminal effect is produced here, the crime is taken to be committed here. Both English and American courts have exercised this kind of extra-territorial jurisdiction. For instance, in *Simpson* v. *State*, [92 Ga.41.17S.E.984(1893)],the victim was in a small boat near the Georgia side of the wide Savannath River. Simpson, the defendant, stood on the opposite South Carolina Bank and fired several shoots at the vessel. The bullets missed the boat but struck the water nearby. The Supreme Court of Georgia held that jurisdiction attached with these circumstances and that Simpson could properly be prosecuted in Georgia even though the defendant was clearly in another state at the time of shooting. The location of the victim and the place where the bullets landed established the basis for the decision. In *R.* v. *Oliphant*, [(1905) 2K.B.67] in which a man in Paris by false returns caused incorrect figures to be entered in the account books of his firm in London, it was held that the office of false accounting was committed by him in London.

If the principle of jurisdiction by 'effects' theory can be accepted in relation to crimes like cross-border killing or conspiracy or false representation, then, with the Internet giving a much wider and global scope of committing crimes (the consequences of which can be almost anywhere in the world), providing for a global jurisdiction to tackle with the crime can well be justified.

Under the Indian criminal law, section 179 of the Code of Criminal Procedure, 1973 embodies the effects doctrine, which reads as under:

"*179. Offence triable, where act is done or consequence ensues*: When an act is an offence by reason of anything which has been done and of a consequence which has ensued, the offence may be inquired into or tried by a court within whose local jurisdiction such thing has been done or such consequence has ensued."

The Supreme Court in *State of Madhya Pradesh* v. *Suresh Kaushal*, [(2001) 4 SCAPE 233], has held that:

"The above section contemplates two Courts having jurisdiction and the trial is permitted to take place in any one of those two Courts. One is the Court within whose local jurisdiction the act has been done and the other is the Court within whose local jurisdiction the consequence has ensued."

For instance, it is well settled that where a sub-standard article is sold and an offence is committed, the place where the same is marketed will equally have jurisdiction to try an offence against the manufacturers as well as the distributors [State of Punjab v Nohar Chand, (1984) 3 SCC 512; State of Rajasthan v Rajesh Medical Agencies. 1987 SCC Supp 242].

Section 179 contemplates cases where the act *done* and its *consequence* happen to be in two different jurisdictions and provides that in such cases, the offence constituted by the act and the consequence may be inquired into or tried in either of the two jurisdictions. In an Indian case of this nature, 'A' at Karachi was making representations to the complainant at Bombay, through letters, telegrams and telephone talks, sometimes directly to 'B' and sometimes through a commission agent. 'B' parted with money in good faith of these representations, which were false. The Supreme Court held that the representations were made to 'B' at Bombay notwithstanding that 'A' was making the representations from Karachi. Hence the entire offence took place at Bombay and not merely one ingredient of it, (which was *consequence* of the false representations), namely, the parting with the money by 'B'. The Apex Court held that the offence would be triable both at the place from where the false representations were made as well as where the parting of property took place [Mobarak Ali Ahmed v State of Bombay. AIR 1957 SC 857].

Section 179 giving statutory recognition to the 'effects' doctrine is squarely applicable in computer crime cases. There would be many situations where we would find that though the initiator of an illegal action is somewhere outside the territory of India, the effect of his digital wrong-doing has caused damage to persons within India. Such persons, by operation of section 179, are liable to be tried in India. The Indian courts would have jurisdiction to try such cyber criminals.

The concept of 'effects' doctrine has been recognised not just by India but by other countries[3] as well. Its application in computer crimes has to be adopted as of necessity due to the peculiarity of the Internet, which permits initiation of the crime from any part of the world with its consequences or terminating effect in any other part of the world without any barriers.

### 10.3.4 Convention on Cyber Crime – Council of Europe

The Cyber Crime Convention of the Council of Europe prescribes for the issue of jurisdiction in Article 22. It requires that every member-nation should adopt legislative measures to establish jurisdiction over any offence established under the Convention, when the offence is committed in its territory. The nations have further option to establishing jurisdiction in case the offence has been committed on board a ship flying the flag of that Party; or on board an aircraft registered under the laws of that Party; or, by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any state. It should be noted that the above Convention applies the theory of subjective territoriality and Nationality theory but avoids the 'effects' doctrine.

Please answer the following Self Assessment Question.

**Self Assessment Question 1** *Spend 3 Min.*

What do you understand by the term 'jurisdiction'?

.....

.....

.....

.....

.....

.....

## 10.4 APPLICABLE LAW IN COMPUTER CRIMES

Once a court has assumed jurisdiction, the next question is: what body of substantive law should be used to resolve the problem? It is the substantive criminal law of a country which declares whether a particular activity is a crime or not. Every country has its own set of criminal laws. What is a crime in one country might be an innocent act in another. Online activities create a vast scope for confusion. It might even act as a haven. An offender can skillfully carve out a niche for himself in the cyber world where he/she is not answerable for his/her criminal activities because of his/her physical presence in a country whose cyber criminal laws are not matured enough to pin him/her down.

In India, the Information Technology Act delves deep into the issue of applicable law in computer crimes. It clarifies that any act which is committed either within or without India would be illegal if it is an offence under the Act.

To begin with, sub-section (2) of Section 1 of the Act states that:

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

Further, section 75 of the Act reads as under:

**75. Act to apply for offence or contravention committed outside India.**

1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

2) For the purposes 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 involved a computer[4], computer system[5] or computer network[6] located in India.

The above two provisions make it clear that the offence, though committed outside India, is punishable in India. Thus, a Nepalese, sitting in Canada initiates a Distributed Denial of Service involving computer networks in India to obstruct Yahoo e-mail services, such a person, if put to trial in India, can be found punishable under the IT Act. The above provisions have been drafted in broad terms.

Certain provisions of Indian Penal Code also suggest applicability of its provisions to illegal actions committed outside India, though subject to certain conditions.

Section 2 of the Indian Penal Code deals with punishment of offence committed within India. This poses no problem. If an illegal act concerning computers is committed within India, it is the provisions of the Code which would apply to such acts.

Section 3 of the Indian Penal Code reads as under:

*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.

This section will apply in a situation where the accused, at the time of committing the offence that he/she is charged with, is amenable to Indian courts. Section 3 of the IPC has a broad ambit and it extends to any person not necessarily a citizen of India but governed by Indian law for acts committed beyond India.

Section 4 of the Indian Penal Code, on the other hand, applies the Nationality doctrine. It deals with acts and omissions of Indian citizens abroad. It further regulates the action of any person irrespective of his/her nationality, if such person happens to be on a ship or aircraft registered in India. The section reads as under:

*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.

Explanation – In this section the word "offence" includes every act committed outside India, which if committed in India would be punishable under this Code.

Thus, the provisions of the Code would apply if an Indian citizen anywhere outside India commits any computer crime punishable under the Indian Penal Code, like digital forgery or cyberstalking.

It is worth noting that the 'applicability' provisions of the Information Technology Act and the Indian Penal Code are slightly on different notes. The IT Act is broader and covers all such persons whose action or omission might be an offence under the Act. This is irrespective of their nationality or their geographical presence. On the other hand, sections 2 and 3 of the Indian Penal Code are not as vast in their applicability. Section 3 restricts itself to only such persons who are liable to be tried within India by virtue of any Indian law. Section 4 of the Code applies only to citizens of India and any person who commits an offence while on any ship or aircraft registered in India.

So far as computer crimes are concerned, the Indian law seems to be in shape. However, issues like extradition of computer criminals and international co-operation also need to be addressed with equal vigour for quicker booking of the guilty.

You may now like to attempt a Self Assessment Question.

**Self Assessment Question 2** *Spend 3 Min.*

Discuss the provisions of Indian laws which deal with the issue of the applicability of law.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

## 10.5 SUMMARY

The Indian Penal Code, the Code of Criminal Procedure and the Information Technology Act cover issues pertaining to jurisdiction of computer crimes and also the law applicable in such cases. Section 179 of the Code of Criminal Procedure gives jurisdiction to the courts in India to deal with any computer crime which leaves its impact or effect within the territorial boundaries of India. The IT Act and the Indian Penal Code are the laws applicable for such crimes and the Courts have to employ them to ascertain whether a particular action or omission is a crime and if the accused is found guilty, to award punishment as provided under the said laws.

## 10.6 TERMINAL QUESTIONS

1) What do you understand by the term jurisdiction? Discuss its significance of it vis-à-vis the cyberspace.

2) Discuss the importance of effects doctrine in cyber crime.

3) Examine the issue of applicable law in cyber crime. How is the issue dealt with by the Indian IT Act?

## 10.7 ANSWERS AND HINTS

1) The issue of jurisdiction of courts in crimes is perplexing in the cyber world and computer crimes era. The digital world makes national and international borders a relic and exercising jurisdiction on the basis of such national and international 'Jurisdiction', as applied to a particular claim or controversy, is the power to hear and determine that controversy. The term imports authority to expound or apply the laws, and excludes the idea of power to make the laws. It refers to the right to adjudicate on a given point; the local extent within which the Court can and does exercise the right when ascertained. The law relating to crimes would generally require that the courts within a state would have jurisdiction to try and adjudicate upon all such offences committed by a person within the territorial boundaries of such court. However, the exceptions have been created where even though the technically and strictly, the offender might not have committed the crime on the soil of the country, yet the courts would exercise jurisdiction over such an offender.

2) The principle is that when an act is done abroad and the criminal effect is produced here, the crime is taken to be committed here. Section 179 of the Code of Criminal Procedure, 1973 embodies the effects doctrine. The Supreme Court in *State of Madhya Pradesh* v. *Suresh Kaushal*, has held that:

   "The above section contemplates two Courts having jurisdiction and the trial is permitted to take place in any one of those two Courts. One is the Court within whose local jurisdiction the act has been done and the other is the Court within whose local jurisdiction the consequence has ensued."

Once a court has assumed jurisdiction, the next question is: what body of substantive law should be used to resolve the problem? It is the substantive criminal law of a country which declares whether a particular activity is a crime or not. Every country has its own set of criminal laws. What is a crime in one country might be an innocent act in another. Online activities create a vast scope for confusion. It might even act as a haven. An offender can skillfully carve out a niche for himself in the cyber world where he is not answerable for his criminal activities because of his physical presence in a country whose cyber criminal laws are not matured enough to pin him down.

In India, the Information Technology Act delves deep into the issue of applicable law in computer crimes. It clarifies that any act which is committed either within or without India would be illegal if it is an offence under the Act.

In India, the Information Technology Act delves deep into the issue of applicable law in computer crimes. It clarifies that any act which is committed either within or without India would be illegal if it is an offence under the Act.

To begin with, sub-section (2) of Section 1 of the Act states that:

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

Further, section 75 of the Act reads as under:

**75. Act to apply for offence or contravention committed outside India.-** (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes 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 involved a computer , computer system or computer network located in India.

Section 2 of the Indian Penal Code deals with punishment of offence committed within India. This poses no problem. If an illegal act concerning computers is committed within India, it is the provisions of the Code which would apply to such acts.

Section 3 of the Indian Penal Code reads as under:

*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.

This section will apply in a situation where the accused, at the time of committing the offence that he/she is charged with, is amenable to Indian courts. Section 3 of the IPC has a broad ambit and it extends to any person not necessarily a citizen of India but governed by Indian law for acts committed beyond India.

Section 4 of the Indian Penal Code, on the other hand, applies the Nationality doctrine. It deals with acts and omissions of Indian citizens abroad. It further regulates the action of any person irrespective of his/her nationality, if such person happens to be on a ship or aircraft registered in India. The section reads as under:

*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.

## 10.8 REFERENCES AND SUGGESTED READINGS

1. Darrel Menthe. "Jurisdiction In Cyberspace: A Theory of International Spaces 4"

   Mich.Telecomm.Tech.L.Rev.69 (1998). <http://www.mttlr.org/volfour/menthe.html>.

2. For example, a wounding inflicted in Scotland is triable in England if a person standing on the Scottish Bank of the Tweed fires at and wounds a person in England. This is the 'terminatory theory' of the criminal act; the elements of the rime being spilt between two countries, it is regarded as being committed where the proscribed result takes place. Even if the attacker misses, he can be tried in England for the attempt.

3. For instance, Section 4 of the Swedish Penal Code states that a crime is deemed to have been committed where the criminal act was perpetrated and also where the crime was completed or, in the case of an attempt, where the intended crime would have been completed.

4. S.2(i) – 'computer' means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

5. S.2(j) – 'computer network' means the interconnection of one or more computers through – (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained.

6. S.2(l) – 'computer system' means a device or collection of devices, including input or output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files which contain computer programs, electronic instructions, input data and output data that performs logic, arithmetic, data storage and retrieval, communication control and other functions.