IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

CYBER JURISDICTION

D.V.L.A.S.Jyothsna, Kiran, Sailaja.

Introduction

In modern times most of human activities tend to depend more and more on technology, especially on the Information Technology. It goes without saying that human beings have edges over all form of life on the earth, as they are bestowed with the ability to think, analyze and act accordingly. Human have the capability to adopt themselves to any circumstances and the concept of 'survival of fittest' made them to strive to achieve their goals lawfully and unlawfully. Historically speaking power has never been in the hands of a single individual or group of individuals for long. The society tends to revolve around those who are the center of the power. Early man lived in caves and hunted animals for food. He slowly learnt the use of fire and tools and started harnessing the power of the Mother Nature for his benefits.

The internet, the network of computer, provided on efficient method of near instantaneous exchange of information across the globe and the world literally become global village. Information technology is assumed to be largest contributor to the shift of power in the hands of those possessing information. The information revolution has brought radical transformation in society and hurdles like distance and money are no more hindrances for accessing knowledge.

This technology has impacted the world more than any other technology, as its use is visible in almost every sphere of life and as a matter of fact it has become indispensible. It has virtually emancipated mankind from the limitation of time, space, nationality and even language. Cyberspace has emerged with in little time with the invention of computer and their interconnectivity. The cyberspace is nothing but innumerable computers connected together, sharing data and information and have become the fastest mode of communication. Cyberspace, therefore, is the places where two people meet, not physically but virtually, and communicate with each other 3 electronically.

Cyberspace is now international in scope and is growing swiftly and steadily in size, wealth and political importance. People from all walks of life, viz., scientist, technicians, journalists, doctors, lawyers, artists, clerks and civil servants are now visiting this 'space'. We are in the process of learning how to live in this newly available space. During this learning process we commit blunders and go about setting it right. The cyberspace is also afflicted to some ills and blessed with all the good things of life as in the real world. Cybercrime, unlike conventional crime is low risk high profit affairs and therefore much more dangerous. In the near future it is bound to take up a lion's share of the efforts and resources of investigating and security agencies. As the industrial revolution affected only certain parts of the world leaving behind the former colonies, the legal systems of the so called developing countries could not, as yet, equip themselves to the challenges of industrialization. Meanwhile, the cyber world has overtaken the world; demolish economic barriers and political boundaries and challenging the established laws of even the industrialized world.

Most developing countries of the world have to take a quantum jump in legislative efforts, if they want to develop capacities to protect national interest and to avoid exploitation by those who own technology-the time limits of which are still unknown. While technologies and business practices have changed dramatically, the associated legal support system did not keep pace with it. The operating canvas being large, it is not possible for a single agency to control or investigate cybercrimes. The problem is compounded by the fact that the internet does not respect national boundaries.

ABOUT CYBER JURISDICTION

Cyberspace and cyber world is a world full of electronic devices where only optical fibers, digital signals, data bytes, and such other elements may be thought of. It is virtual space where you cannot see so many activities and so many things you can see but cannot touch. It is a world away from the world we live in. It is virtual space where you cannot see so many activities; and so many things you can see but cannot touch. It has been variously defined as domain characterized by the use of electronic and electromagnetic spectrum to store, modify, and exchange data via networked systems and associated infrastructures 3 or the electronic medium of computer networks, in which online communication takes place4; or the data stored in large computer or network represented as three-dimensional model through which a virtual-reality user can move

Cyber space could thus be called a new universe and a parallel universe created and sustained by the world's computer and communication lines. From a legal perspective, the term cyberspace and the concept of quasi-physical territory are helpful in attempting to analyze the issues involved with computer communications. The geographical location where conduct occurs is one of the major factors determining which country law applies to activities

The operation of global network pay little heed to national boundaries and one of the arguments frequently mooted is that there is need for new legal perspective and regime in cyberspace. In the context of electronic commerce, comparison is sometimes made with the development of the Mercantile law developed in Middle ages, a body of law and courts developed and administered by those responsible for commercial transactions and which provided a consistent legal basis for international trade for avoiding the vagaries and discrepancies of national legal system. Laws relating to broadcasting, the media, data protection, evidence, contract, tort, defamation, intellectual property, etc. all have a role to play as do provisions of civil and criminal law. Indeed, the most inhabitants of cyberspace may be, at least in that, depending upon the nature of their activities, they may be theoretically be subject to the jurisdiction of virtually all of the world's legal system.

Jurisdiction in cyber space refers to real world government's power and normally existing court's authority over internet users and their activities in cyber world. A significant reality is that net users and the hardware they use are never virtual but have physical presence in one country or other, upon whom the jurisdiction can be exercised and such jurisdiction is called jurisdiction in cyberspace or cyber jurisdiction.

Cyber jurisdiction is still in the stage of development as a legal concept. As internet has led disappearance of boundaries, sometimes a netizen is not aware with who he is chatting with and where the person is located. In such a situation if a legal dispute arises between two persons communicating on internet then which court will have jurisdiction to decide that case is still an issue that is yet to be resolved satisfactorily in other words, there must be law that should provide whether a particular event in cyberspace is controlled by the laws of state where the website is located or by the law of state where the internet service provider is located or by any specific law/laws.

There is no law or international instrument relating to jurisdiction in cybercrime world or cyberspace which is virtual space between two modems or where internet is located. Cyber space information is broken in small bits which can be transmitted according to available capacity. These packets are labeled with address of addressee and

may follow a number of different path routed from computer to computer until reaching final destination where receiving computer resemblances them as these are originally sent. As internet uses packet system of transmission having different nodes situated in different continent so single stake cannot claim that any activity has entirely taken place within its borders so that it can have jurisdiction over it.

In the present scenario an important question is whether present law of jurisdiction of physical world is applicable to cyber world, or a separate law is required?

Physical boundaries have disappeared in cyber world therefore physical world and cyber world are not connected hence separate law of jurisdiction is required by cyber world. In cyber world there are no geographical boundaries but still in physical world these boundaries are existing. Further, because of various reasons (especially wide gap between developed and developing countries) it is not possible to develop separate law of jurisdiction for cyber world.

In cyber world there are no geographical boundaries but netizens are citizens of some countries and they are governed by the national laws of these countries. Therefore, physical world and cyber world are connected and hence present law of jurisdiction of physical world with minor modification can be applied to cyber world. The present law of jurisdiction of physical world, with minor modification is applicable to the cyber world as well. It's easy said than done. Application of theories of physical world with minor modification, to cyber world may seem feasible but in reality may create a number of problems in the exercise of jurisdiction.

Cyber jurisdiction in National cases:-

Cyber Jurisdiction in Civil cases:-

Cyber jurisdiction in civil cases mainly comes into picture when a website or any information hosted on internet leads to commitment of a civil law wrong in another state deciding whether jurisdiction exists over defendant, the U.S. Federal courts apply the law of forum states subject to the limits of due process clause.

In McDonough vs. Fallon Mc Eillgot Inc28 . Defendant from outside California created a website which was accessed by a Californian. Subsequently, dispute arose and the matter had gone to federal court. In this case, the "Federal court of California also refused to exercise personal jurisdiction over the defendant simply because it maintained a website. The court held that the fact that the defendant had a website accessed by Californians was not enough to establish jurisdiction.

Cyber Jurisdiction in Criminal Cases:-

Initially cyber jurisdiction was an issue in civil cases only. But in 1996 in U.S. vs Thomas 32 cyber jurisdiction becomes an issue in criminal cases also. In this case, defendant (a couple) started a pornographic bulletin board from their home in California in 1991 which was accessed by members having password, which could be selected, retrieved and downloaded on their own computers. In appeal, the U.S. District court, Tennessee upheld the conviction under the statute which prevents the channel of interstate commerce from being used to disseminate obscene matter.

Hacking OF Central Board of Direct Taxes Website (CBDT) (2002)

The CBDT is a statutory body in India was Hacked by allegedly Pakistani hackers. This was not new instance. The Kargil war in 1999 had seen numerous governmental website being repeatedly hacked and brought down by Pakistani hackers. While in previous cases, the government did not register cases of hacking, in case of hacking CBDT website, the police did register the case but no effective breakthrough has been achieved nor any progress made in this case. The reason behind this non-action has been that the allegedly Pakistani hacker is located outside

the territorial boundaries of India. India has no legitimate right to arrest such people outside the territorial boundaries. To complicate matter further, the neighboring country does not recognize such people as hackers and instead refer them as patriots. Therefore in this scenario, it becomes an increasingly futile to register cybercrime case; where in perpetrator of the cybercrime is physically located 123 outside the territorial boundaries of India. In this dilemma, India is not alone and shares the same boat with other nations facing challenges36 . The Yahoo! Case illustrates the possible compilations that may arise when the laws of one country against cybercrime conflict with the laws of another country. The CBDT case represents the thorny issues of: What if the damages caused by the cyber criminal reaches the territory behind border? What if committed act not crime in the country of action but considered as crime in the country that damages reaches its territory? If more than two countries want to file the charges which country could have been priority? Which countries have jurisdiction to file charges against the perpetrator of the crime? What should be the basis of claiming jurisdiction over the criminal act? Should it be the territory where the crime was committed (in case it effects more than one country the question becomes more complex) or the nationality of person committing the act or the country of residence of the perpetrator? Such questions are very difficult to answer. Sometimes due to ticklish legal situation arise in jurisdictional matter related to the internet and national laws are found wanting. Cyber jurisdictional issues need to be sorted out in the national laws as well as uniformity in laws need to be brought about in such cases and more importantly, not let the cyber criminals go unpunished due to gaping loopholes in existing laws or due to absence of laws altogether covering such matter both at national as well as international level. In the following chapters of this thesis researcher will further elaborate the problems and challenges in dealing with cybercrime and will present a critical analysis of international efforts in solving the jurisdictional issues.