# CYBER SPACE AND JURISDICTIONAL CONCERNS

**Justice Surya Kant***

It has been a blight upon mankind that most innovations originally designed for the welfare of the human race have fallen into the hands of those who indulge in iniquitous acts and use them to the detriment of other people. The Computer and the Internet, which can be safely touted as the most significant of these innovations, have also fallen prey to such abominable acts in the sphere of cyber space.

The internet is a vast expanse spanning the globe and consists of several computer networks. It is also known as an '*information superhighway*', which refers to the lack of 'limits' and the volume of traffic on the internet. Over the last few years, the use of the internet has witnessed a precipitous transition and it would not be wrong to conclude that it has become a compulsion in today's globalised era. While the internet has given us a multitude of services to be appreciative of, it has also resulted in the commission of numerous types of cyber-crimes (a cyber-crime can broadly be defined as an illegal activity which uses a computer). It has been observed that state and national borders are rendered redundant with respect to such cyber-crimes.

Cyber-crimes can be classified into two major categories of offenses: in the first, the computer is the target of the offense. Attacks on network confidentiality, integrity and/or availability - i.e. unauthorized access to and illicit tampering with systems, programs or data - all fall into this category. The other category consists of traditional offenses (such as theft, fraud and forgery) that are committed with the assistance of, or by means of, computers, computer networks and communication technology. This article employs the broad definition of "cyber-crimes", referring to offenses falling into either category.

Furthermore, as the world has been reduced to a small global village because of the penetration of the internet into each and every

* Hon'ble Judge, Punjab and Haryana High Court, Chandigarh.

country, it knows no boundaries or barriers. Cyber-crimes are committed involving more than one country, concerning more than one sub-continent. Where the prosecution of such a cyber-crime would lie is a question that baffles many.

Determining which country has jurisdiction for the purposes of a criminal prosecution may establish whether the conduct would be a crime, how the crime would be defined, and how it would be punished. Ellen S. Podgor, in her celebrated disquisition, has etched out the cardinal issues in determining jurisdiction in cybercrime. First, the absence of a geographical boundary for commission of the crime; second, the glaring lacuna in the legal arena with the lack of a settled law thriving internationally and the existence of conflicting laws; third, the existence of either positive juridical claims where many countries claim to exercise jurisdiction and the negative juridical claims where there is no claim for jurisdiction by a single country, resulting in crimes going unpunished.

The lack of juridical solutions offered by the P8 expert group set up by the G7 and the plethora of cases that followed only added to the complexity of the issues related to cyber-crimes. A dire need for discussion and setting of rules called for The Budapest Convention on Cybercrime of the Council of Europe which came into force on July 1, 2004 and is one of the most important international documents focused on combating international crime. Article 22 of this Convention titled 'Jurisdiction' deals with requiring countries to accept jurisdiction on the basis of both territorial and nationality basis and also permits the country to disregard any of these bases of jurisdiction.

The Convention also sheds light on the extradition of offenders and the refusal of extradition by a particular country. On the more important question of resolution of conflict of laws, the Convention exudes international cooperation and states that "*when more than one Party claims jurisdiction over an alleged offense established in accordance with this Convention, the parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*"

The Convention on Cybercrime is based on certain agendas. The first goal is the establishment of a specific list of domestic criminal offenses and conducts that are prohibited. The second goal is to adopt a set of

procedural tools and powers to properly and effectively investigate crimes. The last goal is to establish strong mechanisms for fostering international cooperation. The offenses are broken down into the following areas: fraud and forgery, child pornography and copyright infringement (intellectual aspects of hacking). Further, the Convention, from the onset, outlines the areas and provisions which will be treated differently with regards to the procedural or substantive legal processes. The root problem is that for an offense to be considered a crime under the Convention, it would have to be a crime in both the nation it was committed in, and in the nation whose assistance is being lent. Thus, it closes the door on the possibility of extradition.

Moreover, while understanding jurisdictional issues, it is imperative to have an understanding of what the term 'jurisdiction' itself denotes. Black's Law Dictionary defines jurisdiction as "*A Court's power to decide a case or issue a decree; A geographic area within which political or judicial authority may be exercised*". Jurisdiction in cyber-crime encompasses the power to legislate, the power to hear, personal jurisdiction, ability to serve notice, subject-matter jurisdiction, the power to adjudicate, governing law or choice of law, *forum conveniens* or *forum non conveniens* and the enforcement of judgments.

Save for the Council of Europe's adoption of the Convention on Cybercrime, which has been ratified by most countries in the Council of Europe, as well as some other non-member states such as the United States of America, Japan, Canada and South Africa, there has been no international consensus among nation states regarding jurisdictional and prosecution matters for cyber-crimes. As there is no special agreement between all countries regarding distinct jurisdiction for cyber-crimes, traditional jurisdictional standards have to be resorted to in order to resolve all civil internet disputes.

In *The People of the State of New York vs. Gaming Corporation* 714 NYS 2d 844, an online gaming company based in Antigua (where online gambling is legal) maintained corporate offices in New York, a state where online gambling is illegal. The issue in this case was whether the State of New York could bring the online gambling company under its jurisdiction and prosecute it for offering gambling to internet users in the state. The court held that the State of New York had the jurisdiction to prosecute the gambling company as it was *in personam* located in New

York, and thus came within the jurisdiction of a competent court in New York. This illustration provides us the crux of the problem regarding jurisdiction. A company which is based primarily in a foreign land, Antigua, which doesn't seek to cater to the people of New York specifically, was prosecuted successfully in New York simply for having an office in the state. It also leads us to ask what the outcome of the case would have been if the company did not have an office in the state. Could the company have escaped liability even though it provided the people of the state of New York with online gambling facilities?

The confusion regarding jurisdiction in cyber-crimes is apparent. This can be attributed to the lack of a common ground in the framing of cyber-laws by countries. The internet transgresses geographical territories and hence, there must be a common footing for the laws. However, no such common ground exists. Thus, it is evident that the need of the hour is an international convention with all nation states as signatories, with general guidelines for efficient policing of cyber-crimes, and an understanding between countries on how to settle transnational disputes. Guidelines on implementation and prosecution must also be agreed upon. There is a requirement of speedy and urgent preservation of evidence which is synonymous with cyber-crime investigations, and the present mechanisms are lacking in this aspect. This would be possible with the resolution of the numerous jurisdictional issues, and speeding up the prosecution process. International cooperation with respect to cyber-crimes should be to the widest possible extent. There should be a consensus on the identification of cyber-crimes, which will be a step in the right direction to resolving jurisdictional issues. Thus, it is evident that international consensus and cooperation on jurisdiction are the only possible ways to effectively tackle the issue of cyber-crimes.

As stated previously, cyber-attacks do not entail any boundaries. They involve multiple players, raising serious concerns regarding the exercise of jurisdiction. Since the nature of the problem is collective, therefore, an amicable remedy needs to be evolved without deviating from the target of curbing cyber-crime. The Information Technology Act, 2000, also appears to be deficient and unless its provisions are appropriately updated , it may not prove to be an effective tool or a comprehensive law to cover all the legal issues related to cyber-crimes. Even the recent amendment of 2008 is silent on the issue of jurisdiction.

While adjudicating cyber-crime issues involving multiple players, the courts must consider the procedural and substantive policies of other countries whose interests are affected by the court's assertion of jurisdiction .Similarly, utmost care and reasonableness must be exercised without jeopardising the principles of natural justice while extending jurisdiction into the international field.

Since the scope of cyber-crime tends to extend to the international sphere, it is therefore imperative that international conventions and agreements be ratified by the maximum number of nations to cultivate international cooperation, with extradition being one example of the same. However, at present, it is also plagued with various flaws. Extradition is not permitted unless the act constitutes a crime under both states - the requesting state and the state to which the request is made. The domestic law fails when the crime is not recognised under the perpetrator's country.

Consequently, there is an urgent need for creating an umbrella law or convention which covers almost all major crimes related to the cyber world, and the maximum number of nations must be a member of such a convention through ratification. Moreover, a specialised court as a sub-division of the International Criminal Court needs to be established at the international level which should solely deal with cyber issues. Experts related to the cyber sphere should be appointed to adjudicate such matters. Further, India must strengthen the domestic laws by bringing about significant changes in order to make a strong claim over jurisdiction. Additionally, even at the domestic level, it is imperative to establish specialised courts which deal with cyber issues exclusively. Mutual legal assistance and international cooperation can pave the way for swift disposal of cyber-crimes and disputes. Developed nations must take the initiative in discovering the panacea to cyber-crimes. International conventions and treaties can be one of the tools to consolidate the varied troubling issues with respect to the virtual world. It is crucial that jurisdictional issues be harmonised between nations, which must ensure that they lay strong emphasis on retaliating against cyber-crimes collectively and effectively. If these issues are ignored, preventing cyber-crimes will unfortunately be a herculean task in front of the international criminal law system in the coming years.

*********