DE JURE NEXUS LAW JOURNAL

Author:

Hardik Bansal

Ram Manohar Lohia National Law University

3rd Year, B.A. LL.B. (Hons.)

CYBER CRIME AND THE INTERNATIONAL LAW

Abstract

In this article cyber crime is defined and characterized as a field that is yet to be fully explored especially when it comes to its proper and effective understanding globally. Considering internet and the digital era has started only recently the international law and the understanding of cyberspace still has several lacunas which make it almost impossible to understand and regulate the cybercrimes. This problem if further aggravated because of the different views and understanding when it comes to cyberspace and what exactly form a part of it along with the jurisdictional aspect of the same. It then highlights the importance and the role of laws related to cybercrimes and why they are needed. This is followed by characterizing the importance of the same keeping in mind the international law and the commitments therein. Lastly, a way forward in terms of certain measures that can be undertaken to further harmonize the cyber crime and its international understanding are emphasized.

Introduction

Cyber crime is one field of international law that is still in a very nascent stage. This is because of a multitude of reasons ranging from the definition of cyber crime and how it can easily extend boundaries and borders to have far reaching ramifications. Further, it can easily lead to leakage of confidential information of not only individuals but also important government organizations or bodies. It also becomes a major threat that has to be paid heed to and given its due attention considering that we live in an interconnected world wherein because of cyber

connectivity not only has the lines been blurred and better accessibility has come about; but also, we are now more than ever prone to major cyber-attacks and cyber threats be it from individuals or specific organizations working and targeting in this regard. Apart from this aspect cyber-crime also leads to defamation of important heads of state, leakage of pornographic material, obscenity, among several other such things. The question therefore arises as to how should this regulation come about and the proper implementation mechanism of the same. The blurring lines between the places from where the cyber crime has actually taken place and how to properly ensure the liability of an individual or should the liability rest with a state are some of the other major concerns when we try to talk about cyber-crime and the international law. Considering that international law is often not legally enforceable unless the states have ratified the treaties it is important that specific important legal documents, treaties and conventions are put into effect to ensure that crimes happening even through the online means are covered in sufficient safeguards and at least there is some basis or common consensus between the nation states and the members of the United Nations when it comes to how to go about addressing these key concerns and therefore solving the predicaments related to the same. To start this discussion, it is important that before moving forward with how the development of cyber crime and the linkage of the same with international law look like, we pay much needed attention to why the governance and regularization of cyberspace itself is a major issue that needs to be addressed at the earliest.

Regularization of Cyberspace

To understand the dynamics related to what is regularization it is important first and foremost to characterize cyberspace. Considering that cyberspace is actually not a real phenomenon but is a place where just computer and electronic medium exist as a means to an end it is very difficult to recognize and pinpoint on the jurisdiction of cyberspace. On one end people argue that the moment we have some amount of effective control over the medium of cyberspace, the freedom and liberty associated with the free flow of ideas through the online medium will get curbed and hampered to a large extent and thus the benefits accruing out of it would also get curtailed. On the other hand, it is believed that States should be the one to formulate certain laws related to national and international level for the governing of this cyberspace. There is also a view that this regularization should only come about through the International Institutions such as the United Nations considering how cyberspace is something that extends boundaries and has multilateral aspects.

Now focusing more on the aspect of jurisdiction the people in the cyberspace exercising control are also very diverse as they are inclusive of hackers, individuals who are using cyberspace normally such as for contacting their peers, small companies, big companies or even states at large. The regularization thus for all of these actors would thus be very different from each other and would have very distinct and different nuances for each and every one of them. Then the issue arises as to what conduct is the one that should be regulated and what should not be allowed. Is it fine to let's say make parodies which are insulting in nature and upload them online or comment hurtful comments in the way of a joke or is the same is also derogatory and not allowed? Again, the balancing of the freedom of speech and expression along with the regularization of the cyberspace becomes another key issue. Apart from this aspect also the complexities attached to the interplay of various actors that are in play when it comes to cyberspace and the legal enforceability of the issues thereafter is another key concern. Considering that when it comes to international treaties and obligations still there is a lack of proper narrative or any legal norms or instruments to effectively manage or regularize this cyberspace effectively or even remotely the issues keep on getting unresolved.

Another important aspect that needs consideration is the fact that states differ to a great extent when it comes to the development of cyber space and cyber laws in their own jurisdictions. This means that a first world developed country such as the United States of America would have a much-developed legal system with regards to cybercrimes and cyberspace as compared to other third world countries that are still at a very nascent stage in terms of their development and growth. Perhaps, for these countries' cyberspace might not even be an issue of immediate concern hence often discussions related to the same are also neglected not only domestically in these nations but also when their interests are represented at international platforms. However, it is worth noting herein that the problems do not just end here. Even developed countries that have well developed legal regimes to keep in check the cybercrimes and the cyber regime often have very different laws and understanding of the same from each other. This again poses serious ramifications and problems when it comes to a common international understanding of how the regularization should actually come about. Perhaps international customary law is something that can work effectively in this regard to highlight and elaborate upon the conduct that parties necessarily should have when it comes to each other. However, even this issue would again suffer from the lack of disparity among the countries when it comes to laws related to the cyberspace and the role and importance of the same.

Digital Sovereignty

In this backdrop the importance of digital sovereignty is another idea that has been a moot point for discussions when it comes to cyberspace and cybercrimes therefore. It basically is the idea that several facets related to control over the digital realm when it comes to the infrastructure of the same; or when it comes to the communication happening over the internet; or with regards to the accessibility among other such issues should be primarily dealt with by the international actors or important functionaries therein.

This idea has been gaining much prominence because of the role played by countries like China and Russia in this regard. Both have extensively called for and focused on greater control when it comes to their own cyberspace and recognizing the need of greater autonomy in this regard. They also have thus focused on the issues related to non- interference by other international bodies and instruments related to cyber space and the regularization therein. This idea is problematic on multiple grounds as it would effectively mean that digital realm rather than being a common ground would thus be fragmented and it would be extremely difficult to thus have any international instruments or binding agreements in place to make sure that countries actually fulfil their international obligations and there is a common law to govern cyber crime and regularize the cyber space in this regard.

Role of Cybercrime Law

In this regard it is important therefore to establish the role of cybercrime law which would basically enlist certain behavioral standards and norms that are generally by and large accepted by all the countries as the right conduct for the users of the cyberspace. Further the social-legal aspects of the same apart from just the legal ramifications would also be dealt with by the cybercrime laws in the international settings. It would enlist also the procedure that has to be followed and how the countries would thereafter cooperate amongst themselves to ensure that any crime done in the cyberspace is well regulated and thereafter effectively the punishment or the remedies thereafter are put into effect. Thus, it should include multiple levels among itself to ensure that cybercrime is effectively tackled in the international settings.

At the very onset there should be a certain substantive law in place, which in essence means that there should be explicit punishments mentioned and the acts which would result in those punishments. This means that for the cybercrime law to be effective the laws need to be clear and well understood as to the act which is a punishable offence and also as to the punishment of the same or in essence the ramifications of the said act. This can be done in the form of

statutes or penalties in place. For instance, the Iraqi Penal code[1] or The Indian Information Technology Act[2] are two examples which contain substantive provisions regard to punishment of crimes done via the cyberspace or cyber crimes such as identity theft[3]. These cyber crimes would thus like any other crime would have two aspects that would be properly prescribed namely the actus reus or the or the guilty act as it is often referred to along with the mens rea or the guilty mind aspect. It would vary on a state-to-state basis but for an effective regime to come about it is important that certain international ramifications which are common across nations are also thought about.

The next aspect therefore would be the procedural law which would in turn list out the procedure as the name suggests along with the processes that would have to be followed. This would include but not be limited to let's say the jurisdiction aspect, role of evidence and how the same has to be gathered for it to hold value during the trial, the powers with regards to the investigation being done by the police or any other important designated authority. For instance, in India the criminal procedure code[4] talks about the same.

The last aspect but perhaps the most important aspect when it comes to the interplay of international law and cyber crime in this regard would arguably be the preventive law which would focus on mitigating the risks and the damages associated with the cyber-crimes and also regularization of the same. It would thus focus on either preventing the crime altogether through certain important steps or thereafter minimize the negative impacts and damages that have been caused because of the same. In this regard certain countries have enacted laws such as Ukraine[5]. Even certain international bodies have enacted specific laws targeting certain aspects related to cybercrimes such as the EU General Data Protection Regulation of 2016[6] or the African Union Convention on Cyber Security and Personal Data Protection of 2014.[7] These are important regional instruments that need to be looked at from a global perspective especially through bodies such as the United Nations that are not only limited to a particular region but are inclusive of all the major countries in the world.

International Harmonization

[1]Iraqi Penal Code No. 111 of 1969.
[2]The Information Technology Act, 2000 (Act 21 of 2000).
[3]The Information Technology Act, 2000 (Act 21 of 2000), s. 66.
[4]The Code of Criminal Procedure, 1973 (Act 2 of 1974).
[5]The Law of Ukraine on the Basic Principles of Ensuring the Cyber Security of Ukraine of 2017.
[6]The European Union General Data Protection Regulation of 2016.
[7]The African Union Convention on Cyber Security and Personal Data Protection of 2014.

Again, these instruments and legal functionaries would have no practical implications unless there is some amount of harmonization not only between the domestic legislations of these countries but also an international common understanding that might stem from a common interpretation of cybercrime and the cyberspace. In this regard although several legal instruments and treaties have been worked upon by many regional level bodies such as various directives of the European Union in particular the directive of 1995[8] that emphasized on the importance of data privacy and protection of personal data and even the Interpol or the International Criminal Police Organization has taken several efforts in this regard, a combined approach directly tackling the issues related to cyber crimes and harmonizing and unifying the same with international laws still remains a sort of a herculean task.

In this regard although numerous organizations exist, none has the numerical strength of the United Nations which effectively boasts of about 193 countries as its member with certain other functionaries also occupying the position of observers. In this regard although United Nations General Assembly has had several resolutions[9] in place over the years none has had a binding value or any concrete far reaching consequences. For instance, although the UN General Assembly Resolutions[10] have focused on the aspect of cybercrimes and data security as early as 1985 there hasn't been any concrete change or steps taken by the governments domestically to harmonize the same with the international laws and recommendations made by the United Nations General Assembly. Cybercrime, computer related aspects and data breaches along with investigation and coordination when it comes to cyber crimes have all be dealt with but unless there is a proper understanding of cyberspace and jurisdictional aspect of the same the interplay between cyber crime and the international law therefore is yet to properly see the proper light of the day.

Conclusion and The Way Forward

For the international community to recognize the importance of cyber crimes it is imperative that UNSC resolutions which are considered to be binding in nature according to the United Nations Charter Article 25[11] be made in the earnest possible instance. Further, considering that a lot of countries do not have such developed cyberspaces it is imperative that recognition of the protection of cyberspaces and ensuring that cyber criminals do not go Scot free in such

[8]The European Parliament and the Council Directive 95/46/EC of 24 October 1995.
[9]The United Nations General Assembly Resolution A/RES/51/162 of 30 January 1997.
[10]The United National General Assembly Resolution 40/71 of 11 December 1985.
[11]The United Nations Charter, art. 25.

legislation especially should be the need of the hour of the international communities. Countries that are still in very early stages of reaching their developmental goals and aspects in regards to the digital age often have lacunas in the legal systems which result in cyber criminals either within their territory or even outside to get away with the crimes that they have committed.

This aspect aside it is important that the present threats with regards to how the cybercrimes can have far reaching consequences such as in the form of cyber terrorism is also recognized at the earnest. In many places online mediums have been used to spread negativity and fake propagandas to enlist support against the legitimate government in power. A proper international instrument in place that is ratified by most countries would also ensure that the same is effectively taken care of by and large through common cooperation and jurisdictional understanding of the same. Herein capacity building measures and support by countries who already have a lot of know how when it comes to cyberspace towards countries who are still developing in phases or still at nascent stages can go a long way.

Thus, by having binding international treaties and obligations in place with regards to the cyberspace along with a common international understanding of what exactly constitutes cyberspace and how the same has to be regulated can act as a starting point. This subsequently has to be followed by emphasizing on the aspects and role of cybercrimes and the different laws that need to be made both domestically and internationally in this regard. Lastly though common cooperation and capacity building measures being undertaken by the international community by and large the negative impacts and ramifications of cybercrimes can be minimized and tackled effectively.