International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

An Evaluation of the Jurisdictional Aspects of Cyber Crimes under the Regional Agreements with Special Emphasis on the Budapest Convention

S. Karpagapriya

M.L., Advocate, High Court of Madras.

Abstract

Since the advent of the Internet at the tail end of the 20th Century, policymakers have strived to create the perfect convention to regulate the burgeoning transnationality of cyberspace and subsequently, crime within cyberspace. While the Budapest Convention remains the most comprehensive cybercrime treaty to date; several regional treatises have been formulated specifically to serve diplomatically aligned BLOCs. Despite all this, there exists a vacuum in the international fora that can only be fulfilled by an extensive and intricate document regulating cyberspace, which has global enforcement. This article aims to analyze the jurisdictional provisions in some of the most significant cyber treatises and propose an exhaustive and extensive charter that would, on paper, fill in the current Cybercrime legislation. It hopes to tackle the tricky challenge of territorial jurisdiction and sovereignty of states when it comes to the prosecution of cybercriminals.

Keywords: Cybercrime, Jurisdiction, Conventions, Harmonization

Contextualizing the Budapest Convention

This article covers the conception of the Budapest Convention and various other regional agreements to combat the growing scale of cybercrime. It further discusses the parallel regional conventions instituted by blocs to support their specific requirements and how they work for the local legislations therein.

The Committee of Ministers of the Council of Europe decided in February 1997 to establish the Committee of Experts on Crime in Cyberspace (PC-CY). The primary goal of this committee was to formulate a legally binding global treaty on cybercrime. (Cristina Schulman, et. al., 2001) [1].

Providing a precise and succinct description of the concept of jurisdiction is of utmost importance. Jurisdiction pertains to the ultimate authority of a nation to establish and uphold laws within its specific territorial limits [2]. Article 22 of the Convention on Cybercrime outlined several criteria regarding the jurisdiction for cybercrimes. Jurisdiction is created within a nation where cybercrime is committed.

[1] Cristina Schulman, Alexander Seger, Convention on Cybercrime: Special edition dedicated to the drafters of the Convention (1997 – 2001), pg. 1, pg. 6 – 7, 2022, https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e
[2] Convention on Cybercrime Budapest, Art. 22, 2001, https://rm.coe.int/1680081561

Treatises Governing the Cyberspace

UNCITRAL Model Law

The UNCITRAL Model Law on Electronic Signatures was enacted in 2001 with the purpose of permitting the use of electronic signatures as a substitute for handwritten signatures. The United Nations Convention on the Use of Electronic Communications in International Contracts was held in New York in 2005. The agreement was developed with the aim of removing the obstacles encountered in international trade by leveraging internet communications (Jonathan Clough, 2015) [3].

Chapter IV of the provision delineates the scope of authority of the arbitral tribunal; specifically, article 16 elucidates the tribunal's power to make decisions on its jurisdiction [4].

International Telecommunication Union (Constitution and Convention of the International Telecommunication Union)

The main goal of ITU, from its inception, has been the standardisation of technology. Established in 1956 as the International Telephone and Telegraph Consultative Committee, commonly referred to as CCITT (derived from its French name Comité consultatif international téléphonique et télégraphique), this organisation is tasked with establishing worldwide telecommunications standards, excluding radio (Wilfried Hesser) [5].

Section 3 outlines the criteria used to ascertain the international nature of a criminal offence [6].

GDPR (General Data Protection Regulation)

The General Data Protection Regulation (GDPR) of the European Union (EU) is now the most stringent legislation guaranteeing individuals' entitlement to digital privacy. The diverse tactics utilised exemplify the divergent stances taken by nations about the governance of the digital realm and control over data ownership. These inconsistencies are evident in other United Nations objectives, which includes counterterrorism, human rights, and international peace and security. They have impeded states' ability to establish a universally applicable authority for addressing cybercrime. (He Li, et. al., 2019) [7].

CCPCJ (Commission on Crime Prevention and Criminal Justice)

Cybercrime and the United Nations System: Platforms for discussion: the Commission on Crime Prevention and Criminal Justice (CCPCJ) serves as the primary platform for United Nations deliberations on the subject of cybercrime. In 2010, Russia proposed a cybercrime treaty at the Twelfth UN Crime Congress. Nevertheless, the conversations proved fruitless as they were hindered by disputes concerning national sovereignty and the protection of online rights [8].

[3] Vimlendu Tayal, Cyber Law, Cyber Crime, Internet, and E-commerce: Being a Comprehensive Treatment of the Subject with Useful Appendices, Including the Information Technology Act, 2000 (as Amended in 2009), Guide to Globar E-commerce Law, UNCITRAL Model Law, Convention on Cyber Crime, Cyber Crime FAQs, Glossary of Terms, Etc. India, Bharat Law Publications, 2011.

[4] United Nations Commission on International Trade Law (UNCITRAL), Art. 16, 1966. https://uncitral.un.org/

[5] Wilfried Hesser, An Introduction to Standards and Standardization, Beuth.

[6] United Nations Convention against Transnational Organized Crime and the Protocols Thereto, Art. 3.

[7] He Li, Lu Yu & Wu He (2019) The Impact of GDPR on Global Technology Development, Journal of Global Information Technology Management, 22:1, 1-6, DOI: 10.1080/1097198X.2019.1569186

[8] UN rejects Russian cyber-crime treaty, https://www.itproportal.com/2010/04/21/un-rejects-russian-cyber-crime-treaty/ [accessed on: September 2022]

The primary subjects discussed encompassed the ever-changing dynamics of cybercrime, apprehensions regarding an underground cyber economy that trades in data and facilitates diverse criminal activities or terrorism, and the intricacies involving legal protocols for cloud computing and data retrieval [9].

ASEAN Declaration to Combat Cybercrime

The importance of enhancing collaboration and coordination between ASEAN bodies and relevant national bodies or organisations in tackling cybercrime was highlighted. This objective can be accomplished by facilitating the transfer of knowledge, sharing experiences, and promoting the adoption of best practises [10].

It is recognised that even states that are prepared to collaborate, particularly the member states of ASEAN, face difficulties in reaching universal consensus on extensive and explicit legislation regarding a legal matter (Anselmo Reyes, 2014) [11].

Arab Convention on Combating Information Technology Offences

The Arab Convention on Combating Information Technology Offences (Arab Convention) covers a wider range of criminal actions in comparison to the Budapest Convention. The violations included in this grouping are unauthorised access, unauthorised interception, offences against data integrity, misuse of information technology, offences committed through information technology such as forgery, fraud, pornography, and offences related to terrorism, organised crime, copyright, and related rights, as well as the unauthorised use of electronic payment tools (Khalifa, Abdelmonem Mohamed Magdy, 2020) [12].

According to Article (30) of the Arab Convention, a country that is a party to the convention must enforce the necessary measures to extend its legal authority to include any of the acts mentioned in the convention, if the crime is partially or completely committed within the country's territory, on a ship or plane registered in the country, or by a citizen of the country [13].

The Asia-Pacific Economic Cooperation (APEC) In the Asia-Pacific region

The APEC organisation facilitates the synchronisation of the endeavours of its 21 participating economies to promote cybersecurity and tackle the perils presented by cybercrime (APEC, 2003) [14].

Articles 6, 7, and 9 define the jurisdiction and extent of authority of the states involved [15].

The European Union

The European Union has established various efforts to combat cybercrime by advocating for a cohesive approach to law enforcement and the establishment of regulatory standards. The preservation of civil liberties has been a central focus in the efforts to combat cybercrime (Fernando Mendez, 2005) [16].

[9] UN Doc. E/2018/30 - E/CN.15/2018/15, paras 38–40.

[10] ASEAN DECLARATION TO PREVENT AND COMBAT CYBERCRIME, as adopted on 13th Nov, 2017, https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

[11] Anselmo Reyes (2014) ASEAN and The Hague Conventions, Asia Pacific Law Review, 22:1, 25-44, DOI: 10.1080/10192557.2014.11745914

[12] Khalifa, Abdelmonem Mohamed Magdy. Overcoming the conflict of jurisdiction in cybercrime. 2020. American University in Cairo, Master's Thesis. AUC Knowledge Fountain. https://fount.aucegypt.edu/etds/846 [accessed on: March 2022]

[13] Article 30, Arab Convention on Combating Information Technology Offences, 2010.

[14] APEC (2003). Conference Report: Cybercrime Legislation and Enforcement Capacity Building Project, 21-25 July 2003, Bangkok, Thailand

[15] Asia Pacific Economic Cooperation, Art 7(ii), 2009—Limitations on Assistance, https://www.apec.org/

Jurisdiction under Directive 95/46/EC

In the legal case C-230/14 Weltimmo v Nemzeti, a company established and operating in Slovakia allowed Hungarian people who possessed holiday properties to advertise their units on its online platform for real estate. The central question was whether the Hungarian data protection authority have the legal jurisdiction to commence enforcement actions against the firm that was formally established in Slovakia [16].

The CJEU determined that data protection authorities are not required to take into account a contradictory decision taken by a different data protection authority, and that the data protection authority situated in the jurisdiction where the primary data controller works does not possess precedence [17].

The Organization of American States (OAS)

The Organisation of American States (OAS) recognises the importance of a robust legal structure to combat cybercrime and protect the Internet. This is evident through its enduring forum for the Ministers of Justice or the Ministers or Attorneys General of the Americas (REMJA) [18].

Shanghai Cooperation Organization

The organisation holds the distinction of being the greatest regional entity worldwide in regards to both geographical expanse and populace, covering around 60% of the Eurasian landmass and comprising 40% of the worldwide population. In 2021, its aggregate GDP constituted almost 20% of the worldwide GDP [19].

African Union (AU) Convention on Cyber Security and Personal Data Protection

The African continent has witnessed substantial growth in the field of Information and Communication Technology (ICT) and the utilisation of the Internet in the 21st century. Recent research shows that the quantity of Internet users in Africa rose from approximately 4.515 million individuals in 2000 to 453.3 million individuals by December 2017. This accounts for around 35.2 percent of Africa's overall population estimation [20].

The Commonwealth of Nations

The Commonwealth of Nations expeditiously implemented efforts to harmonise the legislation of its member states. The Commonwealth Secretariat created the "Model Law on Computer and Computer Related Crime" in October 2002. The "Model Law" has had a substantial influence on the domestic legislation of all 53 member countries of the Commonwealth. The model law has included the Convention on Cybercrime as a feasible choice within the domain of substantive criminal law. The term "cybercrime" covers a variety of illegal activities, such as unauthorised access, data manipulation,

[16] Weltimmo v Nemzeti, C-230/14
[17] Ibid.
[18] Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas (REMJA II), Chapter V
[19] Iran looks east after China-led bloc OKs entry, https://www.france24.com/en/live-news/20210918-iran-looks-east-after-china-led-bloc-oks-entry [accessed on October 2022]
[20] Miniwatts Marketing Group, Internet Usage Statistics for Africa, 2017 http://www.internetworldstats.com/stats1.htm [accessed on November 2022]

disruption of computer systems, illegal interception of data, unlawful possession of data, and the production or distribution of child pornography (Bourne R, 2002) [21].

The Group of Eight (G8)

Starting in the mid-1990s, the Group of Eight (G8) has formed working groups and issued a series of statements by the heads and plans of action by justice ministers [22].

The Organization for Economic Cooperation and Development (OECD)

The OECD implemented the Guidelines for the Security of Information Systems and Networks in July 2002. The guidelines stress the need of member nations prioritising security planning and management. Additionally, they encourage the cultivation of a culture focused on security among all those involved in order to safeguard information systems and networks [23]

Harmonization of legislation

Various international organisations have placed major emphasis on promoting the harmonisation of legal frameworks. The process of harmonisation in Europe began in the 1980s and reached its culmination with the recent achievement of the Convention on Cybercrime. In addition, numerous international organisations have undertaken initiatives to attain legal consistency and have also implemented mechanisms to evaluate legislation and encourage economies to enact comprehensive laws that are in line with the Convention on Cybercrime and related United Nations resolutions (Li Xingan, 2007) [24].

The way forward:

The jurisdiction prescribed by the Budapest Convention and various regional agreements to combat cybercrimes were analyzed in this article. Information technology is a global phenomenon and it reveals the interdependence and interconnectivity of the contemporary world. With the advent of information technology, the cybercrimes have also grown alarmingly. The issues pertaining to cybercrime jurisdiction are still a challenge in today's world. The United Nations should work towards a global UN convention on cybercrimes addressing issues pertaining to jurisdiction, mutual legal assistance and other relevant areas. Though the various regional conventions prescribe some guidelines relating to ascertaining jurisdiction and mutual legal assistance in the areas of cybercrimes, still there is a long way to go to combat cybercrimes. Like the INTERPOL, if **CYBERPOL** is established to regulate cyberspace wherein all the sovereign nations could collaborate and cooperate in combating cybercrimes, this unregulated space could be regulated to a greater extent. As early as 2007, when I represented India at the 5th International Conference on Cyberspace held at the University of Masaryk, Brno, Czech Republic to present my paper along with my co-author P.T. Kamalapriya on "Combatting Cybercrimes", we put forth a suggestion before the international community that if "**CYBERPOL**" be constituted by the sovereign nations of the world", it could to a great extent regulate the unregulated cyberspace.

[21] Bourne, R. (2002). Commonwealth Law Ministers' Meeting: Policy Brief. London: Commonwealth Policy Studies Unit.
[22] G7, Chairman's Statement, 17 June 1995, Halifax Summit, 15-17 June 1995
[23] Organization for Economic Cooperation and Development (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.
[24] Li, Xingan. "International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene." Webology, 4(3), Article 45, September 2007

Cyber activities are not governed by geographical borders, which makes dealing with such crimes all the more confusing and complex and therefore a lot of cybercrimes go unreported. Apart from the international law and guidelines in this field in the nature of regional conventions, treaties and agreements, it is also important to understand how the different jurisdictions of different nations work in order to check the invisible vast omnipresent cyberspace. The United Nations' effort to adopt an international convention on cybercrimes can be a great step to end the menace of cybercrimes.