„Krytyka Prawa", tom 15, nr 4/2023, s. 95–111, ISSN 2080-1084, e-ISSN 2450-7938, © 2023 Authors.

GAZAL GUPTA[1], PARINISHTHA JINDAL[2]

Jurisdiction: an Issue on the Internet[3]

Submitted: 2.04.2023. Accepted: 22.09.2023

Abstract

This article examines the jurisdictional status of the internet. Because of the underlying nature of technology, nations cannot effectively monitor online transactions that originate or conclude within their borders. Governments can seek to enforce their laws within the constraints of their physical, geographical, and political domains as defined by an atlas, but a borderless cyberworld regulated by fast--expanding technology has a variety of challenges. This study sheds light on those challenges, the jurisdiction for parties to suit, the remedies accessible to them, and the territorial concerns discussed in various domestic courts. It also focuses on the pressures on stakeholders to act, as well as the economic, human rights, and technological infrastructure implications of jurisdictional concerns. In general, jurisdictional issues on the internet have resulted in haphazard and unrestricted jurisdictional implementations, and this article emphasizes the territorial difficulties of internet administration and its direct influence on many nations and elements.

Keywords: jurisdiction, issue, internet, borderless, cyberworld.

[1] Gazal Gupta – Manipal University Jaipur (India); e-mail: gazal.181301022@muj.manipal.edu; ORCID: 0000-0002-7232-5133.

[2] Parinishtha Jindal – Directorate General of Hydrocarbons under the Ministry of Petroleum and Natural Gas (India); e-mail: parinishtha@supportgov.in; ORCID: 0009-0002-5417-5685.

[3] The research in this article has not been supported financially by any institution.

 DOI: 10.7206/kp.2080-1084.641

„Krytyka Prawa", tom 15, nr 4/2023, s. 95–111, ISSN 2080-1084, e-ISSN 2450-7938, © 2023 Authors.

GAZAL GUPTA, PARINISHTHA JINDAL

Jurysdykcja – problem w internecie[4]

Streszczenie

Autorzy badają jurysdykcyjny status internetu. Z powodu zasadniczej natury technologii państwa nie mogą monitorować internetowych transakcji, które zaczynają się lub kończą w granicach tychże państw. Rządy mogą dążyć do wprowadzania ustaw w granicach dominiów fizycznych, geograficznych i politycznych, jednak pozbawiony granic cyberświat regulowany przez szybko rozwijającą się technologię zmaga się z różnymi wyzwaniami. Niniejszy artykuł rzuca światło na te wyzwania, na jurysdykcję odpowiednią dla stron procesu, na środki, które są dla nich dostępne, oraz na problemy terytorialne omawiane w różnych sądach indyjskich. Autorzy skupiają się też na presji spoczywającej na udziałowcach i motywującej ich do działania oraz na prawach ekonomicznych, prawach człowieka i powiązanych z technologiczną infrastrukturą następstwach problemów dotyczących jurysdykcji. Ogólnie rzecz biorąc, kwestie związane z jurysdykcją w internecie poskutkowały przypadkowymi i nieograniczonymi realizacjami w sądownictwie, a niniejszy artykuł podkreśla trudności terytorialne pojawiające się w przypadku administracji online, a także bezpośredni wpływ tej ostatniej na wiele państw i elementów prawa.

Słowa kluczowe: jurysdykcja, problem, internet, bez granic, cyberświat.

[4] Badania wykorzystane w artykule nie zostały sfinansowane przez żadną instytucję.

Introduction

> *In managing, promoting, and protecting [the internet's] presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way for something that is so very different.*
>
> – Kofi Annan, Former Secretary-General of the UN[5]

The internet's international nature has provided mankind with unprecedented social, economic, and political benefits. Simultaneously, it creates problems within an international legal system based on the concept of territorial sovereignty. A result of the creation of the internet is that the real world no longer is the only space in which interpersonal interaction occurs.[6] On the internet, transnational meetings have become commonplace. As a result, conventional mechanisms of interstate collaboration are falling behind in the twenty-first century's digital reality. From occurrences of offensive material to cross-border access to user data, online disputes and cases of abuse provide an unprecedented challenge to the territorially confined international legal system.

When it comes to legal jurisdiction, the internet's most important feature is that it is infinite and unrestricted, which poses a big difficulty. The idea of jurisdiction refers to the authority of any competent court in any legal system to hear and decide a case. The presence of distinct parties in different regions of the world who only have a virtual nexus with one another is the major challenge with cyber law jurisdiction. Thus, the question arises: Where should the parties sue and what remedy is available to them?

Background

The cross-border aspect of the internet has supplied humanity with unrivalled benefits. When it comes to internet-related conflicts and abuse on the global network,

---

5 K. Annan, *Internet Governance*, speech at the opening session of the Global Forum on Internet Governance in New York 2004, https://www.un.org/sg/en/content/sg/statement/2004-03-25/secretary-generals-remarks-opening-session-global-forum-internet (access: 2.01.2022).

6 The Impact of the Internet on Society: A Global Perspective, [in:] Change: 19 Key Essays on How the Internet Is Changing Our Lives (BBVA OpenMind) (2022).

 DOI: 10.7206/kp.2080-1084.641

however, it creates problems between national legal systems based on territoriality of jurisdiction. Nations cannot effectively supervise internet transactions that begin or end within their borders due to the underlying nature of technology. Governments can try to enforce their laws within the confines of their physical, geographical, and political realms as defined by an atlas, but a borderless cyber-world governed by rapidly evolving technology presents a number of obstacles. Even if the exact location of the computer where the transaction originates and finishes could be defined, technology may be able to circumvent or 'mask' it as well.

Jurisdiction and Sovereignty

Jurisdiction is a facet of governmental power that includes judicial, legislative, and administrative authority. Merriam-Webster defines state sovereignty as 'a country's autonomous capacity and right to manage itself'. Despite the fact that jurisdiction is a component of sovereignty, the two are not interchangeable. Because a state's (internal and external) sovereignty does not entail unfettered jurisdiction over all circumstances, international law limits a state's power to exercise jurisdiction. The conventional approach to jurisdiction requires a court to determine whether it has territorial, pecuniary, or subject matter jurisdiction to hear a dispute.[7]

Even if the internet blurs geographical and jurisdictional lines, its users are nevertheless subject to laws and physical jurisdictions, posing problems regarding jurisdiction and sovereignty.[8]

As a result, a single transaction may be governed by the laws of at least three different countries:

1. The laws of the country where the user lives.
2. The laws of the country in where the server hosting the transaction is situated; and
3. The laws of the country that apply to the person or company with whom the transaction is conducted.

As a result, a user in Australia conducting business with a user in Canada via a server in Jaipur may be subject to the laws of all three countries, as they are all relevant to the transaction.

---

7 *Jurisdiction: An Issue on Internet,* https://lawbhoomi.com/jurisdiction-an-issue-on-internet/ (access: 2.01.2022).

8 Y. Vakil, *Jurisdictional Challenges – Cyber Crime Prosecutions*, 1st edition, India, 2005, p. 29.

Stakeholders

Governments: They are responsible for upholding the rule of law on the internet, as well as protecting citizens and combating crime.

Technical operators: They are concerned that the fundamental layer distinction that underlies internet architecture may get muddled.

Global internet platforms: Rather than depending on terms of service to determine the jurisdiction of their place of incorporation, these platforms must now deal with and grasp the national laws of the various nations where they are offered.

Civil society groups: These international organizations are concerned about a potential race to the bottom when it comes to defending freedom of expression and privacy, as well as the commercialization of dispute resolution.

International organizations: Due to overlapping thematic scopes or a non-universal geographical remit, international organisations suffer. While some organizations, such as the Council of Europe, the Organisation for Economic Cooperation and Development (OECD), and the United Nations Educational, Scientific, and Cultural Organization (UNESCO), have made significant efforts to include civil society, the private sector, and the technical community in their processes, their nature remains intergovernmental. As a result, due to a lack of consensus, or worse, disagreement among its members, they are constrained in their ability to place delicate but vital matters on their agenda.

Internet and Jurisdiction

The internet's technological architecture was designed from the start to be cross-border and non-territorial, which is generally seen as a beneficial feature. However, ubiquity has exacerbated tensions since internationally available material and services may be legal in one area but prohibited or even criminal in another.[9] Interactions across borders were historically unusual, but nowadays, most daily online activities include many nations at once, offering numerous possibilities for contradictory regulations to collide. As a result, identifying appropriate laws, allowing them to be enforced, and offering redress procedures in situations of global cybercrime or illegal online behaviour is becoming more challenging.[10]

---

[9] Economic Commission for Latin America and the Caribbean, Digital Economy for Structural Change and Equality, 2019, https://www.cepal.org/sites/default/files/publication/files/46421/S1901092_en.pdf (access: 2.01.2022).

[10] M.A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, "Berkeley Technology Law Journal" 2001, 16, pp. 1345, 1356.

 DOI: 10.7206/kp.2080-1084.641

International Jurisdiction

Although it is a basic principle of international law that a sovereign state has the capacity to make and enforce rules governing activities inside its borders, there is often debate about whether such sovereign powers can extend beyond the state's borders. As a result, the corpus juris on international jurisdiction is one of the most extensive in the field of international law, and it recognizes a wide range of jurisdictional bases. Territoriality is the strongest basis for a state's jurisdiction.[11] A sovereign state must have authority over all individuals, objects, and actions within its borders, according to this idea.[12] Several extraterritorial jurisdiction bases, such as nationality, passive personality, consequences, protection, and universality principles, are recognized by the international community notwithstanding their shortcomings. The idea of nationality permits countries to claim jurisdiction over their citizens no matter where they are.[13] This argument is based on the link between states and their citizens, in which citizens are subject to the laws of their home state since they have citizenship privileges and are aware of its laws.

Similarly, jurisdiction based on the victim's nationality has been created; nevertheless, jurisdiction based on 'passive personality' is not favoured. Another important foundation for extraterritorial jurisdiction is effects jurisdiction. Under this theory, a state might claim jurisdiction over behaviour that has an impact but does not occur inside its borders. Furthermore, the protection principle has protected extraterritorial behaviour that directly damaged essential state interests, such as national security. Finally, many actions are jus cogens by their very nature, and the universality principle allows any nation to have jurisdiction over them. Many states may have concurrent jurisdiction under one or more types of extraterritorial jurisdiction in many instances, resulting in a legal disagreement. Forum selection clauses in international business contracts have become an increasingly important and acknowledged method of resolving international conflict of laws issues in the realm of global commerce.[14]

Despite the fact that the legal system worked quite well in typical scenarios, the internet created new challenges in determining foreign jurisdiction. In the analogue world, courts can quickly ascertain the geographic locations of key persons, objects, and deeds. On the other hand, the digital world of the internet is more difficult to map. Content providers may have a physical presence, do business,

11 M.W. Janis, *An Introduction to International Law*, 4th edition, Aspen, New York 2003, 318.

12 American Banana Co. v United Fruit Co. 213 US 357 (1909).

13 Blackmer v United States 284 US 421, 437 (1932).

14 M/S Bremen v Zapata 407 US 1, 15 (1972).

and host their servers in one location, yet their content is accessible from everywhere on the planet. Furthermore, determining a user's position via the internet has proven to be incredibly difficult, and many internet users exacerbate the situation by purposefully concealing their whereabouts. Traditional international jurisdictional ideas, such as territoriality, are ineffective in dealing with this type of geographic anonymity. Despite the attempts of courts to discover a satisfying answer, there has been little movement towards a single global internet jurisdiction rule.

Importance of the Issue of Jurisdiction

When several parties from different regions of the world are engaged, it is required to identify whether a given occurrence on the internet is governed by the laws of the user's nation, the service provider's country, or the person or business with whom the transaction takes place. As a result, while selecting the proper jurisdiction, the following major considerations must be addressed:

1. Which country's law governs cross-border interactions, and which court has authority over them?
2. What basis does a country have to claim that it is enforcing laws and regulations if internet activity originates in multiple jurisdictions?

Personal Jurisdiction

Personal jurisdiction was one of the first attempts to reject political power. Courts in the United States have had a difficult time finding out how to apply traditional jurisdiction concepts to online conduct. In *Asahi Metal Industry Co. v. Superior Court*, the Supreme Court was more stringent, limiting personal jurisdiction to circumstances where the defendant 'purposefully avails' himself of the forum.[15] Personal jurisdiction is likewise subject to a reasonableness test, according to the Supreme Court in *World-Wide Volkswagen v. Woodson*.[16] Similar rules exist in other states, where a court's ability to hear a case is determined by the defendant's connection to the forum state. Defendants have frequently claimed that a remote forum is free from jurisdiction, since all connections are made entirely through a server situated outside the forum.[17]

15 Asahi Metal Industry Co. v Superior Court 480 US 102, 112 (1987).

16 World-Wide Volkswagen v Woodson 444 US 286, 297 (1980).

17 Barrett v Catacombs Press 44 F. Supp. 2d 717 (EDPa. 1999); Machulsky v Hall 210 F. Supp. 2d 531 (DNJ 2000).

 DOI: 10.7206/kp.2080-1084.641

Choice of Law

In the case of *Twentieth Century Fox Film Corp. v. iCrave TV*, a film studio obtained an injunction against one Canadian service that may legitimately stream video in Canada from Canadian servers.[18] Because the unlawful material might be viewed in France, the court in France determined that the French penal code extended to Yahoo! activities. In a recent libel case, the United Kingdom followed a same approach, determining that the place of downloading determined the appropriate statute. The European Data Privacy Directive, which aims to apply European substantive law to any firm that collects personal data within the European Union, has a similar wide choice of law provision.[19] The attempt by Internet separatists to prevent local law from being enforced poses a serious threat to public order. Outside of the United States, for instance, online hate speech is often outlawed.[20] However, because the First Amendment offers constitutional protection,[21] the United States may become a refuge for people seeking to promote hate speech on the internet. The realization that internet pornography is protected by the Constitution in the United States and that data privacy is a key political right outside the United States causes similar issues.[22]

Human Rights Impact from Jurisdictional Issues

Unchecked internet reterritorialization to address abuses risks obliterating the internet's great human rights accomplishments. Measures like data localization and decryption, on the other hand, may increase rather than diminish monitoring opportunities, putting the right to privacy in jeopardy. Increased pressure on internet firms to accept direct requests might result in a 'race to the bottom', limiting free expression and undermining due process rights. The lack of inexpensive

---

18 Twentieth Century Fox Film Corp. v iCrave TV Nos. Civ.A. 00-121, Civ.A. 00-120, 2000 WL 255989, at *3 (WDPa. 2000).

19 Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 'Undisclosed Information (Trade Secrets), Copyright and Related Rights (Neighboring Rights), Other' (1995-96).

20 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Article 10.

21 R.A.V. v City of St. Paul 505 US 377, 391 (1992).

22 Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 'Undisclosed Information (Trade Secrets), Copyright and Related Rights (Neighboring Rights), Other' (1995-96).

cross-border appeal and redress channels for affected internet users, on the other hand, has a huge detrimental influence on global justice.[23]

Technical Infrastructural Impact from Jurisdictional Issues

Unbreakable encryption technology may lead to a spiral of encryption/decryption conflicts between public and private players, as internet companies try to minimize their multi-jurisdictional liability. The use of a restricted number of internet gateways to link a region in order to allow for filtering procedures may jeopardise the technical network's overall resiliency. Finally, limiting technology like virtual private networks violates Article 13(2) of the Universal Declaration of Human Rights while jeopardizing transaction and communication security.[24]

Global Perspective

The authority of a court over the persons or entities involved in a lawsuit is referred to as personal jurisdiction. One way to look about personal jurisdiction is to ask: What right does a court have to consider the rights of the parties involved in the action? In other words, deciding whether a court has personal jurisdiction over a person entails determining whether a judgement against that person would be reasonable. In order for a court to have personal jurisdiction over the parties to a case, the legislation that regulates it must provide it the ability to do so.

Indian Perspective

The Indian Parliament passed the Information Technology Act of 2000 under the Fifty-First Amendment. The legislature's principal goal in passing this bill was to acknowledge e-commerce and the expanding usage of the internet. The law was enacted to address potential legal issues that may occur as a result of the rapid growth of internet use. In the United Nations Model Law on Electronic Commerce 1996, the Indian Parliament caught the spirit of the General Assembly's proposals of 30 January 1997. (UNCITRAL Model).

---

23 Internet Principles and Rights Coalition, 'Internet Governance Principles' (Human Rights Council, 29th Sess., Agenda Item 3, UN Doc. A/HRC/29/L.35/Rev.1, 17 June 2015), https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf (access: 2.01.2022).

24 A.M. Sukumar, *The Encryption Debate in India*, *Carnegie Endowment for International Peace*, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213 (access: 2.01.2022).

 DOI: 10.7206/kp.2080-1084.641

The Model Law was based on the following principles:
1. To assist rather than regulate electronic commerce.
2. To adapt existing legal requirements.
3. To guarantee basic legal validity and increase legal clarity.

By facilitating e-commerce and e-governance in the country, the Act enhances international trade and acts as an alternative to paper-based communication and information storage. It creates a regulatory framework for the country and specifies punishments for various cybercrimes and offences.

Section 1 specifies the scope of this Act's application (2). Section 1(2) of the Information Technology Act of 2006 states:

> „(2) It applies to all of India, except as otherwise stated in this Act, and it also applies to any act or contravention committed outside of India by any person".

The statute clearly includes any crime or violation committed by a person residing outside of India. As may be seen, subsection (2) emphasizes the nation's extraterritorial jurisdictional power against the perpetrator, regardless of his nationality, domicile, status, or other considerations. To completely grasp Subsection 2, however, it must be read in connection with Section 75. Section 75 of the Information Technology Act of 2000 states that the act applies to any offence or violation committed outside India by any person, regardless of country, involving a computer, computer system, or computer network in India.[25] The Act established a Cyber Appellate Tribunal, which is stated in Section 2(1)(n), for domestic procedures and litigation. The Tribunal was established in accordance with Section 48 of the Constitution (1).

The Delhi High Court clarified India's position on the jurisdictional question in *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*. Despite the fact that neither side was domiciled within the court's regional jurisdiction, the case's most notable characteristic was that both parties' websites were accessible in Delhi. Following the Casio case, the Delhi Court changed its position and said that just having a location in Delhi was not enough to acquire a ward. According to the ruling, the offended party must prove the defendant's 'intentional ailment directed towards the discussion state', establishing that the offended party used the site with the expectation of economic exchange with the site client, resulting in harm or injury to the offended party. It has been suggested that enforcing Indian courts' jurisdiction over foreign cyber criminals would be exceedingly difficult in practice.

[25] Section 75 of the Information Technology Act of 2000.

Furthermore, 'cybercrime' is not an extraditable offence under the extradition treaties that India has ratified.

American Perspective

The realpolitik of internet regulation is the extraterritorial spread of governmental authority. To begin with, governments that have created internet platforms or technical operators can impose their national rules and regulations on these private enterprises, with clear transboundary ramifications for all international consumers of these services. The surveillance capabilities of the United States, as disclosed by the Snowden leaks, are a frequent example. In terms of law enforcement's reach, a major case is presently being litigated to see if US authorities have the jurisdiction to access emails held in Microsoft's Irish data centres. The US Department of Homeland Security has already confiscated domain names registered by foreign registrants solely because they were registered through a US-based registrar or registry (the RojaDirecta case) (the Bodog case). Future law, such as the UK Investigatory Powers Bill or the European Union's General Data Protection Regulation, is increasingly embracing extraterritorial measures.

Finally, litigation is critical in creating new global standards, which have far-reaching consequences that extend beyond the countries concerned. Following a US court judgement on its 'sponsored stories' feature, Facebook, for example, modified its worldwide terms of service. Courts are increasingly establishing competence over services developed in other nations merely because they are available in their jurisdiction, as seen by the recent Yahoo case in Belgium. Implementing the resulting choices might be difficult, as the national ban on WhatsApp in Brazil demonstrated. Local occurrences, on the other hand, might have far-reaching consequences. The French data protection authorities requested that Google expand its de-indexing to all versions of its search engine, saying that the service is based on a single global data processing, following the Court of Justice of the European Union's Costeja judgement (the right to be de-indexed). The case *International Shoe Co. v. Washington* was one of the first to establish the 'Minimum Contact Test', which eventually established the standard for assessing internet jurisdiction across the world. Despite the fact that International Shoe did not claim any land or a permanent location in Washington in this lawsuit, the aggrieved party earned around $30,000 per year from Washington residents. Participating organisations were charged a fee as a required payment to the state's Unemployment Compensation Fund, which was allegedly allocated to the Plaintiff. The US Court of Appeals decided that the court might have jurisdiction over non-resident respondents if

 DOI: 10.7206/kp.2080-1084.641

the suit's maintenance did not violate traditional notions of fair play and generous equity.[26]

Local court decisions might possibly create new global rules for how countries and internet companies interact. For instance, the right to be de-indexed was initially developed by Europe for Google and is now utilized by other search engines such as Microsoft Bing or Yahoo Search, with implications in Asia and Latin America.

European Perspective

The General Data Protection Regulation (GDPR) is the world's most comprehensive data privacy and security regulation. It imposes duties on any firms who target or collect data on EU people, despite the fact that it was created and administered by the European Union (EU). On 25 May 2018, the regulation went into force. Those that break the GDPR's privacy and security standards will face harsh penalties ranging from millions to billions of euros in fines. Even if data is maintained or used outside of the EU, the GDPR applies to businesses based in the EU.

Article 3(1) of the GDPR applies to:

> the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union or not.

In determining whether processing of personal data comes under Article 3(1), the EDPB Guidelines propose using the following approach:

1. It is decided whether or not there is a presence in the European Economic Area ('EEA'). The European Union's Court of Justice (CJEU) looked at the concept of *establishment*, determining that the word should be defined broadly. It comes to the conclusion that 'any genuine and effective activity – no matter how minor' carried out in the EEA through 'stable arrangements' may be enough to qualify as an establishment under European data protection legislation.[27]
2. Examines whether processing occurs 'in the context of' an establishment's activities (that is, is processing inextricably related to the acts of the controller or processor). When tying processing by a controller or processor outside the EEA to the activities of an establishment inside the EEA, the courts have frequently taken a wide interpretation, which is known as the *inextricable*

[26] International Shoe Co. v Washington 326 US 310 (1945).

[27] Weltimmo v NAIH (C-230/14).

connection. Organizations with sales offices in the EEA, as well as those who promote or sell advertising or marketing to EEA residents, are examples cited by the CJEU.

3. Regardless of whether the processing takes place in the EEA or not, the GDPR applies to the formation of a controller or processor within the EEA. The formation of a controller or processor in the EU, as well as processing carried out in the context of such an establishment, according to the EDPB Guidelines, triggers the GDPR's application. As a result, whether or not the actual processing activity takes place in the EU has no bearing on the GDPR requirements.[28]

Under Article 3(2) the GDPR applies to:

> the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

According to the EDPB Guidelines, there are two approaches to analysing the requirements for applying the criteria:

1. Whether the processing is related to the provision of goods or services or the monitoring of data subjects' behaviour in the European Economic Area (EEA).
2. Whether it is for the provision of goods or services, or for the monitoring of data subjects' behaviour in the European Economic Area.

The EDPB Guidelines stress the necessity of 'targeting' persons in the EEA, stating that services must be provided with the goal of targeting individuals in the EEA; delivering services to someone who happens to be in the EEA by chance is inadequate. The data subject does not, however, have to pay to activate the targeting criterion. As a result, the GDPR will undoubtedly have far-reaching implications outside of the EU.

[28] Google Spain SL v Agencia Española de Protección de Datos and Mario Costeja González [2014] C-131/12 [60].

 DOI: 10.7206/kp.2080-1084.641

Convention of Cyber Crimes

As previously said, when it comes to cybercrime, different nations have distinct laws that control them. Different techniques employed around the world to tackle international crimes are ineffectual. As a result, in Budapest in 2001, the Council of Europe and some non-member countries adopted the Convention on Cybercrime, a new attempt to settle this jurisdictional challenge was made. In 1949, the Council of Europe was founded with the goal of promoting human rights, democracy, and the rule of law throughout Europe. It is not a member of the European Union's apparatus. Non-member signatories to the convention include the United States and Canada, both of which have ratified it.

In 2001, the European Council passed the Cybercrime Convention, which took effect in 2004. It is the first and only international treaty to address violations of the law on the internet and other information technology-related offences. The convention aims to protect the confidentiality, integrity, and availability of computer systems, networks, and data, as well as to prevent their misuse. Because numerous large countries across the world are signatories of this convention, and it is the sole convention on cybercrime, India should ratify it because it is the closest thing to a legal framework that might be deemed a global standard. Russia, China, and India, on the other hand, are not signatories to the treaty, since it jeopardizes countries' total sovereignty. Russia has stated that this is the basis for their refusal to join the pact and has stated that it would not cooperate with any law enforcement investigations into cyber crime.

Suggestions

1. **Harmonization of International Laws:** It is strongly recommended that states engage in diplomatic negotiations and enter into conventions or treaties with the aim of harmonizing and standardizing international legal frameworks governing issues of internet jurisdiction. These instruments should delineate uniform principles and protocols, consistent with established international law, to guide the resolution of transnational jurisdictional conflicts arising in the context of cyberspace.
2. **Transparency and Accountability:** Emphasis on the critical imperative of transparency and accountability within the sphere of internet governance. Governments and digital platforms are urged to maintain transparency with regard to their content moderation policies, data access procedures, and mechanisms for upholding the rights of users. It is further advisable to promulgate

legal frameworks and accountability mechanisms to ensure compliance with international legal norms and standards.

3. **Establishing a Global Compliance Imperative:** Contemplation should be given to the institution of a global compliance mandate, either through legislative enactments or judicial discretion, aimed at standardizing legal expectations within the digital milieu. This stratagem would engender awareness and facilitate reasonable adherence to the legal regimes of foreign jurisdictions.
4. **Mitigating Complexities in Expanding Personal Jurisdiction:** The endeavour to broaden personal jurisdiction and the ambit of applicable law in the realm of cyberspace cannot be devoid of the concomitant challenges relating to legal certainty. Acknowledgment is due to the formidable difficulties inherent in orchestrating a harmonized international initiative in this regard.
5. **Deterring Litigious Exploitation:** Robust measures must be instituted to deter vexatious litigation strategies employed in far-flung jurisdictions with the intent of securing default judgments against defendants, who, due to geographical constraints, are unable to mount a robust defence. This imperative assumes pronounced significance, particularly in the realm of online defamation cases.
6. **Contemplating Ramifications for Internet Service Providers (ISPs):** The proposition to broaden the liability exposure of internet service providers (ISPs) holds the potential to compel these entities to reassess their service provision in select jurisdictions, as a strategic response to attenuate legal risks. Such deliberations could, in turn, impinge upon the accessibility of online services in specific geographic domains.

Concluding Remarks

The jurisdictional difficulty of internet governance has a direct influence on other policy challenges, in addition to involving a variety of diverse parties. These include the growth of global digital economies, the formation of clear and predictable legal frameworks, the safeguarding of fundamental human rights, and the upkeep of cybersecurity and public order, among other things. Many players and sectors must actively participate in order to address jurisdictional disputes online and prevent fragmentation of the internet.

Any of the present techniques of dealing with jurisdiction are based on country cooperation. The issue in all of these is that they are all largely reliant on country collaboration. As a result, the authors of this article propose the establishment of a distinct dispute resolution agency that specializes on cyber offences. The parties that approach this body should be bound by its judgment. The UNCITRAL regulations

 DOI: 10.7206/kp.2080-1084.641

should serve as a guidance for the dispute settlement process. In order to find a permanent solution to the challenges of jurisdiction and international collaboration, it is important to build a powerful body similar to the World Trade Organization. The UNCITRAL laws, in combination with the requirements of the Cybercrime Convention, should offer a good framework for the establishment of such an organization.

Even if the current state of knowledge and understanding of cyberspace and related legal issues precludes the development of a detailed law on the subject of jurisdiction, an international monitoring or regulatory body with binding authority could be tasked with reviewing the rules of cyber jurisdiction for aspects on which no agreement can be reached. In the same way as UNCITRAL proposes and adopts specific model laws for states to base their domestic legislation on, a body like this might propose and adopt specific model laws for states to base their domestic legislation on. Furthermore, some parts may need to be addressed by domestic courts since unexpected issues may occur only in a true factual setting, forcing courts to arbitrate on the parties' legitimate interests.

To summarise, the internet is large, sophisticated, and inexorably expanding. Our conventional legal systems have completely collapsed in the face of technological advancements. Rather than altering our present practices and seeking to devise a new and innovative method, we should all compromise a bit and use the resulting compromise to advance justice and fairness. To back to our original point, the government has pushed citizens to use the internet by making all of the government's tools and data readily available online. As forward-thinking and inventive as this notion is, it also has the potential to be hazardous and a source of increased cyber crime. While this is a positive step toward more openness and democracy, it also encourages and aids cyber-terrorism. Several new cyber crimes may surface, demanding immediate action; at that point, questions about jurisdiction would just postpone the process and aggravate the issue. The jurisdictional dilemma of cybercrime law would continue to jeopardize state sovereignty if technologically advanced countries like India fail to build an appropriate legal framework.

Bibliography

Annan K., *Internet Governance*, speech at the opening session of the Global Forum on Internet Governance in New York, 2004, https://www.un.org/sg/en/content/sg/statement/2004-03-25/secretary-generals-remarks-opening-session-global-forum-internet (access: 2.01.2022).

Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 'Undisclosed Information (Trade Secrets), Copyright and Related Rights (Neighboring Rights), Other' (1995-96).

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR), Article 10.

Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 'Undisclosed Information (Trade Secrets), Copyright and Related Rights (Neighbouring Rights), Other' (1995–1996).

Geist M.A., *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, "Berkeley Technology Law Journal" 2001, 16. https://doi.org/10.2139/ssrn.266932.

Janis M.W., *An Introduction to International Law*, 4th edition, Aspen, New York 2003.

Vakil Y., *Jurisdictional Challenges – Cyber Crime Prosecutions*, 1st edition, India, 2005.

Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Article 1(1).

Jurisdiction: An Issue on Internet, *LawBhoomi*, https://lawbhoomi.com/jurisdiction-an--issue-on-internet/ (access: 2.01.2022).

Sukumar A.M., *The Encryption Debate in India*, *Carnegie Endowment for International Peace*, 30 May 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-india-pub-79213 (access: 2.01.2022).

The Impact of the Internet on Society: A Global Perspective, in Change: 19 Key Essays on How the Internet Is Changing Our Lives (BBVA OpenMind) (2022).

 DOI: 10.7206/kp.2080-1084.641