National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

REGULATION OF CYBER SPACE AND THE NEED OF A GLOBAL CYBER FORUM

MR. VIVEK KUMAR

PhD Research Scholar, Department of Laws Guru Nanak Dev University, Amritsar, Punjab

ABSTRACT

The Internet has grown at an exponential rate in recent years, particularly in e-commerce and retail, thereby transforming the way the world lives. The Internet, which was originally largely utilized for commercial purposes, is now an essential component of people's daily life. This quick growth has increased the possibility of online conflicts and posed previously neglected enforcement issues. Millions of transactions are completed online every second throughout the world. Nothing could be easier than an online transaction if it does not meet any difficulties. When a disagreement emerges, the first question is where the conflict may be resolved, or which courts are competent to hear and judge the dispute. When it comes to governing cyberspace, territoriality, or the lack thereof, is without a doubt the most challenging legal challenge. Every computer, however, is hardwired to the earth, allowing nation-states to create and enforce laws. As a result, jurisdictional ideas based on the connection of a computer, computer system, or resource that is either the source or the recipient of electronic communications have emerged in courts across the world. On the surface, the problem of jurisdiction appears straightforward, yet it is one of the most challenging issues faced by any sector of law enforcement. This article focuses on the challenges surrounding cyberspace regulation and the necessity for a supranational cyber framework.

Key words: Global cyber forum, Cyber security, Cyber terrorism, Dark web, Cyber warfare, Cyber collectivism, Cyber libertarianism, Cyber anarchy, Cyber regulations.

INTRODUCTION

The Internet has given rise to a new kingdom without boundaries. The world as we know it has permanently altered. Despite the fact that innovation and the resulting changes in our lifestyles are accelerating, the law continues to stumble through the Internet maze. The absence of borders has created enormous chances for development and advancement, but it has also unleashed an uncontrolled dark side that fights against any form of limitation. Attempts to regulate the field are met with vehement opposition that far outnumbers physical revolutions for liberty. Cyber liberals are prepared to give up full freedom of expression, openness, and privacy in exchange for abuse of the Internet and illicit behavior in its shadowy or secret corridors.

The Internet's early development was organic and self-regulating. Recent discussions have centered on the idea of harnessing the Internet through laws that, of course, are related to actual geographical limits. Most Western nations have taken precautions against laws that encourage heavy control, and there is widespread support for keeping the Internet's current neutral attitude. Divisions in cyberspace are formed

National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

along artificial shadow lines, just as they are in the air or space. Applying traditional jurisdictional principles to this seamless domain is thus intrinsically difficult.

THE "JURISDICTIONAL FACT" PROBLEM IN CYBERSPACE

A "jurisdictional fact" is required for a judicial body to act. A jurisdictional fact is one that establishes whether a court, tribunal, or other body has jurisdiction over a certain subject. It is defined as "a fact that must exist before a court may properly assume jurisdiction over a case" by Black's Law Dictionary. The challenge of deciding which legislative body has suzerainty over the invisible and all-pervasive Internet, or how states would split cyberspace for implementation and control, exists in cyberspace. The next obstacle would be the enforcement of national laws in the seamless cyber realm, which would necessitate mutual recognition of international laws and collaboration in their execution. Although there are no physical boundaries in cyberspace, notional lines define each nation's political and legal control over regions of this virtual world. It is vital to understand how far the long arm of one nation's laws may reach without encroaching on the sovereign rights of another.

In Dow Jones & Co., Inc. vs Gutnic, the High Court of Australia quickly characterized the qualities of the Internet as "ubiquitous, global, and helpful," and stated that because of these features, any issue involving the Internet is susceptible to international jurisdiction. The judgment of the Australian Supreme Court extends to all jurisdictions touched by the Internet, which is, of course, the vast majority of the globe. It further decided that because of the "ubiquity," "universality," and "utility" of its services, any action connected to the Internet and the World Wide Web is susceptible to international jurisdiction.

However, punishing a person according to the laws of all nations, rather than only the rules of the area where he or she is physically present or committed the conduct, would not only be unfair, but would also constitute an infringement on the authority of another sovereign nation. As a result, regardless of how ubiquitous or universal the Internet is, it is critical that a person or organization not be drawn to every location on the planet where a website or web page may be visited. Before considering a case, a court must first assess whether it has jurisdiction over that matter. Jurisdiction is crucial in the physical legal world, yet traditional jurisdictional rules cannot solve the challenges of the Internet. As a result, it may be argued that national laws are ineffective in governing cyberspace. The Court stated in "Blumenthal v. Drudge" that "the internet is truly nowhere and everywhere." "No one state may adopt legislation to govern an area that is not controlled by them."

National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

Many individuals all across the world are calling for a rule-free cyberspace. They contend that the legal system of cyberspace should reflect the community's ethical concerns rather than the coercive authority that defines governance in actual space. This theory is referred to as "cyber-libertarianism" or "techno-libertarianism," and its followers are known as "techno libertarians." It is a political theory that thinks that cyberspace should be free of government regulation, that individuals should have freedom in cyberspace, and that civil rights should be prioritized and respected.

CYBER COLLECTIVISM AND CYBER LIBERTARIANISM

According to cyber-libertarianism, every individual, whether a citizen, client, corporation, or collective, should have the right to follow their own preferences and interests online. "Live and let live" and "Hands off the Internet" are techno-mottos. Libertarianism's A techno-libertarian prefers voluntary solutions and agreements based on mutual consent over government compulsion in social and economic challenges. Cyber-collectivism is the polar opposite of cyber-libertarianism. The idea that cyber-related choices should be made by the state or an elite class based on an amorphous "general will" or "public interest" is referred to as "cyber-collectivism." The work of cyber-collectivists frequently shows the distant influence of Plato, Rousseau, and Marx.

"John Perry Barlow" was a well-known "techno-libertarian" who was not only a talented poet and writer but also a staunch supporter of techno-libertarianism. In his articles, he described the Internet's wonder as an "electronic frontier." Barlow and digital rights activists John Gilmore and Mitch Kapor co-founded the Electronic Frontier Foundation (EFF) in 1990. The EFF considered the bill a danger to cyberspace's freedom and sovereignty. The EFF was formed to resolve "inevitable disputes that develop at the boundary between cyberspace and the physical world."

He intended to construct a legal barrier that would isolate and safeguard the Internet from territorial governments, notably the United States government. He thought that cyberspace would be governed by ethics, enlightened self-interest, and the common good. His notable article, "A Declaration of the Independence of Cyberspace," released in 1996, was written in response to the United States' enactment of the Telecommunications Act of 1996. In it, he argued that the United States lacked the jurisdiction to apply laws to the Internet and that the Internet existed outside of any country's boundaries.

Instead, he claims that the Internet is creating its own social contracts to determine how it will govern its problems in accordance with the golden rule. This release

National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

includes the following excerpt: "I come from cyberspace, the new home of the mind, to the governments of the industrial world; you weary giants of flesh and steel. In the name of the future, I request that you leave us alone. You have no place here. You have no authority where we congregate."

However, many who point out that the Internet is always tied to its underlying geography contradict the premise in the phrase that "cyberspace" is a location isolated from the real world. The premise that morals and ethics should regulate cyberspace is also open to challenge. Cyberspace cannot be separated into multiple nations; it is a single region, yet the globe has no one morality or ethics. What is perfectly decent in one location may be absolutely unethical in another. It may be absolutely moral in one area of the globe to watch adult movies, but it may be completely unethical in another part of the world.

As a result, governing cyberspace with morals and ethics is challenging. Thus, in order to safeguard society from the detrimental consequences of cyberspace, it is important that there be certain rules and regulations that assist prevent this use of the Internet for immoral and unethical acts. Regulating cyberspace, on the other hand, is not as straightforward as it seems. "While these electronic connections wreak havoc on geographic borders, a new barrier forms, made up of the screens and passwords that divide the virtual world from the physical world of atoms," Johnson and Post write. This new barrier establishes a unique cyberspace that requires and can build new legal institutions of its own. This new environment poses a significant challenge to territorially based lawmaking and law enforcement."

There is currently no broad comprehensive United Nations convention or treaty controlling cyberspace.

There are other conventions, such as the "Council of Europe's" "Convention on Cybercrime," also known as the "Budapest Convention on Cybercrime" or "Budapest Convention," which was drafted. It is the first worldwide convention to combat cybercrime by unifying national laws, strengthening investigation procedures, and promoting collaboration between governments. However, it should be emphasized that it was signed in 2004, but only 65 states have ratified it thus far. India has refused to sign it since it purportedly infringes on its sovereignty, and it was not made a party to the pact when it was drafted. Russia has not approved it either.

The United Nations General Assembly decided in Resolution 74/247 to form an ad hoc intergovernmental committee of experts with open participation from all regions to develop a comprehensive international convention on combating the use of

National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

information and communication technologies for criminal purposes, taking into account existing international instruments and efforts at the national, regional, and international levels to combat the use of information and communication technologies.

THEORY OF BROKEN WINDOW

According to the "broken windows hypothesis," chaos and crime are intimately linked, and if one window in a structure is broken, the other windows are likely to be damaged as well. According to this argument, the outcome would be the same in both attractive and dilapidated neighborhoods. This argument is predicated on the premise that leaving one window unfixed demonstrates "no one cares" and therefore that further vandalism would be free. This issue arises in the digital domain as well.

Lawlessness is thought to be natural in the absence of effective enforcement. The inherent issues of the Internet's lack of sovereign rights, the difficulty of territorially bound nation-states regulating the borderless Internet, and the costly and time-consuming procedures and processes for international enforcement all result in large gaps in the space. The wanton criminal feels that the long arm of the law cannot reach far enough or quickly enough for him, leaving the edicts of individual nation-states useless and flaccid. The only way to fix cyberspace's shattered windows may be to establish a multi-stakeholder international body that may go from tiny steps in Internet regulation to greater ones once it has received universal support.

States have acknowledged the necessity for a long-term regulatory framework as well as a worldwide accord to restrict the Internet, which remains ungoverned. The "Budapest Convention" and NATO's "Tallinn Manual" are two failed attempts to create soft rules or guide manuals. However, numerous nations have expressed displeasure and dispute over enacting such soft laws, which they regard as a Western agenda with clear U.S. influence. Ratification of international agreements, soft laws, or policy papers is most often resisted or rejected in criminal and penal legislation.

Despite an abundance of factual facts demonstrating the necessity for a supranational organization without borders, nation-states' unwillingness to renounce their sovereign ability to adopt or enforce criminal laws contradicts logic. It seems to be the product of a blend of political whim and suspicion.

GLOBAL FORUM

The notion of a supranational solution is not new or untested. Organizations such as the United Nations and the Internet Corporation for Assigned Names and Numbers (ICANN) have shown that nation-states are capable of giving up some of their

sovereign powers for the common good, and that such organizations are effective within the scope of the powers delegated to them. The cyber domain relished its touch with the uncontrolled sector, as any young person might, and acted recklessly. However, the virtual anarchy that fit the Internet's early days is no longer an option. The Internet has matured and now requires a period of planned and regulated development in order to attain its full potential. However, regulation does not imply suffocating the Internet or the liberties that individuals have enjoyed on the Internet. as well as the. Despite legislation, the requirements of "cyber-libertarians" can be satisfied as long as it is not restrictive.

Although the cyber-libertarian stance is correct that no one government has power over the Internet, this does not imply lawlessness or "cyber-anarchy." Because computers are based in physical domains, the laws of the country have and will continue to stretch their long arms into the cyber world, albeit with practical boundaries. In such circumstances, civil enforcement is more effective than criminal prosecution. The downfall of the infamous "Silk Road" on the dark web shows the need of internationalism among nation-states in efficiently enforcing criminal laws. This narco-paradise is no longer in existence. Not long ago, the Silk Road was not just a booming black market for drugs, but also the living incarnation of every crypto-dream: anarchist's a safe trading space on the Internet that neither government regulations nor the drug war sparked by the triggering of the triggering could reach. This narco-paradise is no longer in existence.

Disruptive technologies involve disturbing the long-term growth of legislation. As a result, perhaps it is time to loosen the bonds of territoriality and sovereignty by committing Internet legislation and regulation to a supranational agency. This is not to say that every sovereign state should delegate all of its authority to a non-sovereign entity. It merely necessitates a methodical and restricted transfer to the level required for world peace. Nation-states may re-launch negotiations to establish a non-governmental organization based on reciprocity and universal participation.

This might be an existing organization, such as the United States, or a new institution with a comparable framework and adequate representation from all participating member nations. To avoid cyber-attacks successfully, the finest existing models or soft laws, declarations, and standards, such as the Budapest Convention, the Tallinn Manual, and the Code of Conduct for Information Security, may be updated. As previously indicated, the non-sovereign may be given UN-like powers, with legislative authority restricted to the drafting of "soft laws" and enforcement carried out by an efficient executive branch and a substantial judicial body.

National Journal of Commerce and Management (NJCM)
Peer-Reviewed/Refereed Journal
ISSN 2394-6342 (online)
Volume 09, Issue 02, December 2022
http://njcm.pratibha-spandan.org

CONCLUSION

History has repeatedly demonstrated the need of nation-state collaboration and coherence in times of conflict and peace. Great peacekeeping endeavors have evolved after big and horrific interruptions of the peace. The formation of the League of States and the United Nations in the aftermath of World Wars I and II required member nations to give up sovereign powers in favor of a common denominator. The prospect of world peace prompted their initiatives. Despite the fact that politics hampered the UN's efficacy, the organization's foundation was a huge success.

The necessity for a supranational cyber forum is evident since cyber war is a genuine possibility, and everyday criminality serves as a continual reminder of the absence of an efficient global enforcement agency. The absence of prosecution for some of the greatest cyber assaults in recent years is especially noteworthy. The absence of a worldwide platform for filing complaints against nation-states may be the sole reason for the lack of enforcement.

REFERENCES

NS Nappinai, Technology Laws Decoded, (LexisNexis, 27 March 2017)

Talat Fatima, Cyber Law in India, (Kluwer Law International, February 2017)

Prakash Prasad, a Brief Introduction on Cyber Crime Cases, (Creative Space Publishing, July 2017)

William Magnuson, Blockchain Democracy: Technology, Law and the Rule of the Crowd, (Cambridge University Press, 2 January 2020)

Gary E. Marchant, Braden R. Allenby, and Joseph R. Herkert, The Growing Gap between Emerging Technologies and Legal-Ethical Oversight, (Springer; 2011th edition, May 2011)

Jane E. Fountain, Building the Virtual State: Information Technology and Institutional Change, (Brookings Institution Press; Illustrated edition, August 2001)