Page 865 - 877 **DOI:** *https://doij.org/10.10000/IJLMH.112905*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 5 | Issue 2

2022

Anonymity in the Borderless Phenomenon: A Revisit to Regulatory Models of Cyberspace

REVTI RANI ROY[1]

ABSTRACT

Virtual space, commonly called cyberspace is often regarded as a borderless phenomenon- one which is limitless and boundless. Cyberspace, therefore, has often been compared with an unruly horse. In this world, there exist two separate worlds- one that exists in reality and the other that exists in virtual reality. Cyber World is a very novel phenomenon, emerging in the last two decades that has expanded its roots everywhere, crossing boundaries. No wonder it is said that in cyberspace, no one is the sovereign and everyone is the master. It is the other World where anonymity becomes a shield and a sword for users and it is for this reason that it cannot be left unfettered and there arises a need for regulating people's behaviour in the Other World. Therefore, this research paper discusses the risks that cyberspace poses to the users and the need for regulatory frameworks. The paper discusses the various models of regulation of cyberspace and the researcher has proposed a multi-modal approach to the regulatory framework in line with the current requirements.

Keywords: *Sovereign-omnipotent space, Anonymity, Regulatory models, Code, Multi-modal framework.*

I. INTRODUCTION

"Cyberspace is that place where individuals are, inherently, free from the control of real space sovereigns."

This assertion has been proven to be ambiguous and incorrect, as governments and state actors in the actual world are more than capable of managing the affairs of cyberspace. In his 1996 manifesto, *"A Declaration of the Independence of Cyberspace,"* John Perry Barlow contended that cyberspace was fundamentally un-regulable, that its technological foundations defied territorial bounds and so rendered law enforcement based on a physical monopoly of violence ineffective. Various proponents of the idea that internet control is a feasible and practical

[1] Author is a LL.M. student at Chanakya National Law University, India.

 [ISSN 2581-5369]

option, however, have slammed him for his beliefs. As a result, the study project will focus on the necessity for cyberspace regulation, based on the assumption that *"The biggest strength of cyberspace is its biggest weakness!"*

In this study, I've largely focused on the fundamental character of cyberspace, which makes it a contentious topic in terms of regulatory possibilities. It has been discussed how, although being a borderless phenomenon, cyberspace may still be controlled and managed by a variety of elements with the help of both state and non-state actors. Following that, cyberspace has been linked to the limits that govern it, just as they do in actual space. Different regulatory models have been advanced in this field.

The researcher has recommended a multi-modal approach to the regulatory framework in the field of cyberspace as a result of this research work's focus on cybersecurity. The threat of cybercrime extends across disciplines, industries, and approaches. Understanding how the government should intervene to ensure the resilience of its cyberspace and prevent harm to enterprises' continuity and national security has many facets and exposes competing interests and forces. In this vein, the researcher has attempted to examine the 'Freedom vs. Regulation' issue from the perspective of the online landscape. Though cyberspace regulations may appear to be a threat to individual liberty and freedom, if implemented wisely, they may prove to be helpful to the cyberspace regime and the threats that it may expose mankind to if left unregulated. The Multi-Modal Approach to Regulatory Framework has been developed in this regard. Under the premises laid above, the researcher seeks to begin the theory of this research paper.

II. FUNDAMENTAL AMBIGUITY IN THE SELF-PROCLAIMED SOVEREIGN SPACE

"Understanding cyberspace as a separate space is often a utopia."

(A) Cyberspace: Not An Independent, Autonomous Space Free From Regulation

In 1996, John Perry Barlow published his *'cyberspace manifesto,'*[2] contending that cyberspace was fundamentally uncontrollable, that its technological basis defied territorial bounds and hence rendered law enforcement based on a physical monopoly of violence ineffective. In a similar vein, David R Johnson and David B Post published their famous book in 1996. *'Law and Borders- The Rise of Law in Cyberspace,'*[3] claims that cyberspace is a distinct, separate

[2] JOHN PERRY BARLOW, A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE, in *Duke Law and Technology Review* 18, 5-7 (1996).
[3] David R. Johnson & David B. Post, *Law and Borders: The Rise of Law in Cyberspace,* 48 Stan L. R. 1367, (1996).

space devoid of physical boundaries and territorial authority. They explain that cyberspace is not a physical space and thus does not fall under the control of sovereigns whose control is limited to whoever and whatever remains within their territory; they go on to say that the assumption that the effects of any particular behaviour are limited by physical proximity does not hold true in cyberspace. Following this upbeat mood, *Castells* predicted the collapse of the nation-state, which is still built on mutually exclusive jurisdictions, implying that territorial governments are dinosaurs in the expanding network society.[4]

Reilly Jones critiques Barlow's use of terms like "*global social space*" and *"Social Contract,"* claiming that they reveal an all-too-familiar sympathy with the kinds of *"universal rights"* that have left a bloody trail from the French Revolution to the Cold War. He continues by claiming that Barlow's "Declaration" includes a latent intellectual malignancy that could pave the way for universal tyranny. Expressions of political universalism, a recurring utopian yearning that has only resulted in misery, are the source of this disease.[5]

Lawrence Lessig argues out that: *"This is the age of the cyber-libertarian. It is a time when certain hype about cyberspace has caught on. The hype goes like this: Cyberspace is unavoidable, and yet cyberspace is un-regulable. No nation can live without it, yet no nation will be able to control behaviour in it. Cyberspace is that place where individuals are, inherently, free from the control of real space sovereigns."* However, he further refutes this notion by saying:

"In my view, the world we are entering is not a world of perpetual freedom; or more precisely, the world we are entering is not a world where freedom is assured. Cyberspace has the potential to be the most fully, and extensively, regulated space that we have ever known anywhere, at any time in our history. It has the potential to be the antithesis of a space of freedom."[6]

Referring to *Foucault's* term *'heterotopia*[7]*,*' *Julie Cohen* defines cyberspaces as real spaces in which ordinary rules of behaviour can be suspended or transformed in comparison to ordinary spaces, emphasizing the relationship between cyberspace and ordinary spaces, as well as "the embodied spatiality of cyberspace users, who are situated in both spaces at the same time."[8] She further remarks that *"utopian theories of cyberspace as an entirely separated space fail not because of their un-regulability but because of the untenable presumption of experiential*

[4] MANUEL CASTELLS, THE RISE OF THE NETWORK SOCIETY (Oxford: Blackwell, 1996).
[5] REILLY JONES, A CRITIQUE OF BARLOW'S "A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE",(1996).
[6] LAWRENCE LESSIG, THE LAWS OF CYBERSPACE, Draft: April 3, 1998.
[7] MICHEL FOUCAULT, OF OTHER SPACES 22 (1986).
[8] Julie E Cohen, *Cyberspace as/and Space* (107 Columbia Law Rev 210, 213-217) (2007).

separateness."[9] In this way, she goes one radical step further than Lessig[10] and Reidenberg, who, according to Cohen, proved that cyberspace's unpredictability and un-regulability is neither a permanent nor a technologically necessary element.

(B) Cyberspace: a borderless phenomenon or a manifestation of regulated machinery of the human mind

Because of its ostensible lack of borders, the concept of cyberspace as a *global commons* is better viewed as an aspiration rather than a depiction. This approach jeopardizes national and international security and is becoming increasingly unsustainable. It wasn't just that the government wouldn't regulate cyberspace; it was also that the government couldn't regulate it. By its very nature, cyberspace was inherently free from any constraints. Governments could threaten, but they wouldn't be able to control behaviour in cyberspace; laws could be made, but they wouldn't be effective. Cyberspace would be a society unlike any other. There would be definition and direction, but it would be developed from the ground up. The society in this space would be completely self-governing, free of governors and political hacks. .[11] James Boyle[12] would later call it the "libertarian gotcha": no government could survive without the Internet's riches, yet no government could control the life that went on there.[13]

As a result, while cyberspace can be considered a borderless phenomenon, it cannot be so in the context of cyberspace regulation's incapacity; rather, it is a manifestation of the human mind's regulated machinery, which human mind controls by making laws, codes, and architectures to limit its magnanimous giant wings!

(C) Absence of Geographical Boundaries and the Problem of Anonymity

There is no actual relationship between cyberspace and real space. It is impossible to separate it along physical lines. The internet has no link to the physical world beyond the 'backbones' of cables, telephone lines, satellites, and computers. Away from these backbones, the Internet generates its own universe, based on passwords and electronic data. Criminals can conduct a crime in cyberspace and have it have an impact in the real world for a lower cost and with fewer resources.[14]

---

[9] Kevin Hetherrington, THE BADLANDS OF MODERNITY: HETEROPIA AND SOCIAL ORDERING, 20-38 (London: Routledge, 1997).
[10] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (New York: Basic, 1999).
[11] Lawrence Lessig, 'Code And Other Laws of Cyberspace'(2006) Basic Books Publications.
[12] James Boyle, *"Foucault in Cyberspace: Surveillance, Sovereignty, And Hardwired Censors."* (1997) University Of Cincinnati Law Review Vol. 66.
[13] JAN VAN DIJK, THE NETWORK SOCIETY: SOCIAL ASPECTS OF NEW MEDIA, (2nd ed. London: Sage 2006).
[14] KRISHNA KUMAR, CYBER LAWS-INTELLECTUAL PROPERTY AND E-COMMERCE SECURITY, 21 (Dominant Publishers And Distributors, New Delhi 2001).

"While the Internet and other information technologies are bringing enormous benefits to society, they also provide new opportunities for criminal behaviour"

-Former U.S. Attorney General Janet Reno, Jan. 10, 2000.

On the Internet, the sender of information cannot necessarily be presumed to be who he or she is.[15] It is also not always easy for the sender to determine the genuine identity of the recipient. With the help of a cartoon that ran in the New Yorker Magazine, *Graham Greenleaf* explained the difficulty of anonymity on the internet. Two dogs sit in front of a computer in this cartoon. *"On the internet, no one knows you're a dog,"* one dog says to the other.[16] This interesting cartoon shows the difficulties in bringing Internet activities within the clasp of the present legal system. So it has been rightly pointed out that "a user's digital identity has no connection with his physical world identity!"[17]

In other circumstances, the doubt about one's identity is unproblematic. When negotiations have legal and financial ramifications, however, a party cannot be satisfied with just an e-mail address as proof of the other party's identity.[18] The existing identification tools become a failure here. As it is aptly observed that technology is creating new areas in law.[19]

Elizabeth Longworth, says that *"the ability to impose sanction on law violator is fundamentally constrained by the need of physical proximity and physical control."*[20]

"While these electronic connections wreak havoc with geographic boundaries, a new boundary forms, made up of the screens and passwords that separate the virtual world from the real world of atoms", *Johnson* and *Post* write. This new line demarcates unique cyberspace that requires and can build its own legal institutions. This new environment poses a serious challenge to territorial law-making and enforcement.[21]

Because there are no physical boundaries in cyberspace, the foundations of morality and culture in a society may be shattered. A society's morals may differ from those of another society. As a worldwide communication medium, the Internet has the potential to intrude on a society's morality. The publication of indecent materials on the Internet is one example. The sale of

[15] DON GOSSELIN, JAVA SCRIPT, 406 (Vikas Publishing House, Delhi 2000).
[16] GRAHAM GREENLEAF, AN ENDNOTE ON REGULATING CYBERSPACE: ARCHITECTURE VS LAW, at 594 (UNSW Law Journal, Volume 21(2)), https://www.unswlawjournal.unsw.edu.au/wp-content/uploads/2017/09/21-2-5.pdf.
[17] CHRISTOPHER REED, INTERNET LAW: TEXT AND MATERIALS, 118 (Butterworths, London (2000).
[18] Neal Kumar Katyal, *Criminal Law in Cyber-space*, 149 (University of Pennsylvania Law Review 2001).
[19] HUGH A. CANNELL, "THE CONVERGENCE OF TECHNOLOGY AND THE LAW," 4 (University of New Brunswick Law Journal 301) (1999).
[20] Elizabeth Longworth, *The Possibilities for a Legal Framework for Cyberspace—Including a New Zealand Perspective*, in THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW, 15 (Ashgate 2000).
[21] *Supra* Note 3, at 1368 (1996).

obscene materials is prohibited under Indian law.[22] People of all ages may now access and download filthy materials, thanks to the Internet. Even if the exact address of the host website is established, an Indian court cannot prosecute criminals who are located outside of India. Publication of obscene materials may not be illegal in the nation where the host website's server is located. Therefore, it may be noticed that because of the Internet's unique qualities, the problem is significantly more problematic for legal systems, particularly when it comes to jurisdictional issues.[23]

(D) Need for regulations in the sovereign-omnipotent cyberspace: An Irony

"The biggest strength of cyberspace is its biggest weakness!"

Libertarians strongly oppose the government's use of law and regulation to intervene in the development of cyberspace.[24] There have been arguments advocating that cyberspace should not be regulated and that any control in the form of regulation would stifle an unfettered potential for growth.[25] *Judge Easterbrook* is of the clear view that developing sound laws and applying them to cyberspace to makes sense. Cyberspace requires no new laws, for *cyberspace is a sovereign-omnipotent space*.[26] Property in cyberspace, for example, can be effectively analyzed and applied with the creation of strong and powerful intellectual property legislation. In contrast to Judge Easterbrook's viewpoint, Lawrence Lessig claims that thinking about how law and the internet are connected leads to an important general point.

Regulation is necessary in Cyberspace[27] as, without it, evidence suggests that the internet world will be engulfed in uncertainty and abuse will become common. Uncontrolled cyberspace has the potential to destabilize entire legal systems, rip apart societal values, and hinder commercial activity. Cyberspace is in essence a public domain and this is too true in unregulated Cyberspace, where an individual's *right to privacy is a myth*. [28] These essential human rights would be jeopardized in the real world and in cyberspace if cyberspace is unregulated.

---

[22] The Indian Penal Code, 1860, § 292.

[23] Donald T. Stephen, *"Obscenity Online: A Transactional Approach to Computer Transfers of Potentially Obscene Materials"*, 82 Cornell Law Review 905,916 (1997).

[24] JOHN PERRY BARLOW, *A DECLARATION OF THE INDEPENDENCE OF CYBERSPACE* (1996) Davos, Switzerland: Electronic Frontier Foundation.

[25] DELACOURT J. T., "THE INTERNATIONAL IMPACT OF INTERNET REGULATION" (1997) 38 Harvard International Law Journal 207.

[26] Frank H. Easterbrook, *"Cyberspace and the Law of the Horse"*, The University of Chicago Legal Forum, CHICAGO UNBOUND (1996) 207.
https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2147&context=journal_articles.

[27] HANLEY S. M. "INTERNATIONAL INTERNET REGULATION: A MULTINATIONAL APPROACH" (16 John Marshall Journal Computer and Information Law 997) (1998).

[28] Greenleaf G. *"Privacy and Cyberspace: An Ambiguous Relationship, (*3 Privacy Law and Policy Reporter) 88 (1996).

Regulation must be in place to enable individuals to retain and assert these and other fundamental human rights that are vital to the international community and humanity.[29]

III. REGULATORY MODELS IN CYBERSPACE REGIME

The governance of cyberspace is no less a pluralistic endeavour than is the governance of physical territory.[30]

(A) Constraints Regulating Cyberspace

Just as in real space, behaviour in cyberspace is regulated by four sorts of constraints:

1. Law

Law is just one of those constraints.[31] Social norms can play a role in regulating behaviour. They are different kinds of restraint. People who break the law face penalties, which can include civil penalties such as monetary losses when one infringing party is required to compensate another. There is also criminal law, which defines what acceptable and unacceptable behaviour in society is.

2. Norms

Norm is another essential limitation. According to conventional wisdom, I can buy a newspaper but not a buddy. They frown on racist jokes and are undecided on whether or not a male should hold a door open for a lady. Norms, like legislation, regulate by threatening ex-post punishment. This punishment, unlike the law, is not centralized. It is enacted, if at all, by a community rather than by the government. Norms constrain in this way. They, too, regulate in this way.[32] Those who break the rules may face consequences. In a legal system, these consequences do not carry the same weight as penalties or prison sentences. When a sanction is issued, an infringer may be placed outside of a norm group.

3. Markets

Markets govern via price, at least for the goods that are part of the market. For instance, your ability to trade hours of teaching for potatoes is limited by the market. Of course, the market is only so constrained because of other constraints of law, and social norms, for markets, are founded on property and contract law, and they operate within the realm permitted by social

[29] The Universal Declaration Of Human Rights, art. 12 & The International Covenant on Civil and Political Rights, art. 17.1.
[30] LENNON Y.C. CHANG & GRABOSKY, P., "THE GOVERNANCE OF CYBERSPACE", in Drahos, P. (ed) *Regulatory Theory: Foundations and Applications*, Canberra: ANU Press, pp 533-551. (2017).
[31] LAWRENCE LESSIG, "THE LAWS OF CYBERSPACE", Draft: April 3, 1998.
[32] Lawrence Lessig, *"Commentaries The Law of the Horse: What Cyberlaw May Teach"* 113 Harvard Law Review 501 (1999).

norms.[33]

4. Architecture, or "nature," or "real space code."

We recognize how laws control in real space; it is through constitutions, statutes, and other legal systems. We must comprehend how a different *"code"* regulates cyberspace and how the software and hardware (i.e., cyberspace's "code") that make it what it is also regulated cyberspace as it is. This *Code*, as William Mitchell puts it, is the *"law" of cyberspace.*[34] "Lex Informatica," as Joel Reidenberg first put it,[35] or better, "code is the law."[36] In this line, "*if code is law, control of code is power."*[37]

Everyone's conduct, according to Lessig's book, can be defined as a *"pathetic dot"* that is governed by *four modalities of regulation: law, norms, market, and architecture*.[38] In other terms, *regulation* is the complex interaction of the above-mentioned forces.

Lessig gives an example of smoking.[39] If one wishes to smoke, they will confront various limitations that will influence their decision:

- To begin, he explains how the *law* governs behaviour. If you are fifteen and your country prohibits minors from purchasing cigarettes, no business will sell you any, and you won't be allowed to smoke.
- Second, he explains how *norms* control behaviour. Norms are a collection of social regulations that control an individual's behaviour in any culture. When it comes to smoking, there is an unwritten rule that a smoker should not light a cigarette in a restricted location without first obtaining permission.
- Thirdly, he discusses how the law governs and regulates the behaviour *market*. If the price of cigarettes, for example, increased, it is likely that some smokers would be discouraged from smoking and eventually stop.
- Lastly, he discusses how *architecture*, or the technology used to manufacture cigarettes, affects behaviour. The desire to smoke could be stifled, for example, by lowering the

[33] *Ibid*.
[34] LAWRENCE LESSIG, "WHAT THINGS REGULATE SPEECH: CDA 2.0 VS. FILTERING", Draft 3.01: May 12, 1998, https://cyber.harvard.edu/works/lessig/what_things.pdf.
[35] J. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, Economics Texas Law Review (1997).
[36]LAWRENCE LESSIG, "CODE IS LAW", CODE AND OTHER LAWS OF CYBERSPACE, (1999), https://archive.nytimes.com/www.nytimes.com/books/first/l/lessig-code.html.
[37] WILLIAM J. MITCHELL, CITY OF BITS: SPACE, PLACE, AND THE INFOBAHN 112 (1996).
[38] KENNETH A. BAMBERGER, FOREWORD: TECHNOLOGY'S TRANSFORMATION OF THE REGULATORY ENDEAVOR, (2011) 1315-1320, https://www.jstor.org/stable/24118671?seq=1.
[39] LESSIG, LAWRENCE, CODE AND OTHER LAWS OF CYBERSPACE, (Basic Books, New York, at 92-94) (1999).

amount of nicotine in cigarettes.

Based on these ideas, it's evident that society is governed by several constraints. It is the law that directly regulates by controlling and regulating these other restraints. This births the idea of various regulatory models of cyberspace, which have been discussed hereinbelow.

(B) No Regulation

Some theorists claim that cyberspace is impossible to regulate. Because there is no physical connection between cyberspace and actual space, real-space authorities, such as government agencies, are unable to regulate its operations. Judge Easterbrook is adamant that cyberspace does not require new laws; rather, he believes that establishing strong rules and applying them to cyberspace is a superior alternative.[40] Cyberspace, according to *John Perry Barlow*, is a *"global social space,"* and governments around the world have no ability to enact laws and regulations in this area.[41] He goes on to say that cyberspace is fundamentally uncontrollable, that its technological foundations oppose territorial bounds, making law enforcement impossible to implement. However, some observers question whether Barlow's remark about the online regime was one of self-regulation rather than no-regulation. Nonetheless, it is clear that the intrusion of the government in regulating and directing the operations of cyberspace was what Barlow resisted the most.

(C) Self-Regulation

Markets, in addition to *code* and *architecture*, can act as regulating institutions. *'Self-regulation offers better speed, flexibility, sensitivity to market circumstances, efficiency, and less government intrusion'* when compared to laws enacted by the government.[42]. It's also been described as a type of responsive regulation, or regulation that adapts to the unique circumstances of the industry. The private sector's commercial operations, as well as the influence they have on and through markets, are having a considerable impact on regulation.[43] Voluntary, private self-regulation coordinated the early architecture of the internet.[44] There are two main factions in the debate over the internet's regulatory structure. On the one hand, some say that the internet is overly regulated. Network neutrality requirements, they say, are superfluous and unnecessary. Others, on the other hand, advocate for increased regulation,

[40] *Supra* Note 26.
[41] *Supra* Note 2.
[42] Gunningham, N, Grabosky, P and Sinclair, D., *Smart Regulation: Designing Environmental Policy*, Oxford: Clarendon Press (1998).
[43] Grabosky, P. *Beyond responsive regulation: The expanding role of non-state actors in the regulatory process*, REGULATION & GOVERNANCE 7(1): 114–23 (2013).
[44] FEICK, J AND WERLE, R, 'REGULATION OF CYBERSPACE', in R Baldwin, M Cave and M Lodge (eds), The Oxford Handbook of Regulation. (Oxford: Oxford University Press, 523–47) (2010).

notably in the area of technical infrastructure. Some academicians have even suggested that competent self-regulation is the only way to control cyberspace. There are three types of self-regulation[45] that are frequently recognized: voluntary or total self-regulation (without government involvement), mandated self-regulation (involving direct government involvement) and mandated partial self-regulation (partial government involvement).[46] It is quite rare to see pure self-regulation. Most self-regulation has some government involvement in directing, shaping or endorsing the regulation.

(D) Government Regulation

Despite some libertarians' strong opposition to the government using law and regulation to intervene in the evolution of cyberspace, legislation continues to play an important role in preventing cybercrime.[47] State agencies are the most important regulatory institutions. State regulatory entities will intervene or be involved regardless of the regulatory mechanism utilised. Despite the ground-breaking notion that *"code is law,"* there is still a lot of work to be done.[48] Governments frequently use intermediaries to influence behaviour collectively rather than individually. For example, copyright-infringing music and films, as well as any inappropriate content that may come to their attention, are requested to be removed from the Internet. Due to the decentralization and de-territorial nature of cyberspace, state regulatory agencies are limited in their ability to regulate it. Moreover, cybercrime's cross-border nature limits the effectiveness of laws and regulations.

(E) Technological Regulation

"Technologies are used to manage conduct in a way that assures a patterned outcome."[49] Specifically, important governance transformations occur when legal regulation is replaced by "techno-regulation."[50] The traditional assumption that conspicuous (legal) limitations represent agreed notions of what activity is 'legitimate' is diminished by such a substitute. This view of regulation as "an inclusive endeavour to explain the community's best interpretation of its

[45] Gunningham, N, Grabosky, P and Sinclair, D 1998. *Smart Regulation: Designing Environmental Policy*. Oxford: Clarendon Press.
[46] J. Braithwaite, *Enforced self-regulation: A new strategy for corporate crime control,* Michigan Law Review 80(7): 1466–507 (1982).
[47] Goldsmith & T. Wu, *Who Controls the Internet?: Illusion of a Borderless World*, New York: Oxford University Press (2006).
[48] Lawrence Lessig, *"Code Is Law,"* ON LIBERTY IN CYBERSPACE, Harvard Law Magazine.
[49] Roger Brownsword, LOST IN TRANSLATION: LEGALITY, REGULATORY MARGINS, AND TECHNOLOGICAL MANAGEMENT, 26 Berkeley Tech. L.J. 1321,1323 (2011).
[50] Roger Brownsword, *What the World Needs Now: Techno-Regulation, Human Rdghts and Human Dignity*, in 4 GLOBAL GOVERNANCE AND THE QUEST FOR JUSTICE: HUMAN RIGHTS 203 (Roger Brownsword ed., 2004).

 [ISSN 2581-5369]

moral commitments" is an assumption.[51] is, As a result, anything that is (technically) conceivable becomes permitted, and vice versa: "if the door won't open without the appropriate biometric confirmation, there is no way in."[52] By this account, the handoff from law to technology shifts regulation's pitch from the "normative to the non-normative register.[53]

IV. CYBER SECURITY AND A MULTI-MODAL APPROACH TO THE REGULATORY FRAMEWORK

"The Internet is a challenge to the sovereignty of civilized communities, States and nations to decide what appropriate and decent behaviour is."

-- Rep. Goodlatte, in US Congress

An atmosphere that was relatively free of regulations aided the expansion of the Internet and the innovation that accompanied it. However, because of its deep integration into society, the Internet has become a powerful tool for influencing geopolitical conflicts, such as interfering in other countries' internal affairs, undermining national security, destabilizing financial infrastructure, and attacks on critical infrastructure.[54]. One of the key tenets of internet policy was that the government's engagement in this new realm should be kept to a bare minimum, both because it was the right thing to do and because several impediments hinder national governments from exercising sovereign control over cyberspace. This assumption has far-reaching and ultimately devastating security repercussions.[55]

(A) Freedom v. Regulation Debate

Innovation and freedom cannot thrive in a chaotic environment with rampant crime and a lack of rules, norms, and ethics.

For those who consider regulation and freedom, cyberspace offers something fresh. It necessitates a fresh understanding of how regulation works and what governs life in that environment.[56] Every epoch has a potential regulator, a possible menace to liberty. This is the cyberspace era. It, too, is governed by a regulator. This regulator, too, poses a threat to freedom.

---

[51] Retrieved from https://www.jstor.org/stable/24118671.
[52] *Id.* at 1324.
[53] Kenneth A. Bamberger, *Technology's Transformation of the Regulatory Endeavor*, Berkeley Technology Law Journal , Vol. 26, No. 3, *SYMPOSIUM: TECHNOLOGY: TRANSFORMING THE REGULATORY ENDEAVOR* (2011), University of California, Berkeley, School of Law. 1319.
[54] Sanjay Goel, *'National Cyber Security Strategy and the Emergence of Strong Digital Borders'*, Vol. 19, No. 1, (Published by: Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, at 73-86, (2020)).
[55] James A. Lewis, '*Sovereignty and the Role of Government in Cyberspace'*, THE BROWN JOURNAL OF WORLD AFFAIRS, Vol. 16, No. 2 (Spring / Summer 2010), pp. 55-65.
[56] David G. Post, *What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace (A Review of "Code and Other Laws of Cyberspace" by Lawrence Lessig, Basic Books, 1999*), May, 2000; 52 Stan. L. Rev. 1439.

However, we are so fixated on the idea that liberty entails "government-freedom" that we fail to see the regulation in this new environment. As a result, we do not believe that this regulation poses a threat to liberty. *Code*, the software and hardware that make cyberspace what it is, is this regulator.[57] Lessig argued that cyberspace is substantially regulated by *code*- computer programming and system architecture. The internet is built on simple protocols based on the Transmission Control Protocol and Internet Protocol (TCP/ IP) suite, he writes in his book, *"Code: Version 2.0."*[58] Cyberspace is a result of architecture rather than 'God's will.' Lessig stated that the internet is the most regulated space we are aware of because it can reveal who someone is, where they are, and what they are doing through its architecture.

It might be claimed that, while cyberspace rules may appear to be a threat to individual liberty and freedom, if implemented wisely, they may prove to be advantageous to the cyberspace regime and the threats that it may expose mankind to if left unregulated.

In this regard, the *Multi-Modal Approach of Regulatory Framework* is proposed.

(B) Multi-Modal Approach of Regulatory Framework

The interconnected nature of cyberspace's regulatory modes presents a tremendous opportunity for developing a stable and coherent regulatory regime. The multi-model regulatory approach, which emphasizes that the core modalities be individually weighed and balanced with respect to any particular subject in order to create an individualized regulatory mix that is most appropriate to the issue, will be used to fully cater for the intricacies of each individual regulatory issue.

The multi-modal model regulatory framework recognizes that no single regulatory method can provide the best regulatory regime for all subjects.[59] The regulatory mix, as specified by the multi-modal model approach, is extremely flexible, which is an important feature of any cyberspace regulation.[60]

Our choice is not between "regulation" and "no regulation." *The code regulates*.[61] It either implements values or does not. It either allows or restricts liberties. It either protects privacy or encourages surveillance. As a result, the question is not whether people will decide how cyberspace is regulated, but rather how cyberspace will be regulated. The only decision we have is whether or not we will play a role in their decision as a group because it is self-evident

[57] Lawrence Lessig, *"Code Is Law,"* ON LIBERTY IN CYBERSPACE, Harvard Law Magazine.
[58] Lessig, L. *Code: Version 2.0*, New York: Basic Books (2006).
[59] Lawrence Lessig, *Commentaries The Law of the Horse: What Cyber Law May Teach* (1999) 113 Harvard Law Review 501.
[60] Hardy T. *The Proper Legal Regime for Cyberspace*, 55 (U. Pitt. L. Rev. 993, at 1026).
[61] Supra Note 36.

that when the government steps aside, nothing takes its place. It's not as if private interests don't have interests; it's not as if private interests don't have goals to achieve. It is not a solution to press the anti-government button.[62]

As a result, we must allow the government and autonomous cyberspace institutions to collaborate and work together to regulate cyberspace, as this will be the most effective form of regulation in this techno-legal context. We should examine both government-made laws and market products against the ideals we want to instil, according to Lessig, and we should investigate the architecture of cyberspace as thoroughly as we investigate the code of Congress.[63]

V. CONCLUSION AND SUGGESTIONS

Of the various regulatory models of cyberspace, it can be said that a "no-regulation" regulatory regime in the affairs of cyberspace would result in a state of cyber anarchy, and hence is unacceptable. Regulation of cyberspace is required because without it, users' rights in cyberspace will be overrun and suppressed, and the rules of the real world will be weakened. Unregulated cyberspace has the ability to jeopardize legal systems, suffocate cyberspace activities, and degrade community values. Regulation is essential in the cyber world in order to safeguard and uphold rights in both the actual and virtual worlds. The regulation's form, on the other hand, should not be completely legalistic, simply transposing existing real-world legislation. The regulation should not take the shape of *socio-normative self-regulation*. Instead, the ideal best regulatory mix is that which incorporates legal, socio-normative, and contextual concerns. Therefore, there is no "one-size-fits-all" prescription for regulating and securing cyberspace; because no single regulatory model is sufficient to control cyberspace; instead, we must adopt a multi-model regulatory framework, the best of which, in the researcher's opinion, is a radical mix of self and government regulation.

*****

[62] Lawrence Lessig, *"Code Is Law,"* ON LIBERTY IN CYBERSPACE, Harvard Law Magazine.
[63] *Ibid* at 4.