CYBERSPACE AS A PLACE OF EVIDENCE: A CRITICAL REVIEW UNDER INTERNATIONAL HUMAN RIGHTS LAWS

Bayazid Hossain*

ABSTRACT

Cyberspace is domiciled by the people beyond national boundaries. As a result, conventional notion of absolute sovereignty does not operate in this premise. Cyberspace is regulated directly by incorporated bodies having licensed by particular States. This system treats licensing and non-licensing differently. A licensing State may easily call for evidence from any internet intermediary on demand and the cyberspace authority is responsible for providing any evidence required by law of the licensing State in terms of sovereignty. But non-licensing State has no such authority for the limited scope of State sovereignty in cyberspace. This ambivalent nature of cyberspace has rendered cyberspace in a place of discrimination although it ought to accommodate the status of 'Non-State Actor' under international law. This critical position of cyberspace reasonably raises two questions. Firstly, is it justified that every cyberspace should protect a particular State policy in terms of evidence? Secondly, what should be the standard in governing cyberspace? Cyberspace is essentially required to be transformed into a responsible setting for equal protection and promotion of human dignity irrespective of national or geographical identity. Therefore, principles of human rights jurisprudence reflecting through a universal consensus can be the guiding principle in cyberspace jurisprudence.

I. INTRODUCTION

The rooms and spaces used as custody of evidences accommodate tons of papers, seized materials and samples to be used in trials. The paper exclusively argues the scopes and advantages of transformation of paper-based conventional evidencing system into the paperless digital evidencing in the justice systems of the States where the right to justice as human rights is often affected by insufficient evidence. However, internet-based unconventional evidencing policies typically invite unprecedented legal challenges within the domain of existing offline framework. For example, a police officer may easily inspect and visit the place of occurrence committed within his jurisdictional locality. But this situation is complex, if the place of occurrence in cyberspace which is not situated at any location of the real world. Evidence located in cyberspace is possible to be a key-factor in any case.

* **Bayazid Hossain**, LL.M (University of Rajshahi, Bangladesh), is an Assistant Professor (Law), School of Social Sciences, Humanities and Languages; Bangladesh Open University, Bangladesh.

On the other hand, cyberspace is not neutral to all States.[1] This leads States to cumulative effects on justice system of licensing States (LSs) and Non-licensing States (NLSs)[2]. Cyberspace is, at present used in asymmetric ways of communication services for which licensing are being highly benefitted in terms of ensuring justice but the position of non-licensing States for the same cause is entirely opposite. Moreover, any trial court or tribunal of a licensing State can freely enter into cyberspace as a place of evidence but it is entirely unreachable for the courts of non-licensing States. [3] Internet intermediaries like *Facebook* have tremendous power and they can wield that power for good or evil. Evidence stored in Facebook is universally a strong source of evidence because people prefer online communication to offline communication in the ordinary course of dealing. [4] All internet intermediaries are expected to function for the greater common judicial interest of all States. The paper plausibly asks for a review of the existing one-sided and imbalanced performance of internet intermediaries in offering rights to access to information from cyberspace. Therefore, the paper is highly intensified to draw a roadmap in justifying the need of evidence stored in cyberspace required by courts of non-licensing States and State responsibility of licensing States for any ambivalent functions over licensed cyberspace under international human rights laws. The research paper is outlined within a few limitations. The paper incorporates only the online evidences produced through the application of online social networks. This piece explains the position of a licensing state through the social networks

---

1 Hossain, B. "Identity Deception: Is Cyberspace Humane Enough for Women?" in Rahman, M. et al. (Ed.), *Human Rights and Women*, Dhaka, 2017, at p. 99.

2 The terms 'Licensing State', in this paper, refer to a State that grants license to particular body or enterprise in creating, designing and managing internet intermediaries in cyberspace. For example, the *Facebook* is registered under the US laws. The USA is the licensing State of *Facebook* and *Facebook* is accountable US law and orders.

The terms 'Participating State'/'Non-licensing State', in this paper, refer to a State that can only allow/ or disallow its citizens to get access to a particular online network of internet intermediaries but the internet intermediaries have no obligation before the courts this state. For example, the *Facebook* is allowed to be used in Bangladesh under Bangladeshi laws and orders. *Facebook* does not require any license to be operated in Bangladesh. Here, Bangladesh is the Participating State of *Facebook*.

3 See, for example, Facebook's data policies [which are available at, https://www.facebook.com/policy.php?CAT_VISITOR_SESSION=c7b73ebc78d1681ade25473632eae199]. Being the registered company Facebook Inc. is responsible to the US only. However, Facebook is not lawfully and *de facto* responsible to other States because Facebook does not require registration or incorporation to be operated in other States.

4 Miller, R.L. and Hollowell, W.E., *Cengage Advantage Books: Business Law: Text and Exercises*, Boston, 2016, at p. 98.

originated and maintained from US. Therefore, US policies in the administration of online networks have been analyzed to illustrate the tendencies of licensing states. Additionally, by the terms 'online evidence' the paper refers to all forms of online evidences within ordinary course of personal communications *per se*. The paper attempts to analyses the deficiency of evidence in courts of non-licensing States as the key factor of human rights violation arising from discriminatory behavior of cyberspace.

II. NATURE AND SOVEREIGNTY OF CYBERSPACE

Cyberspace is typically thought to be purely a non-legal area if online communication does not require any specification as to rights and liabilities of the users.[5] American poet and essayist *John Perry Barlow*, a known cyberlibertarian, argues for the independence of cyberspace from the legal concepts.[6] This idea of placing cyberspace non-legal domain is based on some assumptions like cyberspace is different from real spaces and it should remain open, decentralized and participatory one, not hampered by legal regulations.[7] However, it is undisputedly practicable that cyberspace is subject of rights and obligations determined by municipal law and international law.[8] The challenges apparent in cyberspace are unconventional in traditional human rights jurisprudence. Most often, State interest confusingly treats internationally common interests in cyberspace. Cyberspace is practically an information highway and states join in this system to enable people for borderless communication with muti-dimensional necessities. [9] In this system, cyberspace is ought to be like *res communis*[10] in which both licensing and non-licensing States would be equally treated in sharing online personal information or evidence for ensuring justice to all. However, this has not been uncomplicated so far and cyberspace is practically controlled under absolute sovereignty of licensing states.

Cyberspace is itself a reality in which corporeal character or the real world is absent. It is generally argued that in many cases, the *res communis* concept

---

5 Tsagourias, N. "The Legal Status of Cyberspace" in Tsagourias, N. and Buchan, R. (eds.), *Research Handbook on International Law and Cyberspace*, Massachusetts, 2015, at p. 13.

6 *ibid*

7 *ibid.*

8 Kittichaisaree, K., *Public International Law of Cyberspace*, Berlin, 2017, at pp. 23-40.

9 See for example from Canadian perspective, Chodos, R. et. al., "*Lost in Cyberspace?: Canada and the Information Revolution*", Ontario, 1997, at p. 10-12.

10 *Res communis* is a Latin term derived from Roman law that preceded today's concepts of the commons and common heritage of mankind. It has relevance in international law and common law.