The nation's ability to control cyberspace

Qiuyi Hou, Yue Yan

Southwest University of Political Science and Law, 401120, China

ABSTRACT. *Nowadays, some people argue that the nation-states are gradually losing the ability to regulate cyberspace. However, other people hold the different opinions.*

1. Introduction

Undoubtedly, tremendous challenges to traditional notions of jurisdiction and regulation of cyberspace are posed by cyberspace and as a result, some people may argue that the regulation of cyberspace is bound to experience a higher degree of failure.[1] This essay will be divided into several parts. Firstly, it will discuss the reasons and some problems due to the failure of regulation in cyberspace. Then, it will discuss whether regulation is needed or not in relation to two totally different theorists. Then, whether regulation is needed or not will be discussed relating to different opinions and some ideas in favor of self-regulation. Then, this essay will illustrate how the nation states will regulate cyberspace if regulation is required. Finally, it will start with some reasonable regulatory methods used by UK currently and in the future.

2. The problems and reasons of failure-regulation of cyberspace

It is obvious that a great number of differences exist between cyberspace and physical space.[2] For example, there is no tie to geography which means that the boundaries between public and private law, national and international law, are not adequate and meanwhile, the cyberlaw is too widespread to be regulated by nation-states. In addition, it is not easy for nation-states to regulate cyberspace due to the anonymity of users as well as that the servers can be moved.

3. Whether regulation is needed or not by nation-states

As for whether regulation is needed or not, different theorists and theories responded differently to the question, and it can be divided into two main parts, including the cyber-libertarians and cyber-paternalists.[4] They believe that the Internet is so widespread that it cannot be easily regulated by nation-states. John Perry Barlow is such a person believing that cyberspace is a separate sovereign space where real-world laws and real-world governments were of little or no effect[5]. In their argument, they believed that as states may only enforce their laws within the confines of their jurisdiction.[6] When a citizen of a physical world enters the Internet world they cross a virtual border to a new sovereign state, the laws of the old sate they left are no longer valid or legitimate. Moreover, because this person is in a virtual environment, they have no corporeal body to imprison.[7] In addition, they hold the belief that it is illegal for the real-world law enforcement authorities to interfere the operations of 'Sovereign Cyberspace because they regard the Internet world a conceptually separate state and as a result, it will be hard for the state sovereignty to function effectively in cyberspace.[8] Therefore, it is hard for law-makers in real world to enforce laws against citizens of cyberspace and further, the regulation of cyberspace by nation-states is not required to some extent and further, the nation-states are gradually losing their authority to regulate the cyberspace. However, based on their arguments, it is easy for us to find weaknesses. Specifically, if an individual were to engage in illegal or antisocial behavior online their corporeal body remains subject to direct regulation of our nation- states in which they are resident at that time. Besides, a group of people hold the opposite position, for example Joel Reidenberg. Targeted at the difficulties and nature of Internet world, two new regulatory borders arising from new rule were identified which involves states, the private sector, technical interests, and citizens. He proposed the second border which was man-made and could be controlled by individuals.[9] He claimed that technical standards could function like geographical borders and a new way was suggested by him to control and regulate the online environment, called as 'Lex Informatica'. In addition,

Professor Lawrence strongly suggested that lawmakers seeking to control the online activities of citizens would seek to indirectly control these activities by mandating changes to the network architecture, or by supporting self-regulatory activities of network designers.[10] One of the most progresses of him was four" Modalities of Regulation" and it can be used individually or collectively, either directly or indirectly, in order to control the actions of individuals whether offline or online. They respectively are called laws, markets, architecture, and norms.[11] In addition, one of the most famous cyber-paternalists is called Lawrence Lessig who also believes that online activity is regulatable once individuals expands the modalities, rather than just focused on law.

4. If regulation is required, then how?

Different professors show various opinions. For example, Wall suggests making use of technology but sometimes the technologies of control can make the problems worser[12] Besides, Murray regards cyberspace as a challenge because it cannot be intervened due to its movement and there are several questions which are hard to answer. For instance, it is not easy to define the regulators when competition emerges between nation-states. In addition, the line between regulators and regulations is blurred and meanwhile, there are no common and standard types of regulation for nation-states. Specifically, France, Europe both requires stricter cyberspace control after the Paris Terror attacks. Turkey fines twitter for failing to remove terrorist propaganda.

5. Self-regulation

Nowadays, a number of people hold the belief that it is no need for the nation-states to regulate cyberspace because the Internet world can be regulated by itself. For example, the ISPs which are increasingly make full use of self-regulation in order to prevent nation-states authority to regulate cyberspace gradually. However, some people also argue that it is considered as being towards one end of a continuum from purely private regulation towards regulation which is characterized by a greater degree of state involvement.[13] It is said that degree of participation of nation-states in two levels, respectively the formation of rules(code) and the enforcement mechanisms used to incentive compliance.[14] It is not beneficial for cyberspace through the way of self-regulation but also bringing advantages for the nation-states. For example, it can be used to reduce the cost of enforcement and at the same time, providing a more business-friendly light. Meanwhile, more intrusive legislative intervention may be ward off. [15]To access this, it is reasonable for us to jump off the state and the industry so that the third party can be considered- the citizen. However, some people are concerned that governments, by compelling intermediaries or industry to take on a regulatory function, may be able to make an end-run around constitutional or procedural limitations which would otherwise constrain their actions.[16] Targeted for this problem, a possible solution was to blend self-regulation and mandatory rules by the nation-states.

6. Several approaches used by nation-states to regulate cyberspace

There is no doubt that there exist several approaches used by nation-states to regulate cyberspace. For example, the narrow-approach often used by the nation-states to pay more attention on infrastructure of Internet. However, the broad approach stresses the importance of going beyond infrastructural issues and address other legal economic, developmental, and socio-cultural issues.[17] Besides, the old-real approach argues that cyberspace cannot not introduce anything new to the field of governance while the new cyber-approach says that the internet is seen as just another device, fundamentally different from all previous ones. Thus, it requires fundamentally different governance.

7. The current UK legal framework for interception

It is justifiable for nation-states to operate surveillance programs for the purposes which are listed in Art.8(2) ECHR: in the interest of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Therefore, in order to protect our collective interests, it is acceptable placed under the surveillance of a few authorities and enforcement agencies. Meanwhile, it is possible for individuals to rely on the principle of proportionality to make sure that these operations not be made use by state to become a method of state control, for example, The early East Germany. Therefore, it is truly necessary for nation-states to operate legislative controls because of the power of surveillance and extensity of data gathering and meanwhile, a strict legal framework is proposed in order to control the powers and ability of the state to monitor its own citizens for

instance, the ECHR itself and Art.8. One of the most striking case is Klass & Ors v Germany. The court stated that only when the nation-states have the ability to counter threats or terrorism, they can have get access to some subversive elements and the court also accepted that under exceptional conditions, existence of some legislation granting powers of secret surveillance through many ways for the interests of national security and or the prevention of crime.[1] However, it still needs to be limited although it enjoys a wide range of discretion.

In conclusion, in order to analyze whether the nation states have lost the authority to regulate cyberspace, this essay has discussed many aspects of it. Firstly, it has discussed the challenges for nation-states to regulate cyberspace. Next, it has analyzed whether it is still meaningful for the nation-states to regulate cyberspace in relation to self-regulation. Thirdly, this essay has illustrated how the nation states regulate cyberspace if regulation is still required. Finally, it has discussed some useful approaches used by nation-states to govern the cyberspace.

References

[1]   JP (1996). A Declaration of Independence for Cyberspace. Stanford Law Review.
[2]   C Reed (2004).   Internet law: Text and Materials.
[3]   P Barlow (2001). A Declaration of Independence for Cyberspace Criminal Justice and Immigration Act.
[4]   Jonson, D Post (1996). The Rise of Law in Cyberspace.
[5]   Reidenberg (1998). Lex Informatica: The information of Information Policy rules through Technology. Texas Law Review.
[6]   Awrence Lessig (1999). Code and Other Laws of Cyberspace. Basic Books.
[7]   Murray (2019). Information and Technology Law. The Law and Society.