PROTECTING VIETNAM'S SOVEREIGNTY IN CYBERSPACE: INSIGHTS FROM HUMAN RIGHT LAWS

VU THI ANH THU[1,2]

Abstract: In order to protect state sovereignty in cyberspace, Vietnamese law has placed restrictions on the right to online free expression. Using qualitative and empirical methods, this article examines the necessity and proportionality of these restrictions. The article finds that the language of a number of restrictive provisions appears to be more political than legal. The second reason is that vague and expansive laws may make it difficult to determine the true extent of damage in criminal prosecutions involving online expression that undermine state sovereignty. It would violate Articles 19 and 20 of the International Covenant on Civil and Political Rights. To surmount this opposition, Vietnamese lawmakers must provide a comprehensive interpretation of the relevant laws to ensure that the freedom of online expression is vitally important but must be balanced with the national interest.

Keywords: Sovereignty, human rights, freedom of expression, cyberspace, cybersecurity, Vietnam.

1. Introduction

The expansion of the Internet has facilitated cross-border communication between nations, communities, and individuals. Information is a crucial communication medium. The Internet provides instantaneous information transfer, enabling consumers to access information from any location at any time (Коровин В. 2017:79). Due to the unique characteristics of the Internet, however, misinformation and disinformation, political hate speech[3], and violent incitement against the state are more likely to spread online and present challenges to state control.

[1] PhD of International Studies, Vice Dean of Faculty of International Studies, VNU-University of Social Sciences and Humanities, Vietnam National University, Hanoi (e-mail: vuanhthu@ussh.edu.vn)

[2] This article has been written as part of a research project "Ensuring sovereignty in cyberspace under the international laws". The author would like to thank Vietnam National University, Hanoi for funding project QG19.32.

[3] The Council of Europe's Recommendation (1997) covers the internationally accepted definition of "hate speech," which shall be understood as "covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance." Subsequently, Mutlu Binark and Tuğrul Çomu (2012) defined political hate speech as "targeting a certain political opinion and its followers. It may sometimes target an ideology as a whole, only one or a few political parties, or even smaller groups".

As soon as negative information is disseminated, it is just as pernicious as cyberattacks against the sovereignty and cybersecurity of a state. Every Internet user has the potential to become a social media news author or commentator. Unchecked information sharing can result in the intentional or inadvertent dissemination of false information about a political event or the domestic or foreign policies of a government. Internet users band together as couriers in a network that Коровин В. (2017) suggests includes social organizations, foundations, non-governmental organizations, movements, and political parties, regardless of whether they are self-interested. He believed that the "Information Society was an appropriate setting for establishing, operating, and utilizing networks. Networks operate in all environments and are not metaphors. They are an objective reality of contemporary culture." (Коровин V. 2017:111-112). The mission of the network is to be able to transmit all but a few signals that can be received, transmitted further on the network, and eventually transformed into actions by what Коровин В. termed "network warfare," which he defined as "the set of activities designed to shape the behavior of neutral forces, allies, and adversaries in times of peace, crisis, and war." (Коровин 2017:116). Unrestrained, malevolent information flows would endanger national autonomy and sovereignty. In addition, Betz and Stevens (2011:69–70) argued that "terrorist use of the Internet as a means of propaganda is a classic case where the state is unable to control what passes its borders. Governments have attempted to restore control by removing videos with terrorist content from the Web". Terrorist organizations, adversaries, and anti-state groups can abuse the Internet and social media in conjunction with "effect-based operation" technology to inform thousands of Internet users of their plans to attack a specific state.

Online calls for protests and collective action sparked a number of significant events, such as the "Rose Revolution" in Georgia in 2003, the "Orange Revolution" in Ukraine in 2004, the riots in Tunisia that sparked the "Arab Spring" in Egypt in 2011, and the domino effect that toppled totalitarian governments in several North African and Middle Eastern nations, including Iraq, Syria, and Yemen. According to Philip Howard and Muzammil Hussain (2011:35–48), "digital media technology has not only stimulated widespread protests in Egypt but also produced a distinctive kind of mass organizing that is repeated across the region". Even more damaging is the manipulation of global media coverage by digital media, which has enticed foreign governments or government opposition movements to intervene in state affairs. Disgruntled or xenophobic people at home and abroad can attack any authoritarian or democratic state via the internet and social media.

Every year, hackers attack thousands of e-information portals, websites run by governmental organizations, local governments, and large corporations, as well as electronic newspapers in Vietnam[4], seizing control, changing the user interface, editing the content, or causing stalls and disruptions. Even hostile forces have cyberspace-directed interconnected activities to carry out terrorist missions in a number of major cities. Hostile

[4] In the first six months of 2021, the High-Tech Cyber Security and Crime Prevention Office detected 1,555 Vietnamese websites (.vn) that were attacked by hackers, inserting messages, including 412 pages managed by state agencies (C Nguyen and Q Nguyen 2022).

forces abroad encourage a large number of people in the country to post fabricated and distorted articles on social networking sites. They employ sophisticated propaganda techniques and incorporate articles that challenge authorities or direct demonstrations, as well as how to interact with security agencies. They broadcast audio and images of demonstrations online in order to attract, provoke, and gather forces in both cyberspace and the real world for the purpose of mental terrorism and generating public opinion in the network community in order to serve malicious purposes that harm politics, order, and social security (Tran D.Q. 2015).

Apparently, state security and sovereignty are more at risk than ever before. States are cognizant of the online threats posed by violent language. They are willing to take the necessary technical measures to censor and filter information on social media, as well as to prevent and block extreme expressions deemed offensive. Inversely, the competent authority's arbitrary, non-selective prevention and treatment efforts may contravene the right to free expression of Internet users.

Threats to sovereignty and security in cyberspace are mentioned in several research papers. In the article 'Cyberspace Sovereignty? The Internet and the International System', Tim Wu (1997) examined access to national cyberspaces and the authority of nations to issue legal regulations governing the Internet and cyberspace. According to the author, cyberspace can be regarded institutionally through a realism lens. When the international system resembles a community of states, state sovereignty over cyberspace is severely constrained and determined by state-level collective interests. This is inadmissible. Consequently, the author analyzes the extent of the state's cyberspace rights according to liberal theory. Individuals and then nations have "minimal sovereignty" over cyberspace, the authors conclude, because they have access to it first.

In the article titled "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights," Lotrionte C. (2012) posed the question: can a state use force to defend itself against cyberattacks by non-state actors residing in a different country? Can the use of force by the infringing state be justified under international law? The author argues that the *Jus ad bellum* principle should be carefully reviewed by states in order to reach a consensus on how to interpret the use of force to ensure peace and security, and whether a cyberattack should be considered a military attack so that a state can use the principle of force in self-defense.

Evidently, states are aware of the threat that adversarial expression and incitement to anti-state violence pose on the Internet and in digital media. States are willing to employ the technical measures they deem necessary to censor and screen news in digital media in order to prevent the anti-state effects of free expression they perceive to exist in cyberspace. However, states must also anticipate the consequences of their stringent, non-selective precautions and prevention measures, which could potentially restrict the freedom of expression of the vast majority of network users.

How to maintain a balance between the protection of state sovereignty and the exercise of the right to freedom of expression by Internet users in cyberspace is the subject

of this article. Can states with supreme authority impose stringent technical and legal restrictions to protect their state sovereignty while ignoring online human rights? Using qualitative and empirical methods, this article examines the necessity and proportionality of restrictive measures imposed on human rights by Vietnamese law under the pretext of protecting state sovereignty in cyberspace. The article begins by analyzing the concept of state sovereignty in cyberspace and, in particular, the right to free expression on social media platforms. Referring to Articles 19 and 20 of the International Covenant on Civil and Political Rights (ICCPR), the article then analyzes the legal basis upon which Vietnam can impose restrictions on freedom of expression. The article further examines two criminal cases judged by Vietnamese courts in response to the question of how to evaluate the appropriate degree of restrictive measures applicable to freedom of expression online on the grounds of protecting state sovereignty in cyberspace. The article asserts that there are threats to sovereignty and violent calls to overthrow the Vietnamese government on social media. However, the content of certain prohibitive provisions of Vietnamese law appears to be more political than legal. To this extent, Vietnamese law is ambiguous and general. Political hate speech and violent incitement speech might make it challenging to evaluate the actual harm they cause. The conclusion of the article is that the Vietnamese legislature has adopted the ICCPR provisions on human rights restrictions. However, further interpretation of the relevant regulations is required to strike a balance between the protection of state sovereignty in cyberspace and the promotion of freedom of expression online.

2. Conceptualizing Cyber Sovereignty

Sovereignty is one of the state's inseparable political-legal characteristics that has been acknowledged over the centuries. The word "sovereignty" comes from the French "souveraineté" and the Old Latin *superanitas*, suprema potestas, or *superus*, all of which mean "supreme power" (Nico Schrijver 1999: 65; Britannica 2020). When discussing the concept of state sovereignty in cyberspace, it is becoming a heated topic of never-ending debate among academics from the perspectives of international law and international relations in the context of globalization, and the impact of the Fourth Industrial Revolution.

The Interdependent Sovereignty or Conditional Sovereignty View in the Context of Globalization

Under the influence of globalization, the supreme and exclusive nature of state sovereignty from the perspectives of absolute sovereignty (advocated by Bodin J. (Edward A. 2011), Machiavelli N. (1532), and Hobber T. (1651)) and independent sovereignty (represented by Rousseau (1944)) is shifting. This fact demonstrates that states actively participate in the globalization process and are subject to the universal standards and norms established by international and intergovernmental organizations such as the United Nations, the World Trade Organization, and the International Monetary Fund. It indicates that they voluntarily restrict the scope of their authority. International action programs increasingly influence and impact domestic policies. States are answerable to their citizens and the international community for their

domestic and international actions that violate human rights or are likely to do so. Although the principle of non-interference in the internal affairs of states, enshrined in paragraph 7 of Article 2 of the 1945 United Nations Charter remains valid as long as states exercise their sovereign rights, it does not permit states to act unilaterally and disregard international obligations.

The influence of globalization on the exercise of sovereign rights has modified the scope of state jurisdiction and control over domestic and international affairs, but globalization does not create new methods to restructure the power of states. This, however, cannot eliminate state sovereignty, namely national self-determination and respect for the principle of non-interference in the internal affairs of states. Therefore, the scope and application of state jurisdiction and control are voluntarily determined when states participate in international treaties. Elizabeth and Ozioko (2011:256) addressed the fact that "states are free to endorse any contract they find attractive. Any treaty among states is legitimate, provided that it has not been coerced. This is the new strength of sovereignty."

State Sovereignty under the Impact of the Information Technology Revolution

With the influence of the information technology transformation, globalization accelerates the international integration of states, particularly those with rapid Internet and telecommunications infrastructure development. In addition to the physical world, the Internet and the information technology revolution have created a virtual world that attracts numerous participants. This virtual world is known as "cyberspace"; it can connect people from anywhere in the world at any time and has brought numerous socioeconomic and cultural benefits to humanity. When criminals and adversaries take advantage of anonymity to commit illegal acts and even imperil state sovereignty and security in cyberspace, anonymity poses significant challenges and risks.

There are many ways to understand the concept of "cyberspace". Dyson E., et al. (1994:295) defined cyberspace as "more ecosystem than machine, cyberspace is a bioelectronic environment that is literally universal: It exists everywhere there are telephone wires, coaxial cables, fiber-optic lines or electromagnetic waves." The U.S. Department of Defense also defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Office of the Chairman of the Joint Chiefs of Staff, 2021:55).

According to the above definitions, cyberspace is a virtual environment that is shaped and founded on the physical characteristics of an interconnected system of electro - electromagnetic apparatus under the state's ownership and control. Hathaway M. et al. (2016:8) further emphasized the social interaction between users in cyberspace, stating that "cyberspace is more than the Internet, including not only hardware, software, and information systems, but also people and social interaction within these networks." The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) also mention the formation of cyberspace through the interaction

of users with the support of information technology, as it is "the complex environment resulting from the interaction of people, software, and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form" (2012). The 2018 Cybersecurity Law of Vietnam (LOC) also takes a broader view, not only from a technical perspective but also from a social connection perspective:

> **Art.3.2**: "cyberspace is the connected network of information technology [IT] infrastructure comprising telecom networks, the Internet, computer networks, information systems, information processing and control systems, and databases, where [being the environment in which] people perform social acts without being constrained by space and time." (VN National Assembly 2018)

In such a networked environment, information is regarded as the center of the electronic transmission process and constitutes the Information Society. In order to reflect the state's influence in international relations and ensure national security in cyberspace, information is an essential asset. Due to the trans-spatial and trans-temporal character of information convergence on the Internet, there are ongoing discussions regarding state control over information flows and electronic transactions in cyberspace. There are various perspectives on the exercise of state sovereignty in cyberspace or the degree to which cyberspace depends on state sovereignty. In this regard, policymakers, researchers, and technology firms have not yet reached a consensus.

Views on the Independence of Cyberspace in relation to State Sovereignty

The work titled "A Declaration of the Independence of Cyberspace" written by Barlow J. (2019:5-7) served as a representation of this viewpoint. He asserted that cyberspace is "the new home of Mind" and "Civilization of the Mind in Cyberspace," thereby establishing a new, non-sovereign community. There is no authority for the state to impose laws and enforcement measures. He emphasized that despite the fact that governments can construct and create tools to facilitate social interaction in cyberspace, they are not welcome in a social space that is so globally accessible. Cyberspace and state sovereignty were therefore distinct from one another. Barlow J. believed that in this anonymous world, users could freely express their opinions without government restrictions, coercion, threats, or punishments. Cyberspace's autonomous and non-physical nature has allowed Internet users' thoughts and actions to transcend territorial boundaries, which is a defining characteristic of state sovereignty.

Views on the Relationship between State Sovereignty and Cyberspace

Numerous governments and experts in international law have disagreed with John Barlow's position that cyberspace should not be subject to state sovereignty. This fact demonstrates an increase in cross-border cyberattacks aimed at vital national technical infrastructure and computer systems. Even a foreign state can use the virtual world to interfere in the internal affairs of other states, which is considered an invasion of national sovereignty and security. Therefore, the assaulted state is permitted to employ technical,

military, and legal means to prevent and stop cyberattacks. Moreover, if the dissemination of malicious code or the use of armed force in cyberspace threatens international peace and security, the countries need to come together to develop international laws and codes of conduct to prevent transnational cyberattacks. Following is a discussion of the two connections between sovereignty and cyberspace.

First, there are the relationships between cyberspace and sovereignty. Betz D. and Stevens T. (2011:55–60) argued that under Article 2 of the UN Charter, political entities in the international relations system are recognized as equal in terms of sovereignty, so cyberspace should also be regarded as a sovereign entity within this system. Cyberspace has *a de facto* legal status as a global space that transcends traditional sovereignty as a result of the blurring of territorial boundaries caused by cross-border information flows. In light of this, the authors proposed that states should respect "emerging cyber sovereignty". In reality, many states have never desired to relinquish their sovereign rights over cyberspace under their authority, so they have not adopted this proposal. In addition, no nation has acknowledged cyberspace as an autonomous entity with independent legal status that functions as a "representative voice" on par with sovereign nations.

Second, there is the relationship between domestic sovereignty and cyberspace. States have absolute sovereignty over the cyber infrastructure on their own territory. Individuals and organizations conducting operations within this cyber infrastructure fall under the jurisdiction of the host nation. On the basis of preserving state sovereignty and security, the state has the authority to exercise its absolute sovereignty in monitoring cyberspace activities and responding to cyber security violations (Liaropoulos A. 2013:19).

States can establish territorial sovereignty over land, airspace, sea, and islands[5] within a specific geographical boundary. Cyberspace, on the other hand, is not a natural environment because it was created by humans and exists alongside physical objects. Numerous states have acknowledged cyberspace as the "fifth domain" subject to their jurisdiction and supervision, as well as the preservation of their security and interests. They are able to take protective measures to prevent and respond to cyberattacks, regardless of whether they originate from within or outside their territory. Chinese President Xi Jinping stated at the Second World Internet Conference in Wuzhen in 2015 that "cyber sovereignty is critical to national sovereignty" (Xinhua 2016).

According to Rule 1 of the Tallinn Manual 2.0 (Schmitt M. 2017:11)

> "States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure…. In certain

[5] For example, Article 1 of Vietnam's 2013 Constitution states, "The Socialist Republic of Vietnam is an independent, sovereign, and united nation whose territorial integrity includes its mainland, islands, territorial waters, and airspace" (VN National Assembly 2013).

> circumstances, States may also exercise sovereign prerogatives such as jurisdiction over cyber infrastructure and activities abroad, as well as over certain persons engaged in those activities."

Resolution 73/266 of the United Nations General Assembly (2018:para5-6) also emphasized that "states have the primary responsibility for maintaining a secure and peaceful information and communications technology environment". Nonetheless, the resolution expressed concern that "technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may affect the integrity of the infrastructure of states, to the detriment of their security in both civil and military fields".

It appears that each state asserts sovereignty in cyberspace to varying degrees and uses its legislative, executive, and judicial powers to enact laws governing information security and safety, manage and monitor activities in cyberspace, and impose administrative or criminal penalties for violations. In contrast, a state that employs violent or non-violent means to attack the essential information infrastructure systems or critical economic and social facilities of another state is viewed as a threat to the latter's national security and sovereignty. Consequently, the preservation of the cyber infrastructure network is an essential activity for safeguarding cyberspace state sovereignty. According to The New York Times (2009), the President of the United States, Barack Obama, stated that "our digital infrastructure -- the networks and computers we depend on every day -- will be treated as a strategic national asset". Protecting this infrastructure will be a top priority for national security.

The analysis presented above demonstrates that the protection of state sovereignty in cyberspace can be viewed from two perspectives:

First, cyberspace is considered a "fifth domain", in which a state exercises its sovereignty authority through measures recognized or regulated by international and national law.

Second, cyberspace is treated as a unique virtual environment with features that have a profound impact on the protection of state sovereignty over traditional territories. Therefore, legal measures are required to prevent and punish cyberspace abuses that violate the sovereignty and security of other states. The International Telecommunication Union (ITU 2010) defines "cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and the organization's and user's assets". In short, cyberspace is a connected, flexible, and open virtual space that is unrestricted by physical borders between states. States have the sovereign authority to control and protect their territories against intrusion, occupation, and expropriation of the information spheres under their jurisdiction (Tran D.Q. 2015). The fact, however, demonstrates that the state is not the only entity that governs cyberspace; any individual or organization may participate and establish its own space through a website,

blog, or Facebook account. Reality has demonstrated that anyone can construct a "virtual living space" in the cyber environment, and Internet users can actively engage in political, social, and e-commerce forums. Their words or actions can have uncontrollable positive or negative consequences in both the virtual and physical realms. Legislators agree, from the standpoint of national security, that states can impose restrictions to prevent non-state actors from perpetrating acts that threaten or violate state sovereignty in both physical and cyber spaces. However, there are still debates regarding the legality, necessity, and proportionality of these restrictions on human rights in cyberspace in order to defend state sovereignty and cybersecurity. This article raises the question of whether legal measures taken by a state to defend its sovereignty affect or violate the human rights of Internet users in cyberspace. The analysis that follows explains, first, the concept of human rights online, specifically the right to free speech in cyberspace, and, second, preservation of state sovereignty under human rights laws.

3. Conceptualizing Online Human Rights

Humans are the primary protagonists in the creation and operation of cyberspace, specifically the social media channels that enable individuals to participate and interact. Any individual can play a pivotal role in establishing and disseminating information and knowledge, which is the basis for a thriving, accessible information society. In addition, it is a forum that allows people to participate regardless of their nationality, ethnicity, gender, race, or political orientation so that they can discuss political, economic, cultural, and social issues, etc. The number of individuals using the Internet and social media has increased each year since Internet access became ubiquitous. Interactions and connections between users in cyberspace have both positive and negative effects on national and human security in the physical world. In terms of national security, it has been demonstrated that states and top leaders are most susceptible to attack by statements and posts on social media and blogs containing disinformation or political hate speech that calls for the overthrow of governments or violates the dignity of communities, states, and leaders. Governments are aware of the critical need to reduce and prevent online political hate speech and violent incitement against them.

Regarding human rights, Hamelink C. (2017) noted that an increasing reliance on vulnerable and error-prone digital systems is also causing cyberspace-related social risks to human security. The "cyberization" of daily life, which reinforces current tendencies toward high-speed, robot-centric societies, is also a risk factor; therefore, freedom in cyberspace must also be protected. His claim recalled the assertion of the UN Human Rights Council (2012) that "the same rights that people have offline must also be protected online". The same rights mean "the right to freedom of opinion and expression that includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers" as indicated in Articles 19 of the UDHR and ICCPR. Particularly, the UN Human Rights Council emphasized how useful the Internet is for enforcing freedom of expression and other human rights and it decided:

> "[t]o continue its consideration of the promotion, protection, and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as how the Internet can be an important tool for development and for exercising human rights, in accordance with its program of work" (UN Human Rights Council 2012:para5).

Big technology companies, social media on one side, and law enforcement state agencies on the other side, argue intensely over the right to freedom of expression in cyberspace. Social media platforms are currently being exploited to promote extremism and intolerance.

Each state has the authority to issue legislation governing the right to free expression and cybersecurity. The challenge that states face is how to strike a balance between the preservation of individual freedom of expression and the maintenance of state sovereignty and national security in cyberspace in the face of disinformation and malinformation that threaten to topple governments.

Vietnam is not immune to the issue. In response to worries about the negative impact of the Internet and social media on politics, national security, and social order, the nation has passed a series of laws that limit the abuse of freedom of expression. The following sections look at the legal limitations on free expression put in place to safeguard cybersecurity and state sovereignty. The comparable framework to existing Vietnamese laws is one of the two criteria for determining the necessity and proportionality of the restrictive measures outlined in Articles 19 and 20 of the ICCPR.

4. Legal Ground for Protection of the Right to Freedom of Expression in Vietnam

Before Vietnam officially joined the United Nations in 1997 and became a member of the ICCPR in 1982, the right to freedom of expression was enshrined in the first Constitution of the Democratic Republic of Vietnam in 1946 and repeated in subsequent Constitutions promulgated in 1959, 1980, and 1992. The most inclusive provision is Article 25 of the 2013 Constitution (as amended by the 1992 Constitution), which states that "citizens have the right to freedom of expression and freedom of the press, as well as access to information, the right to assembly, the right to association, and the right to demonstrate. The exercise of these rights will be governed by laws." (VN National Assembly 2014).

The 2016 Press Law defines freedom of expression specifically as the right to hold opinions, and Article 11 provides a list of topics on which individuals have the right to express themselves:

> "[t]o expression of their opinion on domestic and international affairs; to contribution of opinions on the formulation and implementation of the lines, guidelines, and policies of the Party and laws of the State; and to contribution of opinions, criticisms, recommendations, and complaints and

> denunciations through the press to Party organizations, state agencies ... other organizations, and individuals".

This provision concentrates more narrowly on the right to freedom of expression without incorporating three other aspects of the right "to seek, receive and impart information and ideas through any media and regardless of frontiers" as stated in Article 19 of the Universal Declaration of Human Rights ('UDHR') (UN Human Rights 1949). Vietnam promulgated the 2016 Law on Access to Information to completely realize the meaning of Article 19 of the UDHR. People have the right to access information, unless it must be kept secret to safeguard national defense and security, social order and safety, social ethics, and public health. State agencies and related organizations are responsible for providing information to citizens upon request in a timely, transparent, and accessible manner, in accordance with the procedures outlined by the laws. The right to access information will assist citizens in gaining a greater understanding of domestic affairs, allowing them to express their opinions objectively and thoroughly on matters of concern. The relationship between the right to information and the right to freedom of expression increases the value of the latter because citizens have access to political news and can participate in political discourse. When Vietnam wishes to perfect the socialist rule of law state, this is the foundation for promoting democratic processes and institutions.

The free Internet access policy allows Vietnamese citizens to create private blogs and sign up for social networking accounts in order to interact with the rest of the world. As of July 2022, NapoleonCat (2022) data indicated that there were 84,919,500 Facebook users in Vietnam (representing approximately 83% of the population). The vast majority of social interactions and public voices can be found on this social media platform. Moreover, there are a large number of users on LinkedIn, Instagram, Messenger, etc. In addition, Vietnamese law does not mandate that individuals use their names when creating websites or blogs.

The privacy of individuals is protected and respected, with the exception of situations in which a competent state agency requests a social networking service provider to disclose the personal information of users who are engaged in unlawful, terroristic, or criminal activity (The Government of Vietnam 2023). Article 26 of Decree 72 stipulates that individuals who utilize their website are free to disclose any information and are exclusively responsible for its content (The Government of Vietnam 2013). It confirms that Vietnamese regulations provide citizens with unrestricted Internet access and the freedom to sign up for either domestic or international social networking services without permission[6]. However, Article 26 of Decree 72 allows Vietnamese authorities to block pages that encourage and incite acts of war and violence against the State and the Communist Party, or that divide national solidarity, disseminate pornographic content, or insult the honor and dignity of the country's leaders and individuals (The Government of Vietnam 2013).

[6] According to Vietnam's Human Rights Report for the Third ICCPR in 2017, individuals can access 75 online foreign TV channels such as CNN, BBC, VOA and AP [Section 184].

5. Imposing Restrictions on Online Freedom of Expression under Vietnamese Law

Human rights in general and freedom of expression in particular are not exclusive rights; they may be restricted by law if necessary. Article 14 of the 2013 Constitution stipulates that "human rights and citizen rights may be limited as prescribed by a law in case of necessity for reasons of national defense and security, social order and safety, social morality, and community well-being." In addition, Article 15 of the 2013 Constitution stipulates that "the exercise of human rights and citizen rights may not infringe upon state interests or the lawful rights and interests of others" (VN National Assembly 2014).

Article 8 of the 2018 Cybersecurity Law prohibits acts related to expression in cyberspace and provides legal sanctions applicable to threats to national security and social order based on constitutional restrictions. Particularly, Article 8 prohibits deceiving, manipulating, training, or drilling people to break up the state, distorting national history, denying national revolutionary achievements, dividing national solidarity, committing offenses against religion, gender discrimination, or racist acts, disseminating false or misleading information for the purpose of gaslighting the people, or causing damage to the socio-economic system (VN General Assembly 2018).

Next, Article 16 of the 2018 Cybersecurity Law (VN General Assembly 2018) specifies in greater detail the prohibited content that Internet service providers, social network service providers, and competent state agencies are authorized to prevent and handle, including:

(i) Information containing propaganda against the government. For example, distortion or defamation of the government; psychological warfare; inciting an invasive war; causing division or hatred between ethnic groups, religions, and people of all countries; insulting the Vietnamese people, the national flag and emblem, anthem, leaders, and national heroes;
(ii) Information with content that incites rioting, disrupts security, or causes public disorder, such as calling for, mobilizing, inciting, threatening, or causing division, conducting armed activities, or using violence to oppose the administrative authorities of the people;
(iii) The dissemination of information that demeans, smears, or degrades the honor, reputation, and dignity of others. For example, providing fabricated and false information that violates the honor, reputation, and dignity of others, as well as the rights and legitimate interests of other organizations and people; and
(iv) Information containing content that violates economic management orders. For instance, providing fabricated and false information about products, commodities, currency, … causing harm to socioeconomic activities by gaslighting the public.

Article 9 of the 2018 Cybersecurity Law stipulates that users who violate Vietnam's cybersecurity law are subject to administrative and criminal penalties. In contrast, it

prohibits government agencies from blocking information in cyberspace if Internet users do not violate the stipulations (VN General Assembly 2018). The question is whether the justifications for the prohibition of the right to freedom of expression in cyberspace under Vietnamese law are compatible with paragraph 3 of Articles 19 and 20 of the ICCPR (UN General Assembly 1966). The solution is provided in the analysis below.

Regarding freedom of expression in a liberal society, Fish S. (1994) argued that there is no such thing as "free speech". These words are merely terms used to draw attention to a specific form of human interaction. They do not imply that speech should never be restricted. The viewpoint of Fish S. is a reaffirmation of the limitations imposed on freedom of expression in Article 19 (3) of the ICCPR, which states:

> "The exercise of the rights .... entails special duties and responsibilities. Therefore, it may be subject to certain restrictions, but only those prescribed by law and necessary: (a) for the protection of the rights and reputations of others; (b) for the protection of national security, public order, or public health" (UN General Assembly 1966).

Evidently, the ICCPR authorizes states to impose restrictions on freedom of expression for the legitimate purposes of protecting "the rights or reputations of others" or "national security, public order, public health, and morals". Article 20 of the ICCPR also prohibits citizens from engaging in "propaganda for war or advocacy of national, racial, or religious hatred, incitement to discrimination, hostility, or violence." (UN General Assembly 1966). Subsequently, General Comment No. 34 of the UN Human Rights Committee specifies three conditions for determining whether state-imposed restrictions comply with Articles 19 and 20 of the ICCPR, based on the ICCPR's fundamental provisions.

> First, "the restriction must be provided by law which may "include laws of parliamentary privilege" and "laws of contempt of court";
> Second, "the legitimate grounds for restriction is that of respect for the rights or reputations of others (which relates to other persons individually or members of a community) and of protection of national security or of public order, or of public health or moral"; and
> Third, "the restriction must be necessary and proportionate by addressing a direct connection between expression and the threats to national security, public order, public health or morals; and rights and reputations of others" (UN Human Rights Committee 2011:paras24-29-33).

The enactment of restrictive or prohibitive regulations on the right to freedom of expression requires legitimate reasons to explain the correlation between the necessity of restrictive or prohibitive measures and the threat level and potential for harm that utterances pose to an object or person. Therefore, empowering states to impose restrictions on the right to freedom of expression simultaneously entails their responsibility and accountability for determining which expressions and behaviors are deemed menacing and harmful. All prohibited speech and conduct must be specified in the laws. The ICCPR requires states

to "ensure that the invocation of national security, including counterterrorism, is not used arbitrarily or unjustifiably to restrict the right to freedom of opinion and expression" (UN Human Rights Council 2009:para5).

With reference to Articles 8 and 16 of the 2018 Cybersecurity Law, Vietnam relies on two approaches comparable to European legislative methods to prescribe restrictions on human rights. The first is the approach of exclusion from the protection of the law, including the prohibited acts in cyberspace specified in Article 8. The second is to impose restrictions on the contents of expression, including harmful information that should be prevented and dealt with under Article 16. Clearly, the National Assembly enacted the 2018 Cybersecurity Law prohibiting conduct in cyberspace that satisfies the first requirement of General Comment No. 34.

Assessing the legitimate grounds for restrictions in Vietnamese law as outlined in the second condition of General Comment No. 34, it is evident that Article 15 of the 2013 Constitution covers the obligation of citizens with regard to freedom of expression. The 2018 Cybersecurity Law also meets this requirement. Particularly, restrictions may be imposed on a citizen if the competent authority can demonstrate that an Internet user compromises the rights and interests of the state and other individuals.

Concerning the necessity and proportionality of restrictions on freedom of expression in cyberspace indicated in the third condition of General Comment No. 34, it is evident that the 2017 Criminal Code (VN National Assembly 2017) provides two distinct provisions that should be applied to a suitable case. Article 117 may apply to serious violations of freedom of expression. A user of the Internet may, for instance, utilize social media or websites to distribute and propagate anti-state information and materials. In contrast, Article 331 applies if an Internet user abuses freedom of expression and other democratic freedoms to violate the interests of the state and the legitimate rights and interests of others without intending to oppose the state. The issue at hand is whether the criminal sanctions imposed for violations of expression under Articles 117 and 331 can be evaluated as "proportionality," as described in General Comment No. 34.

As Cianciardo J. stated, many constitutional courts, whether common law or civil law, apply the principles of proportionality "as a procedure that aims to guarantee the full respect of human rights (or fundamental rights) by the state." (2010:177). He claimed that "the principles of reasonableness" in the doctrine of the United States Supreme Court, "reasonable justification" in the Federal Supreme Court of Switzerland, or the standards of "non-arbitrariness" in the German Constitutional Court are all examples of proportionality (2010:178). The conceptual intersection of the justificative distinctions is that proportionality consists of three sub-principles: sufficiency, necessity, and proportionality in the restricted sense. In contrast, the French legal system views them as a "balance between costs and benefits" (Cianciardo J. 2010:180). In STC 66/19515[7],

[7] Constitutional Court of Spain. Case of ECLI:ES:TS 195:66, Judgment of May 8, 1995, para. 5. Available at: http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/2920 (accessed 10 June 2022).

a judge of the Spanish Constitutional Court upheld that a restriction of a right is "proportionate, in the strict sense, that is weighted or balanced because it derived from benefits or advantages for the general interest than harm to other goods or values in conflict," thereby supporting France's position. Similarly, the Inter-American Commission on Human Rights explained:

> "[o]n evaluating the proportionality of a restriction to freedom of expression on the Internet, one must weigh the impact that the restriction could have on the Internet's ability to guarantee and promote freedom of expression against the benefits that the restriction would have in protecting the interests of others" (2013:para54).

With reference to this explanation, the 2018 Cybersecurity Law of Vietnam satisfies the first sub principle of "adequacy" from the perspective of common law system judges. The legislators feel that with the help of the law's restrictive measures, the objective of protecting state sovereignty and security, public order, and the legitimate rights and interests of others can be attained.

In addition, Article 5 of the 2018 Cybersecurity Law specifies a variety of applicable measures for protecting cybersecurity and state sovereignty against violations. State authorities can, for instance, block, suspend, or terminate cyber connections or delete prohibited data. In addition, they have the ability to initiate, investigate, prosecute, and adjudicate administrative or criminal cases in cyberspace (VN National Assembly 2018). This article responds explicitly to the second sub-principle of "necessary" regarding whether the implementation of restrictive measures aids lawmakers in achieving their intended objectives.

In short, state authorities must provide "reasonable justification" for the proportionality of a sanction. The choice between administrative or criminal punishment for a violation must be based on the motivation and severity of the violation's consequences. This topic is examined in greater depth in the subsequent section.

This article examines the provisions of Vietnamese law regarding restrictions on freedom of expression in cyberspace from the perspective of the civil law system. Similar to the preceding explanation, the 2018 Cybersecurity Law clarifies the meaning of the terms "general interests" or "other interests" mandated by law to protect three described targets as outlined in Article 19 (2) of the ICCPR.

First, it serves the interests of the state. State sovereignty and security are the main justifiable goals that states cite for preventing political hate speech and incitement to riots or terrorism.

As previously discussed, Clause 2 of Article 14 of the 2013 Constitution states that "human rights and citizen rights may be restricted when necessary for national defense and security" (VN National Assembly 2014). In the context of cyberspace, cybersecurity protection ensures state sovereignty. Cybersecurity is defined in Article 3 of the 2018

Cybersecurity Law as "the assurance that activities in cyberspace will not harm national security, social order and safety, or the legal rights and interests of agencies, organizations, and individuals" (VN National Assembly 2018). Therefore, the acts and content specified in Articles 8 and 16 of the 2018 Cybersecurity Law are viewed as hazards to state interests and must be restricted or prohibited.

According to the Siracusa Principles on the Limitations and Derogation Provisions in the ICCPR, "national security may only be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation, its territorial integrity, or its political independence against the use of force or the threat of force" (UN 1984). Specifically, Principle 2(a) of the Johannesburg Principles provides a more detailed explanation of the protection of national security interests with respect to the restrictions on freedom of expression mentioned in Article 19(2) of the ICCPR. That is:

> "[a] restriction sought to be justified on the ground of national security is not legitimate unless its genuine purpose and demonstrable effect is to protect a country's existence or its territorial integrity against the use or threat of force, or its capacity to the use or threat of force, such as incitement to violent overthrow of the government" (UN 1996).

Clearly, the restrictive provisions of Vietnamese law are consistent with the interpretation of General Comment No. 34 and other relevant international instruments.

Second, it serves the public good. Consequently, the law must protect the public order, public health, morality, rights, and reputation of others. The proliferation of hate speech and libel on social networks has eroded the social foundations of national cultural values and community cohesion. As a result of empathizing with the targeted individual, there is a potential for social instability and evil. Article 16 of the 2018 Cybersecurity Law thus already specifies the prohibited content in cyberspace.

Third, it is in the economy's interest. The 2018 Cybersecurity Law mandates the avoidance and elimination of disinformation that may threaten the economic safety and security of the financial and banking sectors, commerce, and securities.

According to Clause 2 of Article 19 of the ICCPR, commercial disinformation is not restricted. However, the United States and the European Union limit the right to free speech by prohibiting "commercial speech that is false, misleading, or promotes an illegal product or service." Even if it falls in none of these categories, the government may regulate it more than it may regulate fully protected speech" (Ruan A.K 2014).

Theoretically, legal restrictions on the right to free expression in cyberspace are required to balance public and private interests in a given circumstance. In practice, however, a state must demonstrate that "there is a pressing social need for it, that it pursues a legitimate aim, and that it is the least restrictive means of achieving that aim" and that "when a State party imposes restrictions on the exercise of freedom of expression,

these may not put the right itself at risk" (Inter- American Commission on Human Rights 2013:para21).

In general, Vietnamese laws do not strictly forbid hate speech if they do not contain phrases that call for bloodshed, plot to overthrow the government, disturb social order, or undermine national unity; defame others' honor; unlawfully endanger their safety; discriminate on the basis of gender or race; or threaten economic security. The general political, religious, or social comments or criticisms of the corruption are neither threatening nor destructive, are not viewed as inciting enmity or violence, and are not illegal. The provisions on the application of technical and legal measures to restrict freedom of expression in cyberspace are consistent with General Comment No. 34 and both the common law and civil law systems from a theoretical human rights perspective. Article 4 (2) of the 2018 Cybersecurity Law emphasizes the "close combination of tasks for protecting cybersecurity and information systems critical for national security with tasks for socio-economic development, providing human rights and civil rights, and enabling agencies, organizations, and individuals to conduct activities in cyberspace".

6. Legal Ground for Handling Violations for Online Freedom of Expression in Vietnam

The 2018 Cybersecurity Law specifies two categories of technical and legal measures for dealing with illegal acts and information that threaten Vietnam's national sovereignty and security, public order, and the legitimate rights and interests of others in cyberspace:

To defend cyberspace, authorities can employ technical measures such as information barring and filtering. They predominantly request that online publishers and disseminators remove any content that violates Article 16 of the 2018 Cybersecurity Law. The competent authorities have the authority to collect information or monitor Internet users if there is evidence of a severe violation of national security, the legitimate rights and interests of others, or the disruption of social order and safety. Article 1(10) of Decree 27 asks service providers for social networks or the Internet to collaborate with specialized, competent agencies in order to prevent and address violations. Foreign social network providers and websites such as Facebook, Google, YouTube, and Microsoft must establish a computing facility in Vietnam to administer data generated by Vietnamese Internet users. In accordance with the information safety and security regulation, this requirement seeks to verify, archive, and provide information from social media upon request from the state authority (The Government of Vietnam 2018).

It is argued that this regulation stems from the state sovereignty right in cyberspace, which holds that the State has the right to manage and protect domestic user data in Vietnam to prevent potential threats to Internet users' rights, and simultaneously guarantee the safety and security of cyber information under its jurisdiction in accordance with international agreements, of which Vietnam is a signatory. In support of their views on the relationship between state sovereignty and cyberspace, the Vietnamese and other governments are

cognizant of the immense value of information in the digital age. Big Data affords its owners (whether they are states or non-state actors) numerous competitive advantages and potent positions. Many governments are concerned about the administration of citizen databases on international social networking sites. Foreign companies can simultaneously comply with Vietnamese laws and safeguard the privacy of Internet user data and free speech in cyberspace (The Government of Vietnam 2023).

The state authorities must establish reasonable and proportionate mechanisms and measures to protect cybersecurity and guarantee the right to freedom of expression and uncensored access to information online, provided that the information does not violate Articles 8 and 16 of the 2018 Cybersecurity Law. It is acknowledged that the realization of the right to freedom of expression must be distinguished from the intent and impact of the information that users post, share, and disseminate online regarding national security, public order, public health, and social morality. In a democratic society, the equilibrium between state, society, and community interests and individual liberties is a legitimate requirement. However, there is not always harmony between these two interests. If it desires to maintain public order and national security, the government must swiftly combat overly permissive online behavior. Consequently, the state must take drastic measures promptly to prevent potential transnational cybercrimes and cyberterrorism against international peace and security as well as domestic state sovereignty and security.

In addition to technical measures, Vietnam imposes administrative or penal sanctions on Internet users who violate the law under certain conditions. In accordance with Article 99 of Decree 15, uploading, transmitting, or using images of the map of Vietnam that do not accurately depict or distort its sovereignty is punishable by a fine (The Government of Vietnam 2020). In contrast, Articles 117 and 331 of the Criminal Code of 2017, which are more stringent, outline punishments for numerous violations of the right to freedom of expression.

Making, preserving, and disseminating information, materials, and other items to oppose the state is punishable under Article 117 of the 2017 Criminal Code. This provision pertains, for instance, to an offender who uses social media to propagate false information or disinformation for the purposes of "defaming the Government of Vietnam," "gaslighting the people," or "causing psychological warfare." These violations are categorized as "crimes that compromise national security".

In case 34/2019/HS-ST[8] of Duong Thi L., the People's Court of Dak Nong Province issued the judgment accusing her of creating 21 Facebook pages and luring innocent or dissatisfied people into an organization funded by an overseas organization, to give comments, publish articles, photos, and videos that represent historical facts and

[8] People's Court of Dak Nong Province (2019), Case of Prosecutor v. Duong Thi L. Judgement, 23 September 2019. Available at: https://congbobanan.toaan.gov.vn/2ta347817t1cvn/chi-tiet-ban-an (accessed 3 June 2022).

the Party and State's policies, incite protests, and instill fear and insecurity among the general population. This conduct was judged to impair both the Community Party of Vietnam and national security, and she was acting out of self-interest. Consequently, the judge sentenced the defendant to eight years in prison after finding that she had "spread information, materials, and items opposed to the State Socialist Republic of Vietnam" (The People's Court of Dak Nong Province 2019:para1).

In addition, Article 331 of the 2017 Criminal Code stipulates punishments for the offense of exploiting democratic freedoms to harm the interests of the State and the legitimate rights and interests of organizations and individuals. The law stipulates that anyone who abuses the freedom of expression, freedom of the press, freedom of religion, freedom of association, and other democratic freedoms to infringe upon the interests of the State, lawful rights and interests of organizations, and citizens is subject to a warning, public labor without custodians for up to three years, or imprisonment for six to thirty-six months. If the offense has a negative impact on social security, order, or safety, the offender is sentenced to between two and seven years in prison. It appears that Article 331 is distinct from Article 117 in that violations are classified as "crimes against the administrative management order".

In case 94/2019/HS-PT[9] of Quach Nguyen Anh K., the Appeal Court, based on the Department of Information and Communications of Can Tho province's assessment of "Quach Nguyen Anh K.'s" Facebook account, accused him of "abusing the right to freedom of expression to write, post, and comment on information with the intent to oppose, propagate, incite, and spread reactionary thoughts against the State". The judge determined that:

> "the defendant's actions were dangerous and directly violated the administrative order of the State; affected the leadership, legitimate rights, and interests of the Communist Party of Vietnam; harmed the interests of the State of the Socialist Republic of Vietnam; and disrupted political security, social order, and public safety" (People's Court of Can Tho City (2019:para2).

In the verdict, the judge did not explain Quach Nguyen Anh K.'s intent in exploiting democratic freedom to infringe on the interests of the State and other individuals, or what he hoped to gain. The court's attribution was limited to what was violated, such as administrative order management, the prestige of the Communist Party's leadership, and State interests. In assessing the degree to which the defendant's actions posed a threat to society, the judge did not consider the extent of actual harm, but nonetheless decided to sentence him to six months in prison under Article 331.

[9] People's Court of Can Tho City (2019), Case of Prosecutor v. Quach Nguyen Anh K. judgment dated August 28, 2019. Available at: https://thuvienphapluat.vn/banan/ban-an/ban-an-942019hspt-ngay-28082019-ve-toi-loi-dung-cacquyen-tu-do-dan-chu-xam-pham-loi-ich-cua-nh-105248 (accessed 10 June 2022).

In this case, it can be concluded that defendant Quach Nguyen Anh K. conducted prohibited acts on social media similar to the acts committed by defendant Duong Thi L. But he did not have the motivation of inciting and provoking demonstrations to destroy the State and did not look for gain. It appears that Article 117 of the 2017 Criminal Code aims at offenses to oppose and weaken the State while those in Article 331 of the 2017 Criminal Code are interpreted differently depending on the specific act as abuse of 'democratic freedoms' to infringe upon prohibitions or restrictions without an intention to overthrow the State set out in the 2018 Cybersecurity Law.

During conversations with the judge (H.D) of the Supreme Court in Hanoi, the judge disclosed that there is no legal document that explains the content of Article 331 in greater detail. In practice, justices frequently refer to and consider certain factors when determining the scope and repercussions of a violation of freedom of expression. The first is a specific provision of applicable legal documents, including the Cybersecurity Law, Criminal Code, Civil Law, and National Security Law. The second is the political and social context in which the offender posts and distributes deceptive information that misrepresents, smears, or defames the government's policies and plans of action. For example, if a defendant intentionally commits a violation on the anniversaries of significant national events, during National Assembly elections, or during the Communist Party of Vietnam's congresses, the violation is frequently viewed as more detrimental than on other days. Third is the general cognizance of moral values, cultural traditions, and national customs among the populace. For instance, the local community is likely to object to any statement or action that disparages the images of national heroes or caricatures of the Communist Party or state leadership. In Oriental cultures, these are regarded as disrespectful. The fourth factor is the severity of the offense's impact on national security and social order.

False, fabricated, and defamatory content or hate speech posted or shared on electronic sites or social media has a wider diffusion. Internet users are susceptible to and drawn to information that induces greater psychological vulnerability than conventional media. Therefore, the courts view cyberspace expression violations as detrimental to society and punish them with the appropriate legal measures. The Vietnamese judge's approach is relatively consistent with the Supreme Court of Canada's interpretation of proportionality in *R v. Oakes*[10], which states that "in order to determine the extent to which free speech is legally protected, judges must resolve contentious questions about the conception of democracy most appropriate to the legal system in which they hold office" (Supreme Court of Canada (1986:paras69-70).

However, it is questionable that certain terminology in the provisions of the 2018 Cybersecurity Law and the judgment of Quach Nguyen Anh K. is imprecise and non-quantifiable. For example, how to define acts that "distort history and deny revolutionary

[10] Supreme Court of Canada (1986), Case R v. Oakes. Judgment dated February 28, 1986. Available at: https://scccsc.lexum.com/scc-csc/scc-csc/en/item/117/index.do (accessed 5 September 2022).

achievements" or "false information that causes confusion among the people, damage to socio-economic activities, and obstructions to the operation of state agencies" or acts that "disrupt national fine customs and traditions". Similarly, the content of Article 331 is viewed as overly broad and ambiguous, which raises a number of controversies due to the absence of a definition of "abuse of the right to freedom of expression" and the extent of infringement on the state's interests or the legitimate rights and interests of others. Lacking legal interpretation by the National Assembly's Standing Committee[11] relating terminologies, it is a challenge to human rights if the enforcement agencies rely arbitrarily on their own experiences to assess the dangerous degree of threat or harm derived from political hate speeches and anti-state information.

For adjudicating crimes committed in cyberspace that fall under either Article 117 or Article 331 of the 2017 Criminal Code, the courts must invoke the provisions outlined in the 2016 Press Law and the 2018 Cyber Law if they present more cogent, legally supported arguments. The courts must also consider the actuality of the infringed objects and the objective manifestation of the criminal offenses in order to determine a criminal punishment proportional to the level of danger posed by said offenses.

In reference to the case of Duong Thi L., the judge argued that "the accused's crimes violated the ideological and cultural security of the Socialist Republic of Vietnam, specifically the stability of spiritual life and the unity of the political foundation, as well as the belief of the masses in the political system and socialist institutions, thereby undermining the power of the people's government", and she was acting out of self-interest (The People's Court of Dak Nong Province 2019:para2).

Without an evaluation of the measurable level of danger or the anticipated negative impact on the targeted objects or individuals, such a claim is hardly convincing. The judge's argument appears to be based on subjective and political conjecture rather than a quantitative evaluation of the infringed subjects. Consequences would result if judges arbitrarily provided interpretations of a provision containing political terms or words rather than legal terms based on mere conjecture of potential violations or if they provided hypothetical circumstances derived from the interpretations of a specialized agency regarding facts that are not clearly defined in order to convict and impose liability on violators (Inter - American Commission on Human Rights 2013:para62). If that happened, the court would be deemed to have taken disproportionate measures restricting freedom of expression, as indicated in the Joint Declaration on Freedom of Expression and Response to Conflict Situations that:

> "All criminal restrictions on content – including those relating to hate speech, national security, public order and terrorism/extremism – should conform strictly to international standards, including by not providing

[11] According to Art. 74 (2) of the 2013 Constitution of Vietnam, the Standing Committee of the National Assembly is empowered to give interpretations of the Constitution, laws, and ordinances.

special protection to officials and by not employing vague or unduly broad terms" (UN Human Rights 2015:para3).

To avoid non-transparent regulations, it is asserted that Vietnamese legislators should provide a precise and measurable definition of terms containing political implications. Aside from there, they should provide a clearer explanation of the contents outlined in Articles 8 and 16 of the 2018 Cybersecurity Law and Articles 117 and 331 of the 2017 Criminal Code in order to confirm compliance with the requirement of proportionate technical or legal measures imposed on anti-state expression by Articles 19 and 20 of the ICCPR. According to Anja Mihr (2016:314), "without a commonly accepted 'cyber-constitution' based on human rights and the rule of law based on effective measures and mechanisms to enforce these rules, internet - citizens or citizens 2.0 of this world will struggle to protect and enjoy their human rights in cyberspace." The more transparent the regulations are, the more they will prevent state agencies from restricting citizens' freedom of expression in cyberspace in the name of state sovereignty and security.

Conclusion

The widespread use of social networking sites and the Internet has promoted social interactions between the Vietnamese government and people, as well as between people in the community, and ideas and viewpoints about democracy are widely exchanged on social media. The 2013 Constitution has demonstrated that Vietnam has fully embraced and more explicitly translated the human rights provisions of both the UDHR and ICCPR into specific domestic laws aiming at the comprehensive protection of human rights. It has also strengthened the duties and responsibilities of state authorities to ensure a more transparent exercise of human rights.

In terms of the restriction on the right to freedom of expression in order to protect state sovereignty in cyberspace, this article confirms that Vietnamese law has largely complied with the conditions outlined in Articles 19 and 20 of the ICCPR and the justifications in General Comment No. 34. This article also discusses the maintenance of complex measures to control, restrict, and regulate online information, illustrating Vietnam's reluctance to permit complete Internet access. Similar to other states, Vietnam faces threats and damages posed by terrorism and violent expression in cyberspace against state sovereignty and security, politics, the economy, and society. This restriction is not extraordinary. However, Vietnam may violate the provisions of the ICCPR if administrative or criminal sanctions are applied disproportionately to restrict the right to freedom of expression without reasonable justification. For supporting judges to make stronger, more convincing arguments about Articles 117 and 331 of the 2017 Criminal Code, the relevant political terms and contents outlined in the 2018 Cybersecurity Law must continue to be uncovered in order to provide a more precise and jurisprudential interpretation that ensures a balance between the protection of state sovereignty and human rights in cyberspace.

References

ANJA MIHR (2016), "Cyber Justice: Cyber Governance through Human Rights and a Rule of Law in the Internet", 13 *US - China Law Review*, 314–336.

BARLOW, J. (2019), "A Declaration of the Independence of Cyberspace", 18 *Duke Law & Technology Review. 5-7.* Available at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1337&context=dltr (accessed 19 February 2021).

BETZ D. AND STEVENS T. (2011), "*Cyberspace and the State: Toward a Strategy for Cyber – Power*", 1st ed. Routledge.

BINARK, M. AND ÇOMU T. (2012), "Using Social Media for Hate Speech is not Freedom of Expression", Available at: https://yenimedya.wordpress.com/2012/01/31/using-social-media-for-hate-speech-is-not-freedom-of-expression (accessed 5 May 2021).

BRITANNICA (2020), "Sovereignty". Encyclopedia Britannica. Available at: https://www.britannica.com/topic/sovereignty (accessed 5 July 2021).

CIANCIARDO, J. (2010), "The Principle of Proportionality: The Challenges of Human Rights", 3. *J. Civ. L. Stud.* 177. Available at: https://digitalcommons.law.lsu.edu/cgi/viewcontent.cgi?article=1028&context=jcls (accessed 15 May 2022).

C NGUYEN AND D NGUYEN (2022), "Trends in Cyberattacks and Cybercrime in Vietnam in 2021 and Forecasts for 2022". Available at: https://antoanthongtin.vn/chinh-sach---chien-luoc/xu-huong-tan-cong-mang-va-toi-pham-mang-tai-viet-nam-nam-2021-va-du-bao-nam-2022-107805 (accessed 5 May 2023).

COUNCIL OF EUROPEAN (1997), "Combating Hate Speech". Available at: https://www.coe.int/en/web/combating-hate-speech/background-document (accessed 7 May 2023)

EDWARD, A. (2011). "Jean Bodin on Sovereignty." *Republic of Letter: A Journal for the Study of Knowledge, Politics, and the Arts* 2, no.2. Available at: http://rofl.stanford.edu/node/90 (accessed 3 March 2022).

ELIZABETH, A. OJI AND M.V.C OZIOKO (2011), "Effect of Globalization on Sovereignty of State", *African Journal Online*, 2, 256-270. Available at: http://www.ajol.info/index.php/naujilj/article/view/82410 (accessed 19 May 2022).

ESTHER DYSON, et al. (1994), "Cyberspace and the American Dream: A Magna Carta for the Knowledge Age" (Release 1.2), 12 (3), *The Information Society*, 295-308. Available at: http://doi:10.1080/019722496129486 (accessed 19 May 2022).

FISH, S. (1994), "*There's No Such Thing as Free Speech…and It's a Good Thing too*", New York. Oxford University Press.

HATHAWAY, M. AND KLIMSBUR, A. (2016), "Preliminary Considerations: On National Cyber Security" in Alexander Klimburg, *National Cyber Security Framework Manual*, Tallinn: Nato CCDCOE Publication (2016). Available at: https://www.

belfercenter.org/sites/default/files/files/publication/hathaway-klimburg-nato-manual-ch-1.pdf (access 27 March 2022).

HAMELINK, C. (2017), "Human Rights in Cyberspace" in Leen d'Haenens (ed.), *Cyberidentities – Canadian & European Presence in Cyberspace*, Ottawa, University of Ottawa Press, 31-46. Available at: https://books.openedition.org/uop/1372 (accessed 7 November 2022).

HOBBER, T. (1651), "Leviathan or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civil", Available at: http://name.umdl.umich.edu/A43998.0001.001 (accessed 10 May 2023).

HOWARD, N.P & HUSSAIN, M.M (2011), "The Upheaval in Egypt and Tunisia: The Role of Digital Media", *Journal of Democracy,* 22 (3), 35-48.

INTER-AMERICAN COMMISSION ON HUMAN RIGHTS (2013), "Freedom of Expression and the Internet". Available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf (accessed 10 June 2022).

ISO/IEC (2012), "Information technology – Security Techniques – Guidelines for Cybersecurity". Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed 5 May 2022).

ITU (2010), Definition of Cybersecurity. Available at: http.//itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx (accessed 17 March 2021).

КОРОВИН В. (2014). *Мретья М□ровая Сетевая Война.* Translated from the Russian by Phan, L. (2017) Hanoi: Youth Publishing House.

LIAROPOULOS, A. (2013) "Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction?", 12.2 *Journal of Information Warfare* 19-26.

LOTRIONTE, C. (2012), "State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights", 26 *Emory International Law Review*, 825-919.

MACHIAVELLI, N. (1532), "The Prince" Chapter VI - IX, Available at: http://www.planetpdf.com (accessed 27 May 2022).

NAPOLEONCAT (2022), "Social Media Users in Vietnam July 2022". Available at: https://napoleoncat.com/stats/social-media-users-in-viet_nam/2022/07/ (accessed 1 August 2022).

ROUSSEAU, C. (1944), "*Principes Generaux du Droit International Public"* vol 1, Paris, Éditions Á. Pedone. Tome.

RUANE, K.A. (2014), "Freedom of Speech and Press: Exceptions to the First Amendment", Congressional Research Service 7-5700. Available at: https://fas.org/sgp/crs/misc/95-815.pdf (accessed 10 July 2020).

SCHMITT, M. (ed.) (2017), "*Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*". Cambridge University Press.

SCHRIJVER, N. (1999), "The Changing Nature of State Sovereignty in *British Yearbook of International Law*, Vol 70 (1), 65 – 98. Available at: https://doi.org/10.1093/bybil/70.1.65 (accessed 5 July 2021).

TIM WU (1997), "Cyberspace Sovereignty? – The Internet and the International System", *10 Harv. J. L. & Tech*. 647. Available at: https://scholarship.law.columbia.edu/faculty_scholarship/2227 (accessed 5 July 2022).

THE GOVERNMENT OF VIETNAM (2013), Decree no. 72/2013/ND-CP on Management, Provision and Use Internet Services and Online Information. Available at: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-72-2013-ND-CP-quan-ly-cung-cap-su-dung-dich-vu-Internet-va-thong-tin-tren-mang-201110.aspx.

THE GOVERNMENT OF VIETNAM (2018), Decree no.27/2018/ND-CP on Amending a Number of Articles of Decree 72/2013/ND-CP on the Management, Provision, Use Internet Services and Online Information. Available at: https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-27-2018-ND-CP-amendments-72-2013-ND-CP-management-use-internet-services-online-information/382532/tieng-anh.aspx (accessed 5 May 2022).

THE GOVERNMENT OF VIETNAM (2020), Decree no. 15/2020/ND-CP provides penalties for administrative violations in the fields of postal services, telecommunications, radio frequency, information technology and electronic transactions. Available at: https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-15-2020-ND-CP-penalties-for-administrative-violations-against-regulations-on-postal-services/438738/tieng-anh.aspx (accessed 5 May 2022).

THE GOVERNMENT OF VIETNAM (2023), Decree no.13/2023/ND-CP on the Protection of Personal Data, Available at: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Nghi-dinh-13-2023-ND-CP-bao-ve-du-lieu-ca-nhan-465185.aspx (accessed 10 May 2023).

THE NEW YORK TIMES (2009), "Text: Obama's Remark on Cyber Security". Available at: https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html (accessed 15 July 2021).

TRẦN D.Q. (2015), "*Không gian mạng, Tương lai và Hành động*", Hà Nội, NXB Công an nhân dân.

XINHUA (2016), "Why Does Cyber Sovereignty Matter?". Available at: http://www.chinadaily.com.cn/business/tech/2015-12/16/content_22728202.htm (accessed 15 May 2022).

UN HUMAN RIGHTS COMMITTEE (2011), General Comment no.34, Article 19: Freedoms of Opinion and Expression, Available at: https://digitallibrary.un.org/record/715606?ln=en (accessed 7 March 2022)

UN HUMAN RIGHTS COUNCIL (2009), Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Available at: https://www.un.org/development/desa/disabilities/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development.html (accessed 7 March 2022)

UN HUMAN RIGHTS COUNCIL (2012), Promotion and Protection of all Human Rights, Civil, Political, Economic, Social and Cultural Rights, including the Right to Development. Available at: https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc (accessed 7 March 2022).

UN HUMAN RIGHTS (2015), Joint Declaration on Freedom and Response to Conflict Situations. Available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921 (accessed 20 August 2020).

UN (1949), Universal Declaration of Human Rights. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (accessed 5 April 2021).

UN (1984), The Siracusa Principles on the Limitations and Derogation Provisions in the International Covenant on Civil and Political Rights, Annex, UN Doc E/CN.4/1984/4. Available at: https://www.icj.org/wpcontent/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf? (accessed 17 May 2022).

UN (1996), The Johannesburg Principles on National Security, Freedom of Expression and Accession to Information, U.N. Doc. E/CN.4/1996/39 (1996). Available at: http://hrlibrary.umn.edu/instree/johannesburg.html (accessed 10 July 2022).

UN GENERAL ASSEMBLY (1966), The International Covenant on Civil and Political Rights. Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed 5 April 2021).

UN GENERAL ASSEMBLY (2018), Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement (accessed 7 March 2022).

OFFICE OF THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF (2021), "DOD Dictionary of Military and Associated Terms", as amended. Available at: https://irp.fas.org/doddir/dod/dictionary.pdf. (accessed 5 July 2022).

VN NATIONAL ASSEMBLY (2014), The 2013 Constitution of the Socialist Republic of Vietnam. Available at: https://vietnamlawmagazine.vn/the-2013-constitution-of-the-socialist-republic-of-vietnam-4847.html (accessed 15 July 2022).

VN NATIONAL ASSEMBLY (2017), Criminal Code. Available at: https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Van-ban-hop-nhat-01-VBHN-VPQH-2017-Bo-luat-Hinh-su-363655.aspx (accessed 4 August 2022).

VN NATIONAL ASSEMBLY (2018), The Cybersecurity Law. Available at: https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx (accessed 4 August 2022).

Received: 19th February 2023

Accepted: 5th June 2023