Journal of Human Rights Practice, 2022, 1–18
https://doi.org/10.1093/jhuman/huac007
Article

Article

Human Right Concerns in Vietnam's Cybersecurity Law: From International Discourse to a Comparative Perspective

Quoc-Tan-Trung Nguyen, Thi-Hong-Ninh Bui, and Hong-Thanh Phung*

Abstract

Vietnam's Cyber Security Law, which officially came into effect on the first day of 2019, is considered by the Vietnamese authorities to be an important advance of the Vietnamese legal system in catching up with new information technology issues and addressing the challenges of the Revolution 4.0. The legislation, however, did not come without opposition. Specifically, international dissatisfaction with the law was clearly articulated in January 2019 in the Universal Periodic Review—a major human rights protection mechanism under the management of the UN Human Rights Council; and also, in the Human Rights Committee hearing on Vietnam's implementation of the International Covenant on Civil and Political Rights in March of that year.

Within its limited resources, this article first tries to identify and evaluate recommendations and comments during the two events in relation to the Cyber Security Law, made by international actors including states, non-governmental organizations, and authoritative United Nations institutions. With the data, the article can then categorize three vital human rights concerns regarding the law, according to international perception. They comprise (1) the legal philosophy of national security; (2) obligations imposed on internet businesses; and (3) judicial review/remedy. Finally, the research engages in an extensive comparative analysis between these concerns and international practices to reach different conclusions on their compatibility and possible solutions.

The authors believe that constructive criticisms from the international community can be carefully garnered in order to contribute to the refinement of Vietnams cybersecurity laws in the future.

Keywords: Cybersecurity Law; human rights; UPR; Vietnam

* Quoc Tan Trung Nguyen (nguyenquoctantrung@gmail.com/trungnguyen@uvic.ca) is a PhD candidate at the University of Victoria, CA. Tel: +84 937 212 717. He currently pursues research interests including the international legal framework on the use of force, human rights and democratization; Phung Hong Thanh, Ho Chi Minh City University of Law; Bui Thi Hong Ninh, University of Economics and Finance.

1. Cyber Security Law: internal policies and external dialogues

1.1. The viewpoint of the Vietnamese authorities

The Cyber Security Law of Vietnam (hereinafter the 'VCSL') was passed on 12 June 2018 by the 14th National Assembly, with an approval rating of 86.86 per cent. It officially came into effect on 1 January 2019.

Considered one of the major legislative projects of contemporary Vietnam, the foundations of the VCSL were first established by the Vietnam Communist Party ('VCP') in Resolution No. 13-NQ/T.W., dated 16 June 2012, at the 4th Plenum of XI tenure of the Central Committee on the construction of a synchronous infrastructure system to develop Vietnam into a modern-oriented industrial country by 2020; and then by Direction No. 46-CT/T.W. of the Political Bureau on enhancing the leadership of the Communist Party to ensure security and order in the new situation; also by Direction No. 28-CT/T.W. of the Secretariat of the Party Central Committee; and finally, by Direction 30-CT/T.W. of the Political Bureau on developing and enhancing management of the digital press, social networks and other kinds of communication on the internet.

The Vietnamese government is not unfamiliar with legislation dealing with the internet and mass communication. In 2005, it issued one of the first legislative milestones, The E-Commerce Transaction Law. In 2015, the Law on Network Information Safety was enacted. However, these pieces of legislation mainly deal with the technicality of online businesses and the handling of information in the hands of private entities. Until 2018, the VCSL stood out and attracted the international community's attention since it resulted from a serious political commitment on the part of the VCP to intervening and regulating the flow of information and the behaviour of internet users and intermediate actors. Interestingly, thresholds and justifications for state intervention in the free flow of data on the internet are practically non-existent.

According to the late president of Vietnam, Tran Dai Quang, usually considered the mastermind behind the VCSL, the internet and its added-value products are inherently prone to sophisticated, cunning tricks that can cause internal divisions, infringing national interests and security. He included among the 'sophisticated, cunning tricks', posting articles with 'evil' or 'malicious' content, and offending and slandering the Party's leadership and its officials (Quang 2017). The generalizations go dangerously further by including 'activities that negatively affect' the awareness and thought of people about the leading role of the Communist Party, which means that the very practice of criticism and freedom of expression can potentially be considered unacceptable.

Due to anxiety about how people think and talk about the Communist regime online, the term 'cybersecurity' in Vietnam does not mean what it normally means around the globe.

Writing in the *Communist Journal*, the official mouthpiece of the VCP, Major General Nguyen Minh Chinh, director of the Department of Cyber Security and High-tech Crime Prevention at the Ministry of Public Security ('MPS'), referred to the National Cyber Strategy issued by the White House and to Australia's 2018 Cyber Security Law as evidence of the normality of the VCSL (Chinh 2019).

What he did not take into account, however, is that the National Cyber Strategy prioritizes the protection of American interests and way of life against the intervention of foreign cyber-attacks and manipulation. It does not intend, and would not dare to intend, to interference with the right of free speech. As the document asserts, 'Americans believed the

growth of the Internet would carry the universal aspirations for free expression and individual liberty around the world' (White House 2018: 1).

Major General Nguyen Minh Chinh did also ot account for the fact that the so-called 2018 Cyber Security Law of Australia is actually the Security of Critical Infrastructure Act, which allows the Australian government to keep a firm grip on national 'critical infrastructure', to ensure that foreign entities cannot have access to these vital assets.

In the VCSL, on the other hand, the essence of cybersecurity is public security and order on the internet, which requires the intervention of the state in patrolling and regulating people's thinking and what they say online, their identities and even their right to access the internet. This approach does fit with the post-reform concept of human rights in Vietnam: a communitarian concept focusing on economic and social rights, at the expense of political and civil rights (Bui 2014). But with the assimilation of Vietnam's human rights institutions into international standards, it is clear that such a belief will face challenges in the international arena.

Therefore, although all the Party's viewpoints are maintained, affirmed and strongly protected throughout the internal drafting process and promulgation of the VCSL, the government side of the political regime, apparently, still considers the status of the VCSL in terms of Vietnam's international commitment to human rights. The most concrete evidence for this claim is in the draft report sent by the Vietnam Government to the National Assembly, acknowledging that,

> The Cybersecurity Law will provide specialised cybersecurity measures, including a number of measures that will possibly affect human rights and the basic rights and obligations of citizens by means such as online monitoring and restriction of information. (Vietnamese Government 2017)

This line alone shows that the drafting agency in particular, and the authorities in general, have been cautious and have taken preparatory steps to guarantee that the VCSL will comply with the legal principles of human rights and international practices to a certain extent, thereby limiting criticism from other states and influential non-governmental organizations. Unfortunately, such measures did not eliminate the negative view of a part of the international community. There are several reasons to believe that ease of action and the absolute power of state agencies have been given priority over the protection of human rights in the VCSL.

1.2. The views of others: from the UPR to the ICCPR hearing

During the Universal Periodic Review ('UPR') of the UN Human Rights Council for Vietnam in 2019,[1] the VCSL was constantly challenged by representatives of many member countries and affiliated civil organizations, thus becoming one of the most criticized subjects of the review.

It is significant that the UPR is currently one of the UN's leading human rights mechanisms and receives broad media coverage. By empowering all its members equally to discuss and monitor each other's human rights record (Blackburn 2011), the UPR provides an opportunity to build a comprehensive database of the human rights record of all nations (Dominguez-Redondo 2012). Furthermore, it recognizes and reaffirms each nation's

1 See more about the previous Vietnam sessions and future agendas at https://www.ohchr.org/EN/HRBodies/UPR/Pages/VNindex.aspx (last access on 3 March 2020).

commitment to the implementation of international human rights and creates an environment for condemning and opposing human rights violations by employing 'naming and shaming' (Abebe 2009).

Although the Vietnamese delegation affirmed at the session that, '[The Law on Cyber Security in Vietnam only] sought to address the use of cyberspace to violate the legitimate interest of organizations and individuals, undermine national security and jeopardize social order and security' (Working Group 2019), this plain statement was not sufficient to satisfy the requirements of the UPR mechanism. In fact, dozens of countries voiced their concerns and criticized the Cybersecurity Law. With a series of recommendations to which Vietnam will be required to respond in upcoming reviews, it has been thought best to divide these recommendations into two groups, on the basis of their specificity.

The first group, hereinafter referred to as the General Recommendations Group, includes countries such as France, the Netherlands, New Zealand, Sweden, Austria, and Canada. The point at issue for this group was the failure to describe the technical aspects of the VSCL or indicate which regulations were not consistent with international law and universal human rights standards.

In the case of New Zealand, for example, the recommendations that the UPR delegation proposed to Vietnam were so 'abstract' that it is difficult for anyone to understand what problems were being indicated and what needed to be done. New Zealand requested that Vietnam should amend provisions of the newly issued Criminal Code and Cybersecurity Law to ensure that these two would be compatible with international human rights law in general, and with the International Covenant on Civil and Political Rights (ICCPR) (Working Group 2019: 38, 187). However, New Zealand did not try to offer reasons why a particular clause or article was incompatible, and failed to identify what aspects or what legal content needed to be altered.

In the case of the French delegation, it was suggested to the Vietnamese government that it should guarantee, step by step, the right to freedom of expression, in accordance with the newly approved Cybersecurity Law (Working Group 2019: 38, 168). It could be said that this suggestion was less confusing than the one offered by New Zealand, and that the French government wanted Vietnam to improve its domestic freedom of expression. However, questions concerning the relevance of freedom of expression to the new law or an assessment of the Cybersecurity Law were ignored by the French representatives.

This type of recommendation was also repeatedly made to the Vietnamese by the Canadians and Austrians.

The most vital problem with these recommendations was that they had little practicality and offered no specific benefits in terms of researching or improving the state of the country's human rights regulations. In addition, scholars and observers have also noted that the proposals usually had only a symbolic significance and were intended to relieve pressure from lobbying groups in some of the countries concerned (Goel et al. 2010), and consequently, it would be difficult to seriously review and analyse the recommendations of the countries in this group.

The second group, which could be called the Specific Recommendation Group, put forth clearer arguments against the VCSL.

The Finnish delegation claimed that the concept of 'national security' in the VCSL was too vague, and its interpretation was inherently prone to be subjective. Their recommendation was that Vietnam needed to provide a more detailed definition, or even eliminate obligations imposed on citizens related to the concept of national security, to ensure that it

would not be applied arbitrarily or abused. Vietnamese researchers at least acquired a more substantial perspective on the legal issues that the authors of the VCSL may have needed to reconsider.

On the other hand, Sweden and the Netherlands expressed that the VCSL could affect Vietnam's obligations under Articles 17 and 19 of the ICCPR (Working Group 2019: 38.183). Article 17 of the ICCPR, which protects personal privacy, states that 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation.' Article 19, in particular, focuses on the right to freedom of opinion. Freedom of expression requires governments of countries to take measures to maintain citizens' right to hold opinions and the right to freedom of expression, which includes freedom to seek, receive and impart information and ideas of all kinds.

Thus, the next allegation against the Vietnam Cybersecurity Law was the possibility of causing negative impacts on the exercise of freedom, privacy, and freedom of expression.

The United States, in its familiar straight-talking style, specifically indicated that Articles 8, 18 and 26 of the VCSL failed to meet the standard of international obligations that Vietnam was committed to implement, and that they even failed to meet the standards laid down in the Constitution of the Socialist Republic of Vietnam, 2013.

Article 8 prescribes acts prohibited in cybersecurity activities, including the practice of freedom of speech and personal privacy. Article 18 recognizes the principle of preventing and countering the use of cyberspace and electronic means to jeopardize national security. More particularly, the scope of this principle covers 'Propagation against the Socialist Republic of Vietnam; inciting riots, disrupting security and public order; personal humiliation and slander and so on. . .', the familiar language that has been employed countless times to put activists and journalists in jail. Article 18 also specifies the mandatory obligations of individuals and organizations towards authority. Article 26, on ensuring information security in cyberspace, mainly determines the cooperative obligation of enterprises operating in the field of telecommunications, internet and value-added services towards the requests of competent authorities authorized by the VCSL.

There are notable issues to be discussed and challenged, such as the unquestionable obligation to provide user information to specialized forces upon written request, the obligation of service providers to prevent and delete information deemed to violate the requirements of the VCSL, or the obligation to record and store Vietnamese user data within the territory of Vietnam. Comments from the United States pressured the VCSL drafting team to revise the language of the document and even its philosophical stance in relation to cybersecurity.

Along with everything mentioned above, the hearing of Vietnam before the Human Rights Council on 12 March concerning ICCPR implementation helped observers find a near convergence on the controversy surrounding the VCSL in international human rights dialogues and its legal and technical shortcomings. Since the human rights experts of the Human Rights Committee have authoritative knowledge and reliable information about international law, as well as the situation in Vietnam, they were able to provide a perspective with a higher level of expertise relating to allegations against the VCSL. And these allegations appear well founded.

In general, the Committee agreed that the provisions and the drafting philosophy of the VCSL do indeed affect the international standards and obligations of Vietnam, as set out in Article 17 and Article 19 of the ICCPR, which were briefly mentioned above, with additions from the Committee concerning the principles of 'necessity' and 'proportionality' when

applying administrative actions authorized by the VCSL. The Committee also pointed out particular issues in the law that could affect the human rights situation in Vietnam (UN Human Rights Committee 2019), including,

a. The definition of legal and illegal content in cyberspace;
b. The obligation of service providers and related enterprises to refuse to provide internet services when requested to do so by so the authorities, and to censor or report to the authorities individuals posting illegal content;
c. The obligation of service providers regarding the internet, telecommunications and other value-added services to retain data in Vietnam;
d. A new issue was added by the Committee: the concern as to whether administrative decisions affecting the freedom of expression or privacy that were authorized by the VCSL could go to judicial review.

It can be seen from the above analysis that international criticism of the VCSL had valuable points of intersection, which help us to analyse them and reclassify them into three groups.

The first group consists of those with philosophical concerns, with reference to the complaints of some countries (as well as those of experts and non-governmental organizations) about the general direction and principle of the cybersecurity document. These complaints may relate to the definition and delineation of the concept of 'national security', or criticisms related to Article 8 of the VCSL, which suggest that semantic ambiguity in the law's clauses offers the Vietnamese authorities too many rights and the ability to apply them arbitrarily, in the words of Amnesty International (Amnesty 2018).

The second group is concerned with obligations imposed on enterprises operating in the field of the telecommunications network, the internet, and value-added services in cyberspace. Thus, this group can be considered as concerned with compulsion and obligations, ranging from data localization, data extraction, and the provision of user information upon request, to the termination and discontinuance of telecommunications, internet, and value-added services to any organizations and individuals who are in violation of the VCSL, as determined by the authorized administrative agencies. These obligations would obviously not be welcomed by a large proportion of the international community.

The third group is concerned with the necessity for *judicial review*, which is also an essential issue due to its high level of legal technicality and objectivity. Upon considering this recommendation, the solution may be to synchronize Vietnamese legal philosophy and to create a more advantageous political position in international dialogues.

The three major human rights concerns identified above are substantiated by the reflections of other stakeholders, including national human rights institutions and non-governmental organizations (NGOs).

For instance, Access Now—a major human rights NGO advocating for digital civil rights—noted in their UPR submission that the VCSL (specifically the provisions of 'representative offices' and measures for data localization) takes away from the global character of the internet (Access Now 2019: 22–4). They assert that this can be a future threat to data protection and privacy by the government.

A prominent human rights organization with extensive activism in Vietnam called Vietnam VOICE also shares similar concerns to Amnesty International. In the submission, they contend that the concept of 'national security' and other related ideas in Article 8 of

the VCSL show little predictability, therefore allowing the utilization of VCSL's provisions at the authority's own discretion (VOICE 2018).

Moreover, Legal Initiative for Vietnam (LIV), a legal-focused NGOs advocating for human rights and freedom of expression in Vietnam, is also able to point out the problem with the lack of judicial oversight concerning the responsibility placed upon private service providers to remove and delete content and to deny services to specific users at the MPS ' requests (Legal Initiatives for Vietnam 2018: 7).

There are, indeed, NGOs and civil society organizations that acted as sympathisers for the Vietnamese government during the UPR review. Most Vietnam-based and China-based organizations such as the Center for Environment and Community Research; the Institute of Economics, Law and Management; or the China Society for Human Rights Studies often praised Vietnam's human rights realization and achievements during the reviewed period. As expected, however, most of them shied away from contentious subjects. These reports did not mention the name VCSL despite it being the central dispute between many stakeholders.

Consequently, it is more than probable to conclude that the three groups of human rights concerns represent at least a broad and explicit consensus over the legal complication of the VCSL.

2. The VCSL and international practices

2.1. Regarding the legal philosophy of the VCSL

By obtaining a holistic view of the objections and concerns regarding the VCSL and classifying them, we have a more solid foundation for analysing and comparing the VCSL with international practices.

'National security' has long been a controversial concept in the legal provisions of the ICCPR in particular, and in international human rights law generally. We cannot deny the necessity of the concept of national security in protecting human rights in the worldwide political environment of the present day. Common legal practice around the world demonstrates that when the risk to human rights is weighed against national security risks (as well as risks to public health), human rights are put on hold to focus on the more critical priorities mentioned above (Feinberg et al. 2015).

The UN Security Council has repeatedly shown its concern for national security and public health.

One of the most concrete and practical contemporary examples is the issue of terrorism. In Resolution 2178 (UN Security Council 2014a), adopted on 24 September of 2014, the UN Security Council accepted the dangers imposed by foreign terrorist fighters and reaffirmed that extremism will continue to be one of the greatest threats to world peace and security. In specifying individuals who move from one country to another to engage in acts of terrorism or in terrorist instruction and training, Resolution 2178 (which is legally binding) created a legal basis for a series of national laws to restrict freedom of movement, and prohibit border entry and exit of those on a list of monitored individuals and to enhance the supervision of public activities, both offline and online.

With a similar approach, Resolution 2177 (UN Security Council 2014b) confirmed that the Ebola outbreak in Africa was sufficiently serious to be considered a threat to world peace and security. Shortly afterwards, measures that in nature violated basic human rights, such as home detention, strict controlling of emigration permits, and the imposition of a

duty to periodically report to the authorities and to participate in mandatory epidemic control activities, were officially applied by infected nations.

The examples cited above confirm that international practice (in both national and international law) is no stranger to a 'rational trade-off' between human rights and social priorities, solely dependent on the perception of the authority concerned. Therefore, the employment of the concept of 'national security' as cited in the VCSL is not something invented by Vietnam. It could be argued that the Vietnamese government is simply adopting technical measures and governance models that have long been attested to and recognized by the international community. However, controversy begins with the discussion of how to define 'national security'.

The ICCPR itself avoids the definition of the concept. Article 19(3) of the ICCPR only sets out the exceptions (including national security) by which a country can restrict freedom of speech. Hence, the definition of acts that could be considered violations of national security is a matter for the representative government of the country. However, this lack of explanation does not prevent the Human Rights Committee ('Committee') from making comments to guide the establishment and formation of the concept of national security. General Comment No. 34 of the Committee sets out a number of criteria to ensure that the concept of national security will not be abused by limitations placed on a general freedom of speech.

For instance, the Human Rights Committee argues that the application of the concept of national security by the laws of a country must be clear and provide adequate explanations, so that citizens are able to ascertain what kind of expression is to be restricted. The need for specific and individualized exceptions to limit freedom of expression based on national security is also emphasized. The Human Rights Committee condemns the general and vague use of national security as justification. The Committee was adamant that:

> When a State party invokes a legitimate ground for restriction of freedom of expression, it must demonstrate in specific and individualised fashion the precise nature of the threat, and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the expression and the threat. (UN Human Rights Committee 2011: 25)

Interestingly, in the proportionality and necessity test, the Committee referred to the Siracusa Principles, a product of the UN Economic and Social Council, which stipulated that reasonable national security interests only exist if they are utilized against use of force or threats of use of force that are detrimental to the territorial integrity or political independence of a nation (UN Human Rights Council 1985).

> These suggestions of the UN Human Rights Committee put the VCSL in a difficult situation.

It is a fact that with the exception of Article 8, which stipulates behaviour prohibited on social networks, such as 'Organising, executing, colluding, persuading, buying off, duping, enticing, instructing and training people against the Socialist Republic of Vietnam', the VCSL leaves open the definition of national security and activities that threaten national security. Objectively, it is complicated for readers of this document to determine the extent to which their behaviour will be targeted, or to determine what behaviour will enable the state authorities to extract individual information from online archives.

In other words, the enactment of the aforementioned legal decisions depends entirely on the subjective viewpoint of the competent state authorities and their own interpretation of the concept of 'national security'. This seems to imply that the notion of 'national security'

and its protection in the VCSL fails to meet the requirements of the Human Rights Committee and the ICCPR in general, including the requirement for the creation of specific and individualized exceptions, and the establishment of a direct and immediate connection between the prohibited expression and the national threat. It also seems that the VCSL fails to reflect the spirit of the Siracusa Principles.

The concern is reasonably justified. Long before the VCSL came into effect, the Vietnamese state apparatus was already notorious for its interpretations of 'national security'. For instance, in the criminal case against the activist Phan Kim Khanh in 2017, the 16-page judgment accused him of conducting propaganda against the national security of the Socialist Republic of Vietnam, depicting his 'criminal activities' as, establishing and operating an unlicensed anti-corruption news outlet; being a friend of certain individuals (Le Quoc Quan, Nguyen Do Thanh Phong); criticizing and mocking certain public officials (The People's Court of Quang Binh 2017: 5–6)—allegations that were neither specific, individualized, nor directly connected to an immediate threat to national security. Even more interesting, the panel of experts appointed to 'scientifically' ponder the legality of Mr Khanh's online articles was selected from members of the Ministry of Information and Communication and the Ministry of Public Security, two authorities directly involved in Mr Khanh's arrest.

The recent high-profile case against the Vietnam Independent Journalist Association ('VIJA') at the end of 2020 is exemplary in understanding the arbitrary application of national security in national legal practices. In this case, the final conviction has been unavailable to even the families and the defence attorneys of the convicted for quite a long time. Fortunately, the research team can obtain and study the indictment issued by the Procuracy of Ho Chi Minh City.

Specifically, to substantiate its allegations against the leading members of VIJA that they have been involved in anti-state propaganda that endangers state security, the procuracy listed the member's articles as the primary evidence.

Concerning Pham Chi Dung, the sitting president of VIJA, the procuracy argues that he has written over 1,500 articles, and that 23 of them are deemed as either 'reactionary', 'defamation against the people's regime' or 'libel against the Party's leadership' by the competent evaluation authority (HCMC Procuracy 2020: 4–5). This is only 1.5 per cent of all his works, spanning over one decade. Two other members are accused of publishing a combination of around 12 articles of similar nature, among hundreds of articles.

According to the defence attorneys, the high court accepted these items of evidence as indisputable facts and recorded them in the judgment.[2] Further legal arguments on how and why dozens of journalistic articles can result in harmful effects to national security were not offered. Just by mere observation, we can tell that it is highly counter-intuitive to reconcile such insignificant conduct, within a delayed and uncertain timeline, to an immediate and serious threat against the security of Vietnam as a whole.

The authors note that the VCSL is not directly mentioned as a substantive foundation in the final judgment against these journalists. However, the VCSL certainly creates the legal corridors for the authorities to act without any restraint in obtaining and controlling the convicted's online information. The trials demonstrate that there is little hope that the concept of 'national security' in the VCSL will be applied objectively and adequately, according to international standards.

2 The information is based on our personal interviews with the defence attorneys.

Indeed, Vietnam is not the only country facing this conflicting situation. For example, the Joint Human Rights Committee of the United Kingdom, a nation with one of the oldest traditions of liberal democracy, in scrutinizing the draft of a Counter-Extremism Bill, emphasized that extremism is sometimes not synonymous with direct calls for terrorist actions (Shepherd 2017). Given the freedom of expression, extremism can effectively foster a political atmosphere that is sympathetic to terrorism and nourishes and protects terrorist conceptions. The Council acknowledged that it is difficult to use legal terms to describe the risks associated with extremism without being overly vague, unreasonably general or discriminatory. Hence, it is challenging to determine whether extremism (and its forms of speech) can be included in the scope of national security infringements.

However, as contended by Professor Nowak, there is a consensus among legal scholars all over the world that a national security infringement could be defined as a 'political or military threat to the entire nation', including the 'publication of a direct call to violent overthrow of the government in an atmosphere of political unrest' (Nowak 2005: 464).

Dealing with the relationship between freedom of expression and national security, the Johannesburg principles skilfully recognizes the importance of national security and its relation with restricting freedom of expression in a negative manner. Herein, *unless* the government can demonstrate its '*genuine purpose and demonstrable effect*' to protect the country's existence or its territorial integrity, the justification of national security is unsatisfactory. Specifically, the principles emphasize that the capacity of such restrictions must be able to respond to the use or threat of force, which could be a military threat or a clear incitement to violently overthrow the incumbent Government (Article 19, Principle 2). This argument seems to resemble legal elements that the General Comment of the Human Rights Committee and the Siracusa Principles offer: the ultimate aim of restriction must be the existence of the nation or its territorial integrity and political independence, and it must respond to the use of force or the threat of force.

Sandra Coliver observes in her commentary on the Johannesburg Principles that the Principles might expand the permitted restrictions on freedom of expression to not only the use or threat of force, but also that state's capacity to respond to the use or threat of force (Coliver 1998: 21). Yet simultaneously, the principles further tighten the national security definition.

Principle 2(a) envisages that national security interests are only legitimate in preventing violence aimed at changing a country's government or borders, espionage, or protecting genuine military secrets (movement of troops and details of weapons design).

On the other hand, Principle 2(b) intentionally provides an illustrative list of illegitimate grounds for invoking 'national security'. From using the national security justification to protect the government from 'embarrassment or exposure of wrongdoing', to 'entrench a particular ideology', or to 'suppress industrial unrest', the Johannesburg drafters show that they were well-aware of widespread abuse of the concept over the intervening 10 years from the Siracusa Principles.

The authors believe that it is not too tricky to concretize the concept of national security in a consistent way with the spirit of international practices and beliefs, which also satisfies the Vietnamese government's security demands. However, this is the case only if the regime's intention is to preserve the safety of national territory and protect the integrity of its vital institutions from *violent action*. Using the suggestions from the Johannesburg Principles, the authors argue that what the Vietnamese government is pursuing should be called 'ideological security', which is inherently different from the internationally accepted concept of national security. As long as the Party leadership continues to believe that the

mere expression of an individual's political personality or criticism of the current socio-economic system is equivalent to an attempt to overthrow the regime, the philosophy of the VCSL remains incompatible with international law and the universal practices of responsible nations.

2.2. Mandatory obligations of special enterprises

Article 26 is another heavily criticized component of the VCSL controversy. Apart from the objections of many countries (the harshest comments, those of the USA, have already been summarized herein), there have been condemnations by various non-governmental organizations of the obligations imposed on enterprises providing services on telecommunications networks and the internet, and providing value-added services in cyberspace. For example, in the Open Letter of Amnesty International to the National Assembly of Vietnam (Amnesty 2018), Article 26 occupied a predominant place among the issues presented to the representatives of the Vietnamese National Assembly for reconsideration. Human Rights Watch, another influential non-governmental human rights organization, also strongly criticized Article 26. This was the issue that focused particularly on the human rights risks of VCSL, in a report prepared by Human Rights Watch sent to the UPR in January 2019 (HRW 2018).

So, what provisions of Article 26 make the clause contrary to international practices and standards? The authors would like to summarize the article in terms of four obligations contained within it:

1. To provide any type of users' information and their personal accumulated data to specialized cybersecurity forces upon written request;
2. To immediately block, or delete, any information that violates the VCSL, as designated by authorized cybersecurity forces;
3. To refuse to provide or stop providing services on telecommunications networks, internet, and value-added services to organizations and individuals in response to a request by authorized cybersecurity forces;
4. To archive the data of Vietnamese users and Vietnamese users' data generated in Vietnam within a period corresponding to the detailed regulations of the Vietnamese government.

Many provisions of the VCSL could be problematic, but with a closer look, the obligations stipulated in Article 26 are not unprecedented in terms of international practices.

Although the USA is the most outspoken critic of this article, 'Uncle Sam' is also the most prolific of all internet data collectors. Since the events of 11 September 2001, the US Patriot Act (Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism) has given extensive authority to US security forces and intelligence agencies to monitor, extract and collect information from personal communications in all forms (including but not limited to, information gathered from telephone communications, text messages and personal networking programs), to ransack and seize assets and information, and to monitor political and financial activities in real and cyber environments (ACLU 2011).

Additionally, Chapter 702 of the Foreign Intelligence Surveillance Act (FISA) legislation, which is of the utmost importance in protecting US national security, authorizes the competent authorities to apply all measures to monitor individuals who are not US citizens. It also asserts that the collection of information and exchanges of citizens of the US in the process of contacting foreign subjects who are under investigation is perfectly legal (Schneider 2018).

More specifically, the effectiveness of investigating, monitoring and exchanging information between the US government and network service providers has also been confirmed in many cases. The progress of 'finding and terminating' one of the senior leaders of ISIS, Haji Iman, was mainly based on two years of collecting email communications between him and his accomplices living in the USA.

The plot to attack the New York metro system in 2009 was also discovered and prevented largely thanks to the intelligence and information collection system authorized by Chapter 702. Najibullah Zazi, the person who was apprehended, was a citizen of Afghanistan with permanent residency in Colorado. He sent and received many emails in which crimes were discussed with an al Qaeda intermediary in Pakistan. It is worth mentioning that these practices have been taking place in the USA for nearly 20 years and were accepted by American security professionals and legal scholars. The situation changed only due to the actions of the former CIA officer and NSA contract officer, Edward Snowden, who revealed to the American public and the world the vast extent of public monitoring on the part of the US government (MacAskill 2013).

The 'systematic access', imposed by the government on user data collected by private companies has also become a feature of many countries.

To take another example: in the United States, a special order of the United States Federal Court is automatically re-issued every 90 days; it requires telecommunications service providers across the country to submit information packets of telephone numbers, calls made and time and duration of calls to the US National Security Agency (NSA) (Rubinstein et al. 2014). And under German legislation, network service and telecommunications providers are asked to collect information such as customers' full names, addresses, and phone numbers. This 'inventory information' is sent directly to the data bank of the Federal Network Agency. All other agencies of the Federal Republic of Germany are entitled to submit an electronic extraction request to this agency and to receive the aforementioned information without further procedure (Schwartz 2012). The outreach of the German police is so extensive that they can even request that cell towers pinpoint the location of a particular subscriber in a specified area and for a specified period of time. According to an independent statistic, in 2012 this operation was conducted about 410 times to garner the location and other information of more than 4.2 million subscribers. In the United Kingdom, the competent authorities request information and data related to voice calls up to 500,000 times per year (Brown 2012).

Requests for information on each individual and each internet account on an ad hoc basis (similar to the VCSL approach) have become increasingly common in liberal democracies. It can be said that these administrative activities are now a legalized global phenomenon. A report by the European Parliament shows that a major number of EU member states have been implementing domestic legislation that allows the extraction of data archived by enterprises providing network services and private telecommunications services whenever state agencies deem it necessary, with or without the consent of service providers (European Parliament 2013). The spread of requests to extract information was admitted by Google in the Google Cloud White Paper published in 2018.[3] The paper confirmed that all governments had created legal corridors requesting enterprises to extract user information.

3 See more at https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf (referenced 24 June 2021).

Other operations such as requests to block or share a certain type of information, or to localize the data of national users, which are similar to the aforementioned requests to extract user information, have become so common that analysing and comparing them in detail would turn this small paper into a monograph on cybersecurity measures around the world. To achieve a better understanding of the phenomenon, we borrow the words of Professor John Selby of Macquarie University, Australia. He asserts that it is a fallacy to assume that any legal requirement on extracting and localizing information and data, or requiring removal of opinions, internet posts, and such like, can only be found in developing countries or totalitarian countries (Selby 2017). The empirical data of his research shows that most countries in the world, including well-respected democracies such as Germany, Denmark, Belgium, Finland, Sweden, and the United Kingdom, have all imposed similar legal obligations on enterprises.

Obviously, the above analysis is not intended to deny some of detailed responsibilities of the Vietnamese government in many other new-generation free trade agreements that they have recently signed. However, it shows that provisional measures established by the VCSL (except for the requirement to stop providing telecommunications network services) are certainly not a 'one of a kind' product among current international legal systems.

2.3. Judicial review/remedy

Judicial review here refers to a procedure by which government requests to intervene in the information system, or to extract personal data of users, must be subject to a judicial decision, such as a Court order or the decision of a prosecutor/procuracy.

It is a concept that has great prominence in the legal systems of many countries and is fought for by local human rights groups when national laws begin to apply cybersecurity control measures. Generally, the authors believe that a judicial review procedure of a high standard should always be a legitimate requirement and, on the other hand, should also be compatible with Vietnam's current standard legal process of investigation and procedure.

The Vietnamese legal system itself has done an excellent job in explaining the necessity for judicial review. Article 21 of the Vietnam 2013 Constitution clearly states that: 'The law safely protects information regarding personal privacy, personal secrecy and familial secrecy'. Accordingly, any search or confiscation of personal belongings and information can only be implemented if there is a warrant from the competent Office of Procuracy, as stipulated in the Code of Criminal Procedure 2015.

No other legislation has the power to violate personal privacy, and yet somehow the VCSL is a very convenient exception.

As the regulation now stands (Article 26), either the special forces of the Ministry of Public Security or the Ministry of Culture, Informational and Communication can issue a request demanding the take down of online posts, videos, any kind of information and even the termination of service provision to certain individuals or organizations, without the approval of the procuracy or the court. Similarly, the Ministry of Public Security is authorized direct and unrestricted access to any type of user information collected by these service providers. And as the final nail in the coffin, no judicial remedy against such action is recognized in the document.

Although the research group finds no problem with imposing certain obligations on powerful social and internet enterprises, as explained in Section 2.2, these interventions should be subject to appropriate scrutiny and consideration. Applying a judicial review to the VCSL will contribute to the harmony between Vietnamese laws and worldwide laws

and create a solid moral foundation for Vietnam in future international dialogues. The method of honouring the principle of judicial review/remedy, whilst also not obstructing cybersecurity controls and investigations, and at the same time protecting the right of citizens from abuse of power, can be found in the legal systems of many countries around the world.

In the USA, for instance, the Federal Bureaucracy Investigation (FBI) can send a National Security Letter (NSL) to service providers to request only information consisting of 'full name, address, time of service use or bills of using local or long-distance telecommunications services'. For more detailed information, such as the content of conversations or mail content, a court warrant is a prerequisite.

Judicial review/remedy is not a fundamental problem for the US government in its efforts to monitor online activities to protect national security and at the same time to guarantee the rights of its citizens. As discussed, FISA divides the subjects targeted by US security agencies into two types: US national and non-national. In the case of a US national, an order from the Foreign Intelligence Surveillance Court (FISC) is required in each separate case in which information is extracted. However, in the case of foreign nationals, the investigating agency has full authority without the need for judicial review (Clarke et al. 2013). The application of FISA's legal solution to the current situation in Vietnam is not a bad idea. As the Vietnamese security agency has repeatedly affirmed, plots of riots and subversion against the regime were orchestrated, built, trained, funded and carried out under the control of a handful of 'reactionary' Vietnamese living overseas.

A similar, albeit not identical approach to cybersecurity control can be found in the United Kingdom. Control was at first exerted primarily by the Regulation of Investigatory Powers Act (RIPA), which was replaced by an act with the same name in 2016. Under this Act, no distinction is made between British citizens and foreign nationals. It is the range of communication that is the standard employed for application of security measures. Specifically, RIPA considers two types of communication, internal and external. Internal communication, that is, forms of communication via the internet and other types of wireless network within the United Kingdom, will only be accessible if the competent authorities acquire a court order for each specific case. In contrast, similar forms of communication with contact points outside of the United Kingdom can be monitored without a court order: all that is needed is the provision of a written account of the reason for such interference with privacy (Watt 2017).

Judicial review by the Attorney General (a title equivalent to the Head of the Supreme People's Procuracy in Vietnam) is also a long-standing procedure that is surprisingly similar to the Vietnamese system. With the Australian Security Intelligence Organisation Act 1979 (ASIOA), amended in 2018, Australia demonstrates that proper judicial reviews do not hinder investigation or national security protection measures, as some Vietnamese scholars anxiously maintain (Thai 2019). In particular, ASIOA requires the Australian security agency to justify to the Attorney General the issue of a warrant for interventive measures, such as monitoring electronic devices, accessing personal computer data, or identifying individuals through accounts, information, network data and other types of data.

Overall, a judicial oversight mechanism as a procedural safeguard against the abuse of government surveillance power is a relatively new topic in international legal discourse. Yet, it has received proper and prompt attention from legal experts and human rights advocates.

The International Principles on the Application of Human Rights to Communications Surveillance ('IPAHRS') is discussed and codified by Access Now, the Electronic Frontier Foundation, and Privacy International, along with several NGOs, criminal lawyers, and human rights and privacy advocates. With the endorsement of the UN Human Rights Council and the UN Office of the High Commissioner for Human Rights, IPAHRS is an authoritative illustration of the vital role of judicial authority in the current surveillance rich-environment cloaked in secrecy.

Specifically, out of 13 principles set out by IPAHRS, four revolve around judicial authority. For instance, the Principle of Competent Judicial Authority establishes that any decisions on communication surveillance shall be made through an impartial and capable judicial authority. This authority then uses the thresholds set out by the Principle of Necessity and the Principle of Proportionality, ensuring that the collection of the personal information is governed by sufficient due process guarantees and judicial oversight (IPAHRS 2013).

The principles clearly echo the recommendations of Martin Scheinin, the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism. In his 2009 report, Scheinin asserts 'there must be no secret surveillance system that is not under review of an independent oversight body and all interferences must be authorised through an independent body' (UN Human Rights Council 2009).

The research acknowledges that there is so much more to realizing this so-called judicial authorization/control/review mechanism. Should Vietnam follow that path of an effective adversarial procedure for the authorization of surveillance with the immediate participation of outside stakeholders? Or should Vietnam consider the introduction of internal mechanisms to enable *ex parte* application? Nevertheless, the authors are convinced that recognizing and incorporating judicial review for the use of lawful surveillance into Vietnam's VCSL is a top priority. Only with these mechanisms can the VCSL harmonize the domestic legal system with international norms.

3. Conclusion

One aspect of the current controversy surrounding the Vietnamese Cybersecurity Law is the polarization of opinion concerning its legality and conformity to international law and practice.

As in the laws of all other countries, the VCSL was instigated firstly to ensure the legitimate interests of social order and security, as well as the general political stability of the state. Demonstrated by the evidence herein, the intrusion by governments around the world into network data and online information is undoubtedly an unstoppable legal trend. Therefore, the Vietnam Cybersecurity Law is certainly not the 'odd man out' in international law and practice. Concerning the imposed obligations on special enterprises, this is certainly the case, as we compared and analysed above.

Yet, recognizing VCSL as a legitimate governance tool does not necessarily mean that it is free of flaws. After scrutinizing the perspectives and opinions of international actors and stakeholders via official human rights mechanisms and communication channels, the authors find that there are concerns about VCSL that are justified and needed serious consideration.

First and foremost, there is no disputing that the purposeful ambiguity between national security and ideological security in the VCSL violates positive international human rights law and its normative norms. By mixing up the two concepts, the VCSL creates a legal limbo allowing the authorities to throw in any justification or explanation that fits their narrative and interests. Without thresholds of the violent nature of the threats and the political significance of protected targets such as the country's political independence suggested by international law, VCSL only further enriches the arsenal of the Vietnamese public security forces in arbitrarily dealing with the right to freedom of expression in the country. Similarly, the lack of judicial review/remedy when it comes to cybersecurity-related decisions goes against not only international standards but also the legal tradition of the country.

The combination of the manipulatable philosophy of national security and the non-existence of any independent safeguard institution contributes to making VCSL weak legislation on the whole. Therefore, the authors argue that it is still possible for the philosophical foundation and technical direction of the VCSL to be further revised and improved by means of detailed regulatory legislation on the part of the relevant authority. The acquisition of an international perspective and the attention given to comparative experience will undoubtedly help the Vietnam Cybersecurity Law to occupy a stronger position in future international dialogues.

Conflict of interest statement

The authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest, or non-financial interest in the subject matter or materials discussed in this article.

References

Abebe, A. M. 2009. Of Shaming and Bargaining: African States and the Universal Periodic Review of the United Nations Human Rights Council. *Human Rights Law Review* 9(1): 1– 35.

Access Now. 2018. Submission to the United Nations Human Rights Council, on the Universal Periodic Review 2018 Cycle for Vietnam. https://www.accessnow.org/cms/assets/uploads/2018/07/UPR-Vietnam-digital-rights.pdf (referenced 24 June 2021).

ACLU. 2011. Surveillance under the Patriot Act. https://www.aclu.org/national-security/surveillance-under-patriot-act (referenced 3 March 2020).

Amnesty. 2018. Open Letter – Viet Nam Must Respect Human Rights in the Cybersecurity Law. https://www.amnesty.org/en/documents/asa41/9258/2018/en/ (referenced 3 March 2020).

Article 19. 1995. The Johannesburg Principles on National Security, Freedom of Expression and Access to Information. https://www.refworld.org/docid/4653fa1f2.html (referenced 30 June 2021).

Blackburn, R. L. 2011. Cultural Relativism in the Universal Periodic Review of the Human Rights Council. *International Catalan Institute for Peace*, Working Paper 2011/3.

Brown, I. 2012. Government Access to Private-Sector Data in the United Kingdom. *International Data Privacy Law* 2(4): 230–8.

Bui, T. H. 2014. Deconstructing the 'Socialist' Rule of Law in Vietnam: The Changing Discourse on Human Rights in Vietnam's Constitutional Reform Process. *Contemporary Southeast Asia* 36(1): 77–100. www.jstor.org/stable/43281278 (referenced 10 June 2021).

Chinh, N. M. 2019. Hoàn thiện pháp luật về an ninh mạng trong tÙnh hÙnh hiện nay. *Communist Journal*. http://tapchicongsan.org.vn/an-ninh2/-/2018/812604/hoan-thien-phap-luat-ve-an-ninh-mang-trong-tinh-hinh-hien-nay.aspx (referenced 3 March 2020).

Clarke, R. A., Morell, M., Stone, G., et al. 2013. *The NSA Report. Liberty and Security in the Changing World. The President's Review Group on Intelligence and Communications Technologies*. Princeton, NJ: Princeton University Press.

Coliver, S. 1998. Commentary to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. *Human Rights Quarterly* 20(1): 12–80. http://www.jstor.org/stable/762696 (referenced 24 June 2021).

Dominguez-Redondo, E. 2012. The Universal Periodic Review – Is There Life beyond Naming and Shaming in Human Rights Implementation? *New Zealand Law Review* 4: 673.

European Parliament. 2013. National Programmes for Mass Surveillance of Personal Data in E.U. Member States and Their Compatibility with E.U. Law. http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf (referenced 3 March 2020).

Feinberg, M., L. Niada-Avshalom, and B. Toebes. 2015. National Security and Public Health: exceptions to Human Rights? *International Journal of Human Rights* 19(4): 383–7. DOI: 10.1080/13642987.2015.1044812.

Goel, V., and M. K. Tripathi. 2010. The Role of NGOs in the Enforcement of Human Rights: An Overview. *Indian Journal of Political Science* 71(3): 769–93.

HRW (Human Rights Watch). 2018. Submission to the Universal Periodic Review of Vietnam. https://www.hrw.org/news/2018/07/23/submission-universal-periodic-review-vietnam (referenced 3 March 2020).

Institute of Economics. 2018. Law and Management. The Press and Law Protect Human Rights Together. https://www.upr-info.org/sites/default/files/document/viet_nam/session_32_-_january_2019/ielm_upr32_vnm_e_main.pdf (referenced 24 June 2021).

International Principles on the Application of Human Rights to Communications Surveillance. 2013.

Legal Initiatives for Vietnam. 2018. Statement for UPR Pre-Session on Vietnam. https://www.upr-info.org/sites/default/files/document/viet_nam/session_32_-_january_2019/1._legal_initiatives_for_vietnam_stmt.pdf (referenced 24 June 2021).

MacAskill, E. 2013. Edward Snowden: How the Spy Story of the Age Leaked Out. 11 June. The Guardian. https://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile (referenced 3 March 2020).

Nowak, M. 2005. *U.N. Covenant on Civil and Political Rights CCPR Commentary*. N.P. Engel.

HCMC Procuracy (The Procuracy of Ho Chi Minh City). 2020. Indictment 543/CT-VKS-P1. 20 November 2020.

Quang, T. D. 2017. 'Tăng cường cÂng tác bảo đảm an toàn, an ninh mạng trong tÙnh hÙnh mới'. *Vietnam Government Portals*. http://baochinhphu.vn/Hoat-dong-cua-lanh-dao-Dang-Nha-nuoc/Tang-cuong-cong-tac-bao-dam-an-toan-an-ninh-mang-trong-tinh-hinh-moi/314458.vgp (referenced 3 March 2020).

Rubinstein, I. S., G. T. Nojeim, and R. D. Lee. 2014. Systematic Government Access to Personal Data: A Comparative Analysis. *International Data Privacy Law* 4(2): 96–119. DOI: 10.1093/idpl/ipu004

Schneider, J. 2018. What is Section 702 of FISA. CNN. https://edition.cnn.com/2018/01/11/politics/trump-fisa-section-702-surveillance-data/index.html (referenced 3 March 2020).

Schwartz, P. M. 2012. Systematic Government Access to Private-Sector Data in Germany. *International Data Privacy Law* 2(4): 289–301.

Selby, J. 2017. Data Localisation Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology* 25(3): 213–32. DOI: 10.1093/ijlit/eax010 (referenced 3 March 2020).

Shepherd, A. 2017. Extremism, Free Speech and the Rule of Law: Evaluating the Compliance of Legislation Restricting Extremist Expressions with Article 19 ICCPR. *Utrecht Journal of International and European Law* 33: 62–83. DOI: 10.5334/ujiel.405 (referenced 3 March 2020).

Thai, H. S. 2019. Nhận Diện và Đập Tan Những Luận Điệu XuyÁn Tạc Luật an Ninh Mạng. *The E-Journal of Vietnamese Communist Party*. http://dangcongsan.vn/tieu-diem/nhan-dien-va-dap-tan-nhung-luan-dieu-xuyen-tac-luat-an-ninh-mang—489084.html (referenced 3 March 2020.)

The People's Court of Quang Binh Province. 2017. Case 59/2017/HSST'.

UN OHCHR (The Office of the United Nations High Commissioner for Human Rights). No date. About Universal Periodic Review. http://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRMain.aspx (referenced 3 March 2020).

UN Human Rights Committee. 2011. General comment No. 34 on Article 19 Freedoms of opinion and expression. CCPR/C/GC/34.

———. 2019. List of issues in relation to the third periodic report of Viet Nam. Human Right Committee CCPR/C/VNM/Q/3. https://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fVNM%2fQ%2f3&Lang=en (referenced 03 March 2020).

UN Human Rights Council. 1985. Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights. United Nations Economic and Social Council. E/CN.4/1985/4.

———. 2009. Report of the Special Rapporteur on the Promotion and Protection of Human Rights while Countering Terrorism, Martin Scheinin. A/HRC/13/37.

UN Security Council (UNSC). 2014a. Resolution 2178 on Threats to International Peace and Security caused by Foreign Terrorist Fighters. S/RES/2178.

———. 2014b. Resolution 2177 on the Outbreak of the Ebola virus in and its impact on West Africa. S/RES/2177.

US Department of Justice. 2014. Preserving Life & Liberty. http://www.justice.gov/archive/ll/archive.htm (referenced 3 March 2020).

VOICE. 2018. *Submission to the UN Universal Periodic Review 32nd Session of the UPR Working Group*. https://www.civicus.org/documents/JointCIVICUSUP RSubmissonVietnam.pdf (referenced 18 March 2022).

Vietnamese Government. 2017. Tờ trình dự án Luật An ninh mạng. http://duthaoonline.quochoi.vn/DuThao/Lists/DT_DUTHAO_LUAT/View_Detail.aspx?ItemID=1382&TabIndex=2&TaiLieuID=2775 (referenced 3 March 2020).

Watt, E. 2017. The Right to Privacy and the Future of Mass Surveillance. *International Journal of Human Rights* 21(7): 773–99. DOI: 10.1080/13642987.2017.1298091.

White House. 2018. National Cyber Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (referenced 3 March 2020).

Working Group. 2019. Report of the Human Rights Council Working Group on the Universal Periodic Review Thirty-second session. A/HRC/41/7.