Mandates of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the rights to freedom of peaceful assembly and of association; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism

Ref.: OL VNM 6/2023
(Please use this reference in your reply)

18 September 2023

Excellency,

We have the honour to address you in our capacities as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; Special Rapporteur on the rights to freedom of peaceful assembly and of association; Special Rapporteur on the right to privacy and Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, pursuant to Human Rights Council resolutions 52/9, 50/17, 46/16 and 49/10.

In this connection, we would like to bring to the attention of your Excellency's Government information we have received concerning several laws and decrees, including the **Constitution of the Socialist Republic of Vietnam** (2013), the **Criminal Code** (2015), the **Press Law** (2016), the **Access to Information Law** (2016), and the **Cybersecurity Law** (2018), as well as **Decree 72/2013/ND-CP** on "management, provision, and use of internet services and information content online", **Decree 15/2020/ND-CP** on "penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information technology and electronic transactions", **Decree 119/2020/ND-CP** on "penalties for administrative violations in journalistic and publishing activities", **Decree 53/2022/ND-CP** on "elaborating a number of articles of the law on cybersecurity of Vietnam", **Decree 13/2023/ND-CP** on "protection of personal data", and draft amendments to the **Telecommunication Law** (2009).

We would like to share several observations and comments about this legislation to ensure the compliance of these norms with Viet Nam's obligations under international law, in particular those contained in the International Covenant on Civil and Political Rights (ICCPR). We have strong reservations that their overbroad language and pursuit of objectives beyond what are considered legitimate under international law may lead to criminalization of the legitimate exercise of the right to freedom of expression online.

This communication builds on and complements our previous communication VNM 7/2021. While we thank your Excellency's government for the reply we received on 27 April 2022, we recommend review and reconsideration of some aspects of these laws and decrees to ensure compliance with Viet Nam's international human rights obligations.

Background

The **Constitution of the Social Republic of Vietnam** (No. 64/2013/QH13)[1] is the foundational national framework. It includes the respect and protection of

[1] Law No. 64/2013/QH13, 28 November 2013.

fundamental freedoms and rights, but also provides for the restriction of such rights on grounds of "national defence, national security, social order and security, social morality and community well-being" (article 14), which is also reflected throughout all national legislation.

The **Criminal Code** (No. 100/2015/QH13)[2], at Chapter XIII, creates several "offences against national security". Articles 109, 113 and 299 provide prison terms of up to 20 years for establishing or joining an organization that acts against the people's government and for various offences classified as "terrorist", defined in the Law on Counter-Terrorism (No. 28/2013/QH13).[3] Article 117 provides a prison term of up to 20 years for "making, storing, or spreading information, materials or items for the purpose of opposing the State of the Socialist Republic of Viet Nam". Under article 331, "abusing democratic freedoms to infringe upon the interests of the State, lawful rights and interests of organizations and/or citizens" is punishable with a community sentence or imprisonment of up to 3 years, or up to 7 years if the offence has "a negative impact on social security, order or safety".

The **Press Law** (No. 103/2016/QH13)[4] regulates and organises the media, defined as print, broadcast, and online news media, and it regulates freedom of the media and the freedom of expression in the media of citizens. Article 4 describes the press as "the essential media for social life; the mouthpiece of the Party and State agencies … and the people's forum." Article 9 of the Press Law creates a large number of offences, including:

- distorting, defaming, or denying the people's government
- fabricating and causing panic among people
- causing division
- distorting history
- offending the nation and national heroes
- providing false information, distorting, slandering, or hurting the prestige of organizations, agencies, or the honour and dignity of individuals
- hurting the honour and dignity of journalists and reporters.

Article 13 provides that the State must create favourable conditions for media freedom and freedom of expression broadly. It also states that "[n]o one is allowed to abuse the freedom of the press, freedom of speech in the press to infringe upon the interests of the State or the legitimate rights and interests of organizations and citizens." Article 25 sets out various rights and obligations of journalists; the various other provisions regulate the activities of the media in great detail, including those of foreign media.

---

2 Law No. 100/2015/QH13, 27 November 2015.
3 Law No. 28/2013/QH13, 12 June 2013.
4 Law No. 103/2016/QH13, 05 April 2016.

The **Access to Information Law** (No. 104/2016/QH13)[5] provides for the exercise of the citizens' right of access to information, principles, procedures for exercising the right of access to information, and responsibilities of state agencies in ensuring the citizens' right of access to information. Article 6 elaborates further on inaccessible information, which consists of:

- Classified information that contains important contents associated with politics, national defense and security, foreign relations, economics, science, technology, and other fields as regulated by the law

- Information harming the national interests, causing adverse influence on the national defense and security, international relations, social order and security, social ethics and the community health; harming human life, living or property of others; information classified as working secrets; those concerning internal meetings of state agencies; documents drafted by state agencies to serve their internal activities.

The **Cybersecurity Law** (No. 24/2018/QH14)[6] creates several offences specifically with regard to online activity. These include, in article 8:

- using information technology equipment to defame the government or insult the nation, the national flag, the national emblem, the national anthem, great men, leaders, famous people, national heroes

- publishing defamatory information online

- publishing false information online about economic or financial issues

- publishing false information online that causes confusion, damages, or that causes difficulties for the operation of state agencies.

Article 16 of the Cybersecurity Law also criminalises the online publication of propaganda against the State, which is defined as including anything that defames the State, offends the people, or that desecrates the national flag, national anthem, political leaders, or national heroes It also criminalises calling for public gatherings intended to oppose or cause disruption to government agencies. The Law furthermore requires IT administrators to implement administrative and technical measures for the prevention, discovery, and removal of any criminal information, at the request of cybersecurity forces; and ISPs and other providers are required to cooperate with any investigations.

Article 17 of the Cybersecurity Law lists a number of acts that are considered cyber espionage or that are considered to be a deliberate violation of state-secrecy, work-related confidentiality, business confidentiality, family confidentiality or online privacy. These include the following:

- the illegal obtainment, trade, collection, deliberate revelation of information classified as state secret or otherwise confidential and that harm the dignity, reputation or lawful rights and interests of another

---

5 Law No. 104/2016/QH13, 06 April 2016.
6 Law No. 24/2018/QH14, 12 June 2018.

organization or individual

- the deliberate deletion, causing of damage, loss or changes to information classified as state secret or otherwise confidential and that is stored online

- the deliberately changing, cancelling, or neutralizing of a technical measure that is meant to protect state secrets or material that is otherwise confidential

- publishing state secrets or material that is otherwise confidential online

- eavesdropping on or recording conversations

- any other intentional violations of state secrecy or confidentiality.

Decree 72/2013/ND-CP[7] on management, provision, and use of internet services and information content online became effective on 1 September 2013. It was later amended by Decree 27/2018/ND-CP[8] and Decree 150/2018/ND-CP.[9] Under the Decree and its subsequent amendments, the use of the internet can be subject to various restrictions depending on the purpose or effect of its use. In article 5, the Decree prohibits the use of internet services and online information to:

- oppose the Socialist Republic of Vietnam

- threaten the national security, social order, and safety

- sabotage the national fraternity

- arouse animosity among races and religions

- contradict national traditions, among other acts.

It furthermore requires social media companies to provide user information to the authorities when this is requested for the purpose of fighting crime, including terrorism, or when relevant to other violations of the law. Under the Decree, internet providers including social media companies are liable for content that they store, host, transmit or otherwise spread, and are required to have at least one server in the country.

In April 2022, draft amendments to Decree 72/2013-ND-CP were made public. If adopted without further changes, the Decree will require social media companies to remove content it deems illegal within 24 hours. No further information on the status of these amendments has been made public since.

Decree 15/2020/ND-CP[10] on penalties for administrative violations against regulations on postal services, telecommunications, radio frequencies, information

---

7 Decree No. 72/2013/ND-CP, 15 July 2013.
8 Decree No. 27/2018/ND-CP, 01 March 2018.
9 Decree No.150/2018/ND-CP, 07 November 2018.
10 Decree No. 15/2020/ND-CP, 03 February 2020.

technology and electronic transactions became effective on 15 April 2020. It sets out and increases various penalties for administrative violations in the fields of telecommunications, information technology, and electronic transactions, *inter alia*. The Decree also stipulates specific administrative penalties for users who post or share "false information" on social networks, which are imposed in addition to other eventual civil or criminal liabilities related to distortion, slander, defamation, *inter alia*.

Article 100 (3) imposes several penalties on social network providers who fail to prevent such information from being posted on their social networks or who intentionally provide, store, or transmit violating content that is not in the State's interest. These social network providers are also required to remove such information or risk being subject to the suspension of their social network license and/or the revocation of their social network's domain name.

Article 101 specifically sets out penalties for violations of regulations on the use of social networks, which include administrative fines between VND 10-20 million (about 400-900 USD) for social network users who commit any such violations. The Decree further provides for higher administrative fines of VND 20-30 million (about USD 900-1300) for the disclosure of information classified as state or personal secrets, but which are not serious enough to face criminal punishment. Additionally, violators are required by the Decree to remove the identified false information or violating content that was posted or shared.

Decree 119/2020/ND-CP[11] on penalties for administrative violations in journalistic and publishing activities came into force on 1 December 2020. It provides for fines, licence suspension, or other penalties for any media outlet or journalist who publishes information that, amongst others, is "unsuitable to the national interest, causes confusion among people, affects the independence, sovereignty and territorial integrity of the nation, or insults the nation". Similarly, Decree 119/2020/ND-CP imposes fines for violations such as "posting news, photos that do not suit Vietnam's fine customs or information that encourages bad tradition, superstition; posting false information that causes extremely serious consequences; posting information that is not suitable to the interests of the country and the people; that is distorted, fabricated or causing confusion among people; that affects the independence, sovereignty and territorial integrity of the Socialist Republic of Vietnam; that distorts history, denies revolutionary achievements, or offends the nation, national heroes; that affects the great national unity bloc".

Decree 53/2022/ND-CP[12] on elaborating a number of articles of the Law on Cybersecurity of Vietnam came into force on 1 October 2022. The Decree seeks to clarify the application of measures included in the Cybersecurity Law (2018), in particular in relation to the "data localisation" and "mandatory physical establishment" requirements introduced by the Law. It also sets out legal bases for authorities to take action against illegal activities in cyberspace, such as issuing takedown requests, requesting data disclosure or terminating operations of information systems.

The Decree foresees the establishment of a specialized Task Force for cybersecurity protection, comprising of the Department of Cybersecurity and High-

[11] Decree No. 119/2020/ND-CP, 07 October 2020.
[12] Decree No. 53/2022/ND-CP, 15 August 2022.

Tech Crime Prevention and Control under the Ministry of Public Security; and the Military Security Protection Department, the General Political Department, and the Cyber Command, all under the Ministry of National Defense (article 2). The Task Force is responsible for "organizing the appraisal, assessment, inspection, supervision, response and remedy of cybersecurity incidents for information systems important to national security according to their assigned functions and tasks" (article 7).

In article 19.1, the Decree seeks to clarify the type of "illegal content" that may be subject to be taken down. This includes content that:

- infringes national security, propagandizes against the state
- incites violence
- disrupts security or public order
- is humiliating or slanderous
- infringes upon economic management order
- or fabricates or distorts the truth, causing confusion among the people or causing serious damage to socio-economic activities.

According to article 20, illegal activities in cyberspace are those that infringe upon national security, social order and safety, or the lawful rights and interests of agencies, organizations, and individuals. The Director General of the Department of Cybersecurity and High-Tech Crime Prevention and Control (A05) decides on measures to collect e-data to serve the purposes of investigation and handling of such activities.

According to article 26 and 27, a Vietnamese enterprise must store "regulated data" in Viet Nam, namely:

- personal data of users
- data created by Viet Nam-based users, including account name, time of usage, credit card information, email address, IP address, most recent log-out, and registered phone number
- data on the relationships of service users in Viet Nam (i.e, data reflecting and determining the relationship between a service user and other people in the cyberspace).

A foreign enterprise becomes subject to the requirement to store its regulated data and to establish a branch or representative office in Viet Nam only when these triggering conditions are met:

1. The foreign enterprise is doing business in Viet Nam in one of the following fields: telecommunication services; data sharing and storage, provider of a national or international domain for Vietnamese users; e-commerce; social network and social marketing; online games;

provision, management, or operations of other information on the internet in the forms of messages, telephone calls, video calls, email, or online games

2. The services provided by such an enterprise are used to violate the Law on Cybersecurity

3. The Task Force has notified the enterprise and requested the enterprise's cooperation with the prevention, investigation, and handling of such a violation, but the enterprise has not taken any measures for avoiding, dealing with, fighting against, or preventing such breach, or it has resisted, obstructed, or ignored requests from the relevant authorities.

Finally, article 21 details the procedures for implementing measures to suspend, temporarily suspend, or request the termination of operations of information systems and revoke domain names. The Article also prescribes that, in urgent cases, to promptly stop the operation of an information system to avoid causing harm to national security or to prevent potentially harmful consequences, the Department A05 can request concerned agencies, organizations, and individuals to suspend or stop the operation of such information system, and within 24 hours from the time of the request. If this time limit is exceeded without a written decision being issued, the information system may resume operation.

Decree No. 13/2023/ND-CP[13] on the Protection of Personal Data was adopted on 17 April 2023 and will enter into force on 1 October 2023. The decree categorizes personal data as two types: basic and sensitive. Basic personal data includes information about personal identification, such as name, date of birth, place of birth, address, nationality, ethnicity, marital status, ID cards number, and "personal data that reflects activities and activity history in cyberspace". Sensitive personal data includes political and religious opinions; health-related information and genetic data; biometrics; sexual orientation and gender identity; criminal records; financial information; location; and others.

Article 9 elaborates on a wide range of rights individuals have regarding their personal data, including:

- to consent or refuse data processing by others of one's own personal data
- to be informed of personal data being processed by others
- to withdraw consent and demand an end of data processing
- to delete data processed
- to file complaints about violations
- to demand compensation in cases of data abuse

[13] Decree No. 13/2023/ND-CP, 17 April 2023.

Article 13 establishes that data subjects should be notified and give consent before the personal data is processed. However, personal data can be processed without prior notification in the following cases:

- the data subject knows and fully consents to the contents specified in clauses 1 and 2 of article 13

- the personal data is processed by the competent state agency with a view to serving operations by such agency as prescribed by law.

Article 17 further elaborates on circumstance under which personal data can be processed without the consent of data subject, such as:

- to protect the life and health of the data subject or others in an emergency

- in the event of a state of emergency regarding national defense, security, social order and safety, major disasters, or dangerous epidemics; when there is a threat to security and national defense but not to the extent of declaring a state of emergency; to prevent and fight riots and terrorism, crimes and law violations according to the provisions of law.

Finally, article 18 allows competent agencies and organizations to process personal data obtained from audio and video recording activities in public places to protect national security, social order and safety, legitimate rights and interests of organizations and individuals as prescribed by law without the consent of the data subjects. When making audio and video recording, competent agencies and organizations shall notify the data subjects that such data subjects are being recorded, unless otherwise provided for by law.

To enforce Decree 53/2022/ND-CP and Decree 13/2023/ND-CP, the Ministry of Public Security (MPS) has been working on a draft Cybersecurity Administrative Sanctions Decree (CASD). Moreover, the Ministry of Information and Communications of Viet Nam has been working on amendments to the **Telecommunication Law** (2009), which are expected to pass at the end of 2023 and enter into force in 2024. Reportedly, as they stand now, the draft amendments require foreign and local social media networks to confirm the identities of their users. Those who refuse or fail to comply could find their accounts blocked.

Overview of international legal obligations

Before sharing specific observations, we would like to remind your Excellency's Government of the relevant international human rights norms and standards applicable to the right to privacy and freedom of expression, especially online. as guaranteed by articles 17 and 19, respectively, of the International Covenant on Civil and Political Rights ("ICCPR"), which was ratified by Viet Nam on 24 September 1982.

Article 19(1) of the ICCPR protects the right to "hold opinions without interference." Article 19(2), which protects the right to freedom of expression, states that this right shall include the "freedom to seek, receive and impart information and

ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his [or her] choice." As a result, international law protects freedom of expression, including freedom of information, both offline and online.

We would like to further emphasise that, according to international law, any restriction on fundamental rights must be formulated with sufficient precision, be accessible to the population and be subject to a restricted system of exceptions.[14] Article 19, para. 3 of the ICCPR lays down specific conditions which must be fulfilled for the restriction of such rights, and which must further conform to the strict tests of necessity and proportionality:

1. Restrictions must be provided by law. Any restriction "must be made accessible to the public" and "formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly."[15] Moreover, it "must not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution."[16]

2. Restrictions must only be imposed to protect legitimate aims, which are limited to those specified under article 19(3). The term "rights...of others" under article 19(3)(a) includes "human rights as recognized in the Covenant and more generally in international human rights law."[17]

3. Restrictions must be necessary to protect legitimate aims. The requirement of necessity implies an assessment of the proportionality of restrictions, with the aim of ensuring that restrictions "target a specific objective and do not unduly intrude upon the rights of targeted persons."[18] The ensuing interference with third parties' rights must also be limited and justified in the interest supported by the intrusion. Finally, the restriction must be "the least intrusive instrument among those which might achieve the desired result.[19]

The General Assembly and the Human Rights Council have concluded that permissible restrictions on the Internet are the same as those offline.[20] The State has the burden of proof in demonstrating that restrictions are compatible with the Covenant. In cases of national security and counterterrorism, implicating any form of restriction on freedom of expression, States have a duty to justify the genuine purpose and the demonstrable effect of protecting a legitimate national security interest (General Comment No. 34, CCPR/C/GC/34).

It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such

---

14 CCPR/C/GC/34 para. 22.
15 CCPR/C/GC/34.
16 *Id.*
17 *Id.*
18 A/HRC/29/32; CCPR/C/GC/34.
19 CCPR/C/GC/34.
20 A/RES/68/167; A/HRC/RES/26/1.
CPR/C/GC/34, para. 30.

information.[21]

We also recall that the principle of legality requires that laws be formulated with sufficient precision so that individuals can access and understand the law and regulate their conduct accordingly. This clarity and precision prevent unnecessary and disproportionate use of criminal provisions to limit the legitimate activities of human rights defenders, civil society actors and social media activists in the country. In a report to the Human Rights Council, the Special Rapporteur on the right to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions highlighted that the law should be unambiguous, and "sufficiently precise to enable an individual to assess whether or not his or her conduct would be in breach of the law, and also foresee the likely consequences of any such breach" (para. 30).[22] Broadly worded restrictions are not only incompatible with the requirement of legality, but also risk making the scope of the restrictions wider than those required to achieve the legal objective.

We would like to notably underline the "principle of legal certainty" under international law, as enshrined in articles 9(1) and 15 of the ICCPR and article 11 of the UDHR, which requires that criminal laws are sufficiently precise so it is clear what types of behaviour and conduct constitute a criminal offense and what would be the consequence of committing such an offense. This principle recognizes that ill-defined and/or overly broad laws are open to arbitrary application and abuse (A/73/361, para. 34.). Moreover, the law must be formulated with sufficient precision so that the individual can regulate his or her conduct accordingly.

The Human Rights Committee underscored in its general comment N. 27 (1999) the conditions under which States could request to derogate from the right to privacy, as enshrined in article 17 of the ICCPR, in states of emergency or national threat. For such limitations to be international law compliant, they must: (a) be provided by the law (paras. 11–12); (b) not to infringe on the essence of a human right (para. 13); (c) be necessary in a democratic society (para. 11); (d) not allow unfettered discretion when implementing these restrictions (para. 13); (e) serve legitimate aims and be necessary for reaching this legitimate aim (para. 14); (f) be appropriate to achieve their protective function, be the least intrusive instrument amongst those which might achieve the desired result, be proportionate to the interest to be protected (paras. 14–15); (g) be consistent with the other rights guaranteed in the Covenant (para. 18).

Legal analysis

In light of the background, standards, and context above, we would like to bring to your attention the following legal analysis and comments.

Constitution of the Socialist Republic of Viet Nam (2013)

The scope of interpretation of the limitations to fundamental freedoms and rights appears to be overly broad and to go beyond the restrictions permissible under articles 18, 19, 21 and 22 of the ICCPR.

---

[21] CCPR/C/GC/34, para. 30.
[22] A/HRC/31/66.

Criminal Code (2015)

Amendments to the *Criminal Code* passed in 2015 increased the number of prohibited conducts under crimes pertaining to "Offenses Against National Security" and introduced heavier penalties for such crimes. Some of these provisions carry sentences up to life imprisonment or death penalty. The definition of certain crimes related to national security may encompass legitimate expression and may violate the principle of proportionality.

Several UN Human Rights Mechanisms have found that these amendments are not in line with international standards, in particular with the principles of legal certainty, necessity and proportionality of sentencing. They noted that articles 109, 116, 117 and 331 are broadly formulated and vaguely worded, making no distinction between violent crimes and the peaceful and legitimate exercise of the right to freedom of opinion and expression. In the 2019 Concluding Observations on Viet Nam, the Human Rights Committee noted "severe restrictions on freedom of opinion and expression in the country, including through laws and practices that appear not to comply with the principles of legal certainty, necessity and proportionality, such as: (a) The vague and broadly formulated offences in articles 109, 116, 117 and 331 of the Criminal Code and their use to curtail freedom of opinion and expression, and the definition of certain crimes related to national security to encompass legitimate activities, such as exercising the right to freedom of expression". [23]

We acknowledge that the criminalization on the basis vague concepts, such as "Offenses Against National Security", could infringe on protected activities under international human rights law, involving the freedom of opinion and expression and arbitrarily characterize them domestically as 'terrorism', allowing for the arrest, detention or harassment of individuals for exercising internationally protected rights. This definitional conundrum would contravene the "principle of legal certainty", the fundamental principle that the punishment must be commensurate with the crime, and the nullum crimen sine lege prohibition under international law.

Press Law (2016) and Access to Information Law (2016)

Article 9 and Article 13 of the *Press Law* and articles 6 (2) and 11 (2) of the *Access to Information Law* seem to gravely limit the exercise of the freedom to share, seek, receive and access information. These articles punish sharing information not in line with official narrative and make inaccessible the information which "if published, can cause harm to State interests" or which is "against the Social Republic of Viet Nam". Such vague formulations would provide a wide scope of action for authorities to limit the freedom to seek, receive and impart information.

We recall that in its 2019 Concluding Observations on Viet Nam, the Human Rights Committee raised concerns about "State control over the media, with restrictions aimed at ensuring strict adherence to and promotion of government policy, including through the Law on the Press of 2016, which prohibits any criticism of the Government".[24]

---

[23] CCPR/C/VNM/CO/3.
[24] CCPR/C/VNM/CO/3, para 45, article 109.

Cybersecurity Law (2018), Decree 15/2020/ND-CP (2020), Decree 119/2020/ND-CP (2020) and Decree 53/2022/ND-CP (2022)

The *Law on Cybersecurity* and *the recently promulgated Decree 53/2022/ND-CP* may be used to unduly restrict the freedom of expression in cyberspace by prohibiting the provision and use of Internet services to spread information opposing or criticizing public policies. This was also noted by the Human Rights Committee in its 2019 Concluding Observations on Viet Nam.[25]

While combating disinformation online may be a legitimate policy concern, the Cybersecurity Law and Decree 53/2022/ND-CP seem at odds with the principles of legality and legitimate purpose. Vague and overbroad provisions that do not clearly define what information can violate 'national interests' or 'good traditions', and what type of content 'infringes national security, propagandizes against the state' or 'fabricates or distorts the truth, causing confusion among the people or causing serious damage to socio-economic activities' do not seem to comply with international standards. These provisions also seem to allow for unfettered discretion of authorities in determining who 'distorts the people's government' or acts 'against the State' online. We encourage your Excellency's Government to consider alternative means to combat disinformation. Rather than restrictive regulations, the Special Rapporteur on freedom of opinion and expression has previously encouraged States to combat disinformation by enhancing their own transparency and flow of public information, strengthening media freedom, promoting media and digital literacy (See A/HRC/47/25).

In addition, *Decree 15/2020/ND-CP* and *Decree 119/2020/ND-CP* are likely to prevent the sharing information that may be critical of the government positions or policies. Article 101 of Decree 15/2020/ND-CP provides for new and increased penalties against individuals, including civil society actors, who disseminate content such as diverging political views, or reactional ideologies on social media platforms, which do not seem to comply with the principles of necessity and proportionality. The same observations apply to the fines foreseen for violations of Decree 119/2020/ND-CP, as detailed above.

Any restrictions to the operation of websites, blogs or any other internet-based, electronic, or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with article 19 (3) of the ICCPR, as previously underscored by the former Special Rapporteur on freedom of opinion and expression (See A/HRC/35/22). Permissible restrictions should be content-specific. It is also inconsistent with paragraph 3 to prohibit a site or an information dissemination system from publishing material solely on the basis that it may be critical of the government, or the political social system espoused by the government.[26] As such, these provisions seem to seriously infringe on the freedoms of expression and opinion online.

Decree 72/2013/ND-CP (2013)

Article 5 of Decree 72/2023/ND-CP, through its list of prohibited acts, appear to impose undue restrictions on the type of information that civil society actors can

[25] CCPR/C/VNM/CO/3, para 45, article 109.
[26] CCPR/C/GC/34, para. 43.

share and access online. The vagueness of the terms used in the article, such as "false information" or "information for opposing the Socialist Republic of Viet Nam", encompasses a wide range of information. Such limitations may likely contravene the free flow of ideas, a fundamental principle under international human rights law, as guaranteed by article 19 of the ICCPR.

With regard to the use of the term "false information", we recall that the Special Rapporteur on freedom of opinion and expression has previously raised concerns that, whilst recognising the difficulty in finding appropriate responses to the phenomenon, State responses to the issue have often been problematic, heavy handed and had a detrimental impact on human rights (See above mentioned report, para. 3).[27] Often, such laws often do not define with sufficient precision what constitutes false information or what harm they seek to prevent, nor do they require the establishment of a concrete and strong nexus between the act committed and the harm caused (paras. 53-54).[28] The vague and overly broad nature of such laws allows Governments to use them arbitrarily against journalists, political opponents, human rights defenders, and civil society actors.

The Special Rapporteur also emphasised in her report that the right to freedom of expression applies to all kinds of information and ideas, including those that may shock, offend or disturb, and irrespective of the truth or falsehood of the content, and that under international human rights law, individuals have the right to express ill-founded opinions or statements or indulge in parody or satire if they so wish (para. 38).[29] In order to protect legitimate expressions, it is critical that responses by States to the spread of disinformation be grounded in international human rights law, including the principles of legality, legitimacy, necessity, and proportionality (para. 30).[30]

Decree 13/2023/ND-CP (2023)

Articles 13 and 17 of *Decree 13/2023/ND-CP* allow for circumstances under which personal data can be collected and processed by authorities without prior notification and consent from the data subject. These circumstances include 'state of emergency regarding national defense, security, social order and safety, major disasters, or dangerous epidemics; when there is a threat to security and national defense but not to the extent of declaring a state of emergency; to prevent and fight riots and terrorism, crimes and law violations according to the provisions of law'. The overbroad definitions may lead to violations of the right to privacy. We urge your Excellency's Government to take measures to promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online, as a way to protect the right to seek, impart and receive information. We refer you to the report of the Special Rapporteur on freedom of opinion and expression which underscored that "Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression,

---

27 A/HRC/47/25.
28 *Id.*
29 *Id*; CCPR/C/GC/34, paras. 47 and 49; and European Court of Human Rights, Salov v. Ukraine, application No. 65518/01, judgment, 6 September 2005, para. 113: "Article 10 of the [European] Convention [on Human Rights, on freedom of expression] does not prohibit discussion or dissemination of information received even if it is strongly suspected that this information might not be truthful."
30 A/HRC/47/25.

political accountability, public participation and debate." (para. 47).[31] We also note that such vast powers to collect and process personal data without an independent oversight mechanism would allow for arbitrary and unlawful interference with the right to privacy, with implications on other human rights (See also the conclusions of Special Rapporteur on the right to privacy regarding the guiding international principles underpinning privacy and personal data protection that must be incorporated into the national legal system to mitigate the risk of misuse of information and communications technologies (A/77/196) paras. 138-150).

We concur with the findings of the Special Rapporteur on the promotion and protection of human rights while countering terrorism recognizing the considerable impact of surveillance on multiple human rights. The Special Rapporteur highlighted in her report (A/HRC/52/39, para. 45) that "[t]he right to privacy functions as a gateway right protecting and enabling many other rights and freedoms, and its protection is intimately related to the existence and advancement of a democratic society. She therefore sees the escalation in the use of secret surveillance and the collection of content information and metadata for purposes of countering terrorism, combined with the runaway development of underregulated new technologies, as a significant threat to democratic societies."

We respectfully encourage your Excellency's Government to review the abovementioned legislation to bring into line with international human rights norms and standards. National laws and decrees should respect, protect and fulfill human rights. We are at your disposal for any technical expertise you may require in this endeavour.

As it is our responsibility, under the mandates provided to us by the Human Rights Council, to seek to clarify all issues brought to our attention, we would be grateful for your observations on the following matters:

1. Please provide an additional information and/or comment(s) you may have on the above-mentioned observations.

2. Please provide information on the steps your Excellency's Government may take to bring the aforementoned legislation in line with international human rights standards.

3. Please provide further information on the positive measures and oversight provided by your Excellency's Government to protect the right to privacy and protection of personal data and enable the free enjoyment of the right of everyone to freedom of expression online, to end restrictions on online sources of information and the use of the Internet, and to provide a safe space and enabling environment for all to express themselves online freely and safely.

4. Please provide the definitional elements of the terms "threaten the national security, social order, and safety; and sabotage the national fraternity" stipulated in Decree 72/2013/ND-CP; "unsuitable to the national interest, causes confusion among people, affects the independence, sovereignty and territorial integrity of the nation, or

[31] A/HRC/29/32

insults the nation" in Decree 119/2020/ND-CP; "disrupts security or public order" in Decree 53/2022/ND-CP; and "state of emergency regarding national defense, security, social order and safety" in Decree No. 13/2023/ND-CP. Please explain how these terms upholds the principle of legal certainty under international law.

5. Please provide information on the compliance of the abovementioned legal framework invoking "counterterrorism" and "national security" with the provisions of the United Nations Security Council resolutions 1373 (2001), 1456(2003), 1566 (2004), 1624 (2005), 2178 (2014), 2242 (2015), 2341 (2017), 2354 (2017), 2368 (2017), 2370 (2017), 2395 (2017) and 2396 (2017); as well as Human Rights Council resolution 35/34 and General Assembly resolutions 49/60, 51/210, 72/123, 72/180 and 73/174, requiring States to ensure that measures taken to combat terrorism and violent extremism comply with their obligations under international law

This communication, as a comment on pending or recently adopted legislation, regulations or policies, and any response received from your Excellency's Government will be made public via the communications reporting website after 48 hours. They will also subsequently be made available in the usual report to be presented to the Human Rights Council.

Please accept, Excellency, the assurances of our highest consideration.

Irene Khan
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Clement Nyaletsossi Voule
Special Rapporteur on the rights to freedom of peaceful assembly and of association

Ana Brian Nougrères
Special Rapporteur on the right to privacy

Fionnuala Ní Aoláin
Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism